THE UNIVERSITY OF CHICAGO

PERFORMANCE EVALUATION OF WIRELESS NETWORKS USING DEVICE-BASED MEASUREMENT

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER SCIENCE

BY
MUHAMMAD IQBAL CHOLILUR ROCHMAN

CHICAGO, ILLINOIS
JUNE 2024

In loving memory of my father, and with gratitude

to my ever-supportive mom and brother.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The Ph.D. journey is filled with challenges and triumphs, and I'm so grateful for the special people who've celebrated the highs and pushed me through the lows. Their support has made this journey all the more rewarding.

First, I want to offer my gratitudes to advisors and mentors in UChicago CS. Starting with Prof. Monisha Ghosh, I am not sure words are enough to express how grateful I am. We have our own struggles, but you patiently worked with me through my mental health episodes. You helped me navigate my doctoral study and life in general. Thank you for not giving up on me. Prof. Nick Feamster and Prof. Heather Zheng: I feel honored to have you in my doctoral committee. Your unique perspectives and thought-provoking questions have helped shape my research.

Although not directly associated with my research, I want to extend my deepest gratitude to Prof. Haryadi Gunawi to whom I owe my future. You recognized my motivation and lifted me up so I can enter this prestigious institution and further my pursuit of knowledge. Prof. Andrew A. Chien, Prof. Borja Sotomayor, and Prof. Junchen Jiang: thank you for allowing my to be your teaching assistant. You made me realize the joy of teaching and how rewarding it is to see students succeed.

At the start my doctoral study, our research group only consists of me and a postdoc, Vanlin Sathya. For that, I want to thank Vanlin for being my friend and life mentor–we were the best research team that I can ask for. As the lab moved to Notre Dame, we finally got new members: Armed and Seda, thank you for motivating me in academy and spiritual life; Hossein and Josh, our time is still short, so I am looking forward to knowing you better in the future.

Living far from homeland can be very hard, and for that I want to thank my extended Indonesian family: Daniar, Ray, Martin, mas Aji, mas Riza, mas Jeffrey, mbak Lien, mas Jamal, and Tito. You guys made life in this in this foreign land more bearable. Renyu and

Tushant: I'm so grateful to be tackling this Ph.D. alongside you! Thank you for being such a great support.

Thanks also to external collaborators and mentors: Prof. Bill Payne, Prof. Ahmed S. Ibrahim, Prof. Zhi-li Zhang, Prof. Feng Qian, Wei Ye, Arvind Narayanan, Ahmad Hassan, Arun Ramamurthy, Bariq Firmansyah, Damian Fernandez, and Norlen Nunez. All of them have played a role in shaping my wireless research.

The CS department and CS Tech Staffs have been essential to the timely progress of my research projects. I would like to extend my gratitude to current and past staff members: Nita K. Yack, Megan Woodward, Donna Brooms, Sandra Quarles, Margaret Jaffey, Tom Dobes, and Bob Bartlett. I also want to thank the UChicago counselors, Jeong-Eun Suh, Robin Mathew, and Danielle Keys, who helped me navigate my mental health crisis during the pandemic.

I would like to acknowledge the grants that supported my research: NSF (National Science Foundation) CNS-1618692, CNS-1618836, CNS-1618920, CNS-2132700, CNS-2226437, and CNS-2229387.

Last but certainly not least, this journey would have been impossible without the unconditional love and endless support of my family. My late father always encouraged me to pursue a higher degree, even amidst financial hardship. My mother has been a steadfast source of prayer and trust, even when I chose a path beyond her expectations. And my brother, who took care of our family while I was abroad–no words can express my gratitude. Thank you for allowing me the space to discover myself.

ABSTRACT

Traditional network performance simulations and lab tests often miss the complexities of the real world. Device manufacturers and network operators may omit implementing optional features like Multiple User MIMO (MU-MIMO) or massive MIMO due to practical or economic limitations. The resulting lack of clarity on deployed network performance highlights the need for independent, academic measurement reports, free from commercial operators' bias. To achieve this, a scalable and easy-to-use measurement methodology is essential to enable comprehensive assessment of as many deployed networks as possible.

Our research explores the design, techniques, and challenges of leveraging consumer devices as wireless measurement tools. We extract wireless data from devices using standard device APIs and root-access capabilities: the prior is simpler to implement but provides limited access, while the latter requires specific devices but yields more detailed information. These two approaches complement each other: the non-root method enables large-scale data collection with reduced complexity, while the root-based method focuses on in-depth analysis at a smaller scale.

Our combined approach reveals key performance differences between 4G and 5G deployments in low-band (<1 GHz), mid-band (1-6 GHz), and high-band/mmWave (>24 GHz). First, while we confirm the Gigabit-level downlink throughput advertised in 5G mmWave networks, it is limited by range, poor indoor penetration, and device thermal limitations. Next, we observe 5G mid-band outperforms 5G low-band and its 4G counterparts, which is primarily driven by increased bandwidth rather than advanced features. We also uncover adjacent and co-channel interference between 4G and 5G mid-band channels (*i.e.*, CBRS, C-Band spectrum), due to insufficient guard bands and mismatched TDD configurations. These findings underscore the importance of additional spectrum in future 6G networks, while it is also imperative to prioritize the implementation of new features, such as MU-MIMO and higher modulation, for optimal performance.

Beyond cellular networks, our methodology has proven valuable in evaluating the unlicensed spectrum. First, we highlight the sensitivity threshold and hidden node problem that occurs in the coexistence between Wi-Fi and LTE in the unlicensed 5 GHz. Next we focus on the newly released unlicensed 6 GHz utilized by Wi-Fi 6E, particularly the low power indoor (LPI) regime which was created to protect incumbent fixed links. While concerns persist regarding LPI's interference, our extensive measurement campaigns across two university campuses revealed negligible interference due to significant building entry loss. However, further research is necessary to determine appropriate signal levels for the proposed client-to-client (C2C) mode in future Wi-Fi 7 specifications.

Our device-based methodology effectively characterizes both previous-generation (4G and Wi-Fi 5/802.11ac) and current-generation (5G and Wi-Fi 6E) wireless networks. Our findings have directly informed spectrum policies, including energy detection thresholds in the unlicensed 5 GHz spectrum and C2C signal levels in the 6 GHz band. Importantly, our API-based approach has proven scalable and is currently utilized by various US universities within SpectrumX's Broadband Map US project. Additionally, the extensive data we've collected provides a valuable resource for machine learning applications, such as indoor-outdoor classification.

CHAPTER 1

THESIS STATEMENT

In quantifying the performance of a wireless network, it is important that the experiment methodology reflects the actual condition and usage of the said network. While simulations and controlled lab experiments are helpful to understand a wireless deployment, it may not accurately replicate the actual condition of a deployed commercial network due to, for instance, hidden parameters set by the commercial operators. Thus, there is a need of a device-based measurement to observe a deployed network, independent from controlled tests by commercial operators. However, we observed an insufficient number of such measurement methodology in current literature. Therefore, we propose a measurement methodology using currently available consumer devices (*i.e.*, smartphones) as a viable alternative to simulation and lab-based methodology. Our device-based methodology aims to evaluate the performance of cellular and unlicensed wireless networks, enabling us to gain deep insights into network characteristics, identify current challenges and opportunities, and propose data-driven improvements to shape the future of wireless networks.

CHAPTER 2

INTRODUCTION

2.1 Next-Generation Wireless: Challenges and Opportunities

Cellular and Wi-Fi technologies have rapidly evolved, offering dramatic improvements in network speed, capacity, and responsiveness. 5G, the latest generation of cellular networks introduced in the 3GPP Specification Release-16 [2], brings a significant leap forward with new spectrum and wider bandwidths (*e.g.*, mmWave, C-Band), along with advanced techniques like beamforming, massive MIMO (Multiple-Input Multiple-Output), and advanced modulation and coding. Alongside 5G, Wi-Fi 6E [7] has similarly introduces beamforming and massive MIMO techniques, with the addition of the newly opened 6 GHz spectrum. These new features provides greater capacity, lower latency, and reduced interference for demanding applications like virtual and augmented reality, high-definition video streaming, vehicular networks, and large-scale IoT deployments. No doubt, global 5G subscription has grown to 1.6 billion in 2023 [80], while 473 million Wi-Fi 6E devices are expected to be shipped in 2023 [81].

Despite substantial progress, deploying advanced networks like 5G and Wi-Fi 6E poses unique challenges. 5G introduces new spectrum bands, specifically the high-band/mmWave (>24 GHz) and mid-band (1-6 GHz), offering increased bandwidth to complement existing low-band (<1 GHz) deployments. Similarly, Wi-Fi 6E opens up 1200 MHz of unlicensed spectrum in the 6 GHz band. This focus on expanding bandwidth underscores the push by wireless stakeholders to support ever-increasing data demands. Consequently, policymakers face a crucial question: Do operators genuinely require additional spectrum, or are existing allocations underutilized? Cellular carriers tout the progress of their 5G networks [24, 36], potentially introducing a bias in performance evaluations. Additionally, the Citizen Broadband Radio Service (CBRS) band offers a valuable case study, as it pioneered shared-environment

deployment of a 3GPP system. Understanding coexistence dynamics in CBRS is crucial for optimizing future designs and spectrum sharing strategies. These factors underscore the vital need for independent, unbiased research to assess real-world network performance and guide effective spectrum policy.

2.2 Device-Based Methodology for Performance Measurement

We chose user device (*i.e.*, smartphone) which possess a range of sensors and software capabilities that enable the extraction of granular network performance metrics. Additionally, their ubiquity allows for large-scale, geographically distributed data collection, reflecting the real-world experiences of users under diverse conditions. Passive background monitoring using devices can provide valuable insights into network performance variations across time and location. Timestamping and GPS tagging of data can be used to map coverage and identify location-based performance trends. This approach is arguably cost-effective, avoiding the need for specialized equipment.

Network measurement tools in smartphones can be broadly categorized into two approaches based on their data source:

- **Device APIs:** This approach offers access to various wireless parameters, including cell signal strength (RSSI, RSRP, RSRQ), unique network identifiers (PCI, BSSID), channel frequency and bandwidth, and network configuration data. While easier to implement, the data is limited to the parameters exposed by the device manufacturer's API.

- **Root Access:** This method enables direct interaction with the radio chipset, yielding detailed information such as carrier aggregation details, beamforming information, modulation and coding schemes, and more. However, it requires specific devices with root access and relies on technical knowledge that may not be publicly available.

These approaches present a trade-off: the non-root API method is simpler and supports large-scale data collection, but with a limited set of parameters. The root-based approach offers in-depth analysis at the cost of complexity and device restrictions. Combining these approaches allows for flexible measurement strategies: the non-root method for wide-scale data gathering, and the root-based method for focused, detailed studies. Both approaches can be enriched by incorporating active measurements to gather metrics like throughput, latency, and jitter.

Device-based measurement has compelling use cases. It enables crowd-sourced network mapping to pinpoint coverage gaps or underperforming areas. Users can leverage it for personal connectivity troubleshooting. Operators benefit from user-generated data for network planning and optimization. Lastly, researchers can use this approach to investigate network performance trends, the impact of device heterogeneity, or the effectiveness of new wireless technologies.

2.3 Thesis Outline and Contributions

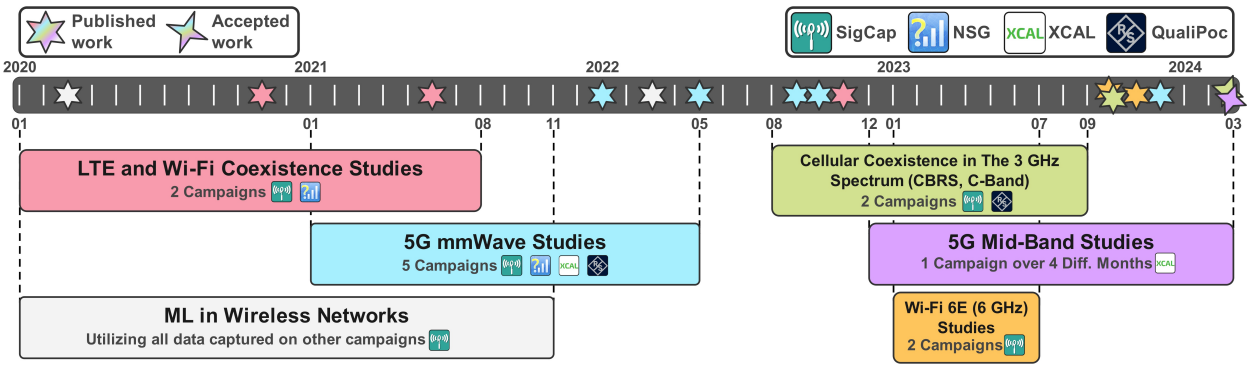


Figure 2.1: Timeline depicting measurements campaigns and published works.

We start with providing the necessary background on our methodology in Chapter 3. In particular, our API-based methodology has been utilized in the FCC's pilot wireless measurement program as a part of the Broadband DATA Act [46], and in the SpectrumX's

Broadband Map US project [59]. The remaining outline and major contributions of this dissertation is discussed below in the given order.

(Chapter 4) *LTE and Wi-Fi Coexistence in The 5 GHz Spectrum*: With growing demand, cellular networks are extending into unlicensed bands traditionally used by Wi-Fi. Two key approaches are Licensed Assisted Access (LAA) and LTE-Unlicensed (LTE-U). LAA utilizes listen-before-talk (LBT) with an energy detection threshold, while LTE-U relies on duty cycling. Our research investigates the impact of these parameters on coexistence. Simulations suggest a symmetrical threshold for LAA and a 0.5 duty cycle for LTE-U offer optimal performance [93]. Focusing on LAA deployments in Chicago, we observed dense coexistence with Wi-Fi, leading to potential hidden node issues due to asymmetrical thresholds (LAA energy: -72 dBm, Wi-Fi preamble: -82 dBm, Wi-Fi energy: -62 dBm) [103]. Our study is the first measurement study on LAA deployments at this scale. Further studies at specific locations confirmed the hidden node issues which shows performance degradation for Wi-Fi clients [108, 101]. Moreover, our findings have influenced European regulations to standardize the energy detection threshold of -72 dBm for all technologies accessing the 6 GHz band [37].

(Chapter 5) *Wi-Fi 6E (6 GHz) Deployment Studies*: The release of the 6 GHz spectrum introduces two distinct approaches for mitigating interference with incumbent point-to-point fixed links: standard power (SP) with higher transmit power but constrained by an automatic frequency control (AFC) system, and low power indoor (LPI) with reduced power and no AFC, but with more stringent requirements to prevent outdoor deployments (no weatherizing or battery power). Since LPI deployments are the only one currently available, we focus on evaluating their potential interference [29, 30]. Our extensive measurement campaigns across two university campuses are the first measurement studies at this scale, and they indicate negligible interference from LPI access points (APs). Outdoor RSSI values

ranged from -64 to -95 dBm (median -89 dBm), demonstrating substantial signal attenuation caused by double-pane low-emission windows (12-16 dB loss) and solid brick walls (25-33 dB loss). Additionally, only 5% of indoor BSSIDs were detectable outdoors. These findings have been submitted to the FCC [52] for spectrum policy considerations. Additionally, we have submitted a comment to inform FCC on the appropriate signal levels for the proposed client-to-client (C2C) mode in the 6 GHz spectrum [54].

(Chapter 6) ***Survey and Analysis of 5G Deployments*****:** As the 5G specification matures and deployments expand, we focus on measuring various aspects of newly deployed 5G networks across different frequency bands. Our analysis of a dense mmWave deployment in Chicago, compared with a similar deployment in Miami, confirms the potential for Gigabit-level downlink throughput but reveals severe range limitations [95, 96]. Furthermore, our comparison of two operators' mmWave deployments in the Chicago Loop area highlights the impact of configuration parameters (*e.g.*, beam management, signal propagation) on coverage and performance [76]. Importantly, we also identified performance degradation in mmWave networks due to thermal throttling and outdoor-to-indoor losses [99, 94]. As operators begin deploying 5G mid-band, we investigated its performance compared to 4G mid-band networks [97]. We observed higher throughput in 5G mid-band deployments compared to the 4G mid-band counterparts, while both 4G and 5G mid-band outperformed low-band networks. However, this improvement appears primarily driven by increased bandwidth availability rather than the full implementation of new 5G features like massive MIMO and 1024-QAM. Our findings underscore that while bandwidth expansion is crucial for network advancement, operators must also prioritize the implementation of new 5G features such as massive MIMO, advanced modulation, and channel aggregation. These features are necessary for realizing the full potential of 5G technology.

(Chapter 7) ***Cellular Coexistence in The 3 GHz Spectrum*****:** The repurposing of

the 3 GHz spectrum is crucial for 5G development in the US. This spectrum encompasses AMBIT (3450-3550 MHz), CBRS (3550-3700 MHz), and C-Band (3700-3980 MHz), with the Department of Defense's 3100-3450 MHz band also under consideration [79]. Due to the lack of guard bands and diverse implementation strategies within these segments (*e.g.*, power limits, technologies, channelization), adjacent channel interference is a concern. Our research reveals interference issues between adjacent CBRS and C-Band deployments, with highest downlink throughput performance degradation due to the offending client transmitting in uplink [98]. This interference problem are mitigated when the CBRS channel is moved 20 MHz lower, introducing a guard band. The CBRS spectrum is particularly notable for pioneering shared-access model, using the General Authorized Access tier, enabling flexible deployment by multiple service providers. However, this flexibility raises the challenge of secondary coexistence, where overlapping channels occur. Our work uncovers high occurrences of overlapping channels between South Bend City's private CBRS and Verizon's deployments, attributed to the Spectrum Access System (SAS) not taking coexistence into account during channel allocation [120]. These overlaps degrade throughput performance due to co-channel interference. We actively addressed this by coordinating non-overlapping channels with South Bend's provider. Understanding secondary and adjacent channel coexistence is crucial for optimizing future spectrum designs and policies. Our work underscores the need for coordination mechanisms or refined SAS algorithms to prevent interference in shared-spectrum environments, ensuring equitable access for all users while maximizing spectrum efficiency.

(Chapter 8) ***Machine Learning in Wireless Networks*****:** Our device-based methodology captures a large wireless dataset with abundant parameters, thus they are challenging to analyze manually, such that we focus only on specific set of parameters. On the other hand, machine learning (ML) offers a powerful alternative to traditional heuristics, enabling us to extract valuable insights for network performance improvement. One example in-

volves applying machine learning to facilitate fair coexistence between LTE-U and Wi-Fi. Our work utilizes machine learning to detect the number of Wi-Fi transmissions based on received signal strength (RSSI), allowing for dynamic adjustment of the LTE-U duty cycle [32]. This approach achieves a near-perfect detection rate with minimal delay. Another of our work leverages machine learning on cellular and Wi-Fi data to determine whether a device is indoor or outdoor based on captured wireless data [89]. This is particularly relevant for LPI deployments, where APs are typically limited to indoor use due to restrictions on weatherproofing and battery power. Our approach utilizes machine learning to predict the indoor/outdoor environment for both APs and clients, potentially relaxing these limitations. The model achieves a high accuracy of 99.1%, even when relying solely on Wi-Fi signals (reducing accuracy to 98.8%), but may struggle in specific scenarios like storefronts with large windows. This highlight the need of incorporating a wider range of data and labels (*e.g.*, "indoor near window"), as the classification accuracy will further improve with more data from diverse environments.

Lastly, Appendix A contains supplementary information including the detailed information of signal parameters captured by one of our device-based measurement tool, SigCap.

CHAPTER 3

OVERVIEW OF DEVICE-BASED METHODOLOGY

Wireless network measurements can be broadly categorized as active or passive. Active measurements generate traffic to obtain performance metrics, while passive measurements analyze existing network signals. While both approaches offer valuable insights, we prioritize passive measurement techniques due to the limited availability of tools for this methodology. Recognizing this gap, we developed SigCap, an Android application for passive extraction and analysis of cellular and Wi-Fi signal information using standard APIs [92]. SigCap provides an accessible solution for researchers, though API limitations restrict the types of data it can collect. To overcome these limitations, we also explore root-based passive measurement tools like Network Signal Guru, Accuver XCAL, and QualiPoc [87, 8, 100]. These tools offer access to detailed signal data, leveraging device root privileges. However, their complex setup, expense, and difficulty in extracting data limit their widespread use.

Consequently, we adopt a combined methodology tailored to our research goals. SigCap provides ease of use and accessibility for initial analysis. When deeper insights into specific signal parameters are needed, we opt for root-based tools despite their challenges. This flexible approach maximizes the advantages of both methods while addressing their limitations. Table 3.1 summarized the general feature differences between SigCap and NSG, note that "all channels" denotes primary, secondary, and neighboring channels.

Table 3.1: Measurement Apps' Features

Features	**SigCap**	**Root-based Apps (NSG, QualiPoc, XCAL)**
LTE Cell Information	**All LTE channels:** PCI, EARFCN, Band, RSRP, RSRQ, RSSI, Primary/Other CA Designation. **Primary LTE:** Bandwidth	**All LTE channels:** PCI, EARFCN, Band, Bandwidth, RSRP, RSRQ, RSSI, SINR, CQI, MIMO Mode, MCS Index, Modulation, RB Allocation, BLER, Primary/Secondary/Neighboring CA Designation.
5G Cell Information	**All NR channels:** PCI, NR-ARFCN, Band, SS-RSRP, SS-RSRQ, Primary/Other CA Designation.	**All NR channels:** PCI, NR-ARFCN, Band, Bandwidth, SSB/Beam ID, SS-RSRP, SS-RSRQ, SINR, CQI, CSI-RSRP, RI, CRI, MIMO Mode, # of MIMO Layer, MCS Index, Modulation, RB Allocation, BLER, Primary/Secondary/Neighboring CA Designation.
Wi-Fi Information	**Connected and neighboring APs:** BSSID, SSID, Primary Frequency, Center Frequency, Bandwidth, RSSI, Wi-Fi Amendment, Transmit Power, # of Connected Clients, Channel Occupancy Ratio. **Connected AP:** TX & RX Link Speed, Max. TX & RX Link Speed.	***(QualiPoc Only)*** **Connected and neighboring APs:** BSSID, SSID, Primary Frequency, Center Frequency, Bandwidth, RSSI.
Throughput-related Metrics	Application layer throughput and latency.	Application, RLC, MAC, and PHY layer uplink/downlink throughput.
Other Parameters	GPS Coordinates and Accuracy, Phone Model.	***(QualiPoc and XCAL Only)*:** GPS Coordinates and Accuracy, Phone Model.
Root access	No	Yes

3.1 API-based Approach (Non-Root): SigCap

SigCap is an Android app we developed to extracts cellular and Wi-Fi signal values from the Android Application Programming Interface (API) [14, 28]. These signal values are associated with a timestamp and a GPS location [27]. Further on our research, we were also interested in capturing sensor data, particularly CPU and skin temperature [13]. These API values are directly extracted from the modem chipset, therefore we assume the values are valid as it is also used by the chipset's operations. However, there are some limitations on some API calls which we further discuss on Appendix A, thus we limit our assumption and analysis only to parameters that are confirmed to be accurate. We check for parameters' accuracy by doing preliminary measurements and confirm the values with root-based apps.

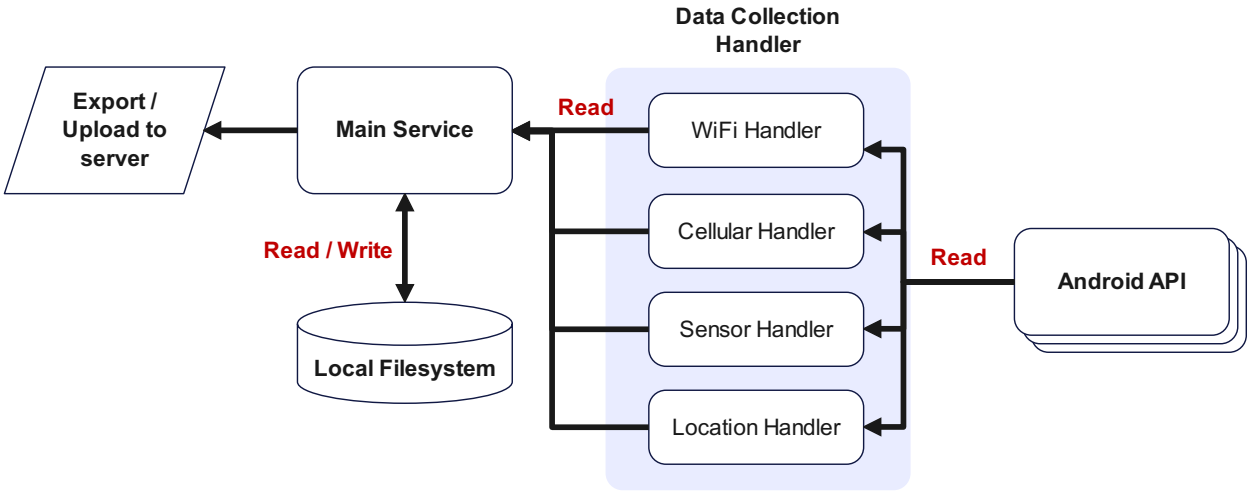


Figure 3.1: SigCap architecture.

Fig. 3.1 shows the application architecture of SigCap. Each of data collection handler calls its respective API and updates the main service with the newest data. Table 3.2 shows the list of parameters collected in each update interval. In summary, every data point contains a timestamp, a GPS location data, a sensor data, along with multiple LTE, NR, and Wi-Fi data. Each LTE, NR, and Wi-Fi data point represents the respective unique cellular base station or Wi-Fi access point. As of recent, we added a suite of active measurement tools

Table 3.2: SigCap Datapoint.

Parameter	**API Call / Derived**	**Explanation**
Version	API Call	SigCap version number.
Android Version	API Call	Android API version number.
UUID	Derived	Randomly generated string to identify a single device.
Device Name	API Call	Device model name as assigned by the system.
Operator Name	API Call	Describes current operator name, as shown in the OS UI.
SIM Operator Name	API Call	Describes SIM operator name, may be different to the operator name due to roaming.
Carrier Operator Name	API Call	Describes carrier operator name, may be different to the operator name due to roaming.
Network Type	Derived	Describes cellular network type (*e.g.*, LTE, NR). Extended from API call by adding extra labels (*e.g.*, Wi-Fi, NR-SA, NR-NSA) derived from the Wi-Fi and cellular information.
Phone Radio Type	API Call	Describes type of radio used in voice call (*i.e.*, None, GSM, CDMA, SIP).
Timestamp	API Call	Timestamp at the data creation/update including timezone.
Location Data	Derived	Location data as described in Table A.5.
Sensor Data	Derived	Sensor data as described in Table A.6.
LTE Data	Derived	Set of LTE channel data as described in Table A.2.
NR Data	Derived	Set of NR channel data as described in Table A.3.
Additional NR Data	Derived	Additional NR-NSA data as described in Table A.4.
Wi-Fi Data	Derived	Set of Wi-Fi AP data as described in Table A.1.
iperf Data	Derived	Downlink/uplink throughput using TCP/UDP protocol.
ping Data	Derived	Round trip latency using ICMP.
HTTP Data	Derived	Downlink throughput using HTTP protocol.

to SigCap: iperf [61] and a simple HTTP downloader to measure throughput, along with a ping tool to measure round trip latency. Prior to that, we utilized **FCC Speedtest (FCC ST)** [45] which similarly measures throughput and latency in a limited interval.

SigCap data collection is linked to GPS updates, limiting the sampling interval to the minimum allowed by the Location API (SigCap can handle up to 1 second sampling interval, but we set it to 5 seconds for battery efficiency). We store each data point as a JSON file on the device's filesystem, allowing for easy export (*e.g.*, via email or messaging) or upload to a cloud server. For further analysis, we process the JSON files in two ways: as CSVs for data

visualization, or as maps for spatial analysis. This methodology was used in the majority of our works, as discussed in §4.3, §5.2, §6.2, §6.4, and §8.3. Furthermore, SigCap has been utilized in the FCC's pilot wireless measurement program as a part of the Broadband DATA Act [46], and in the SpectrumX's Broadband Map US project [59].

3.2 Root-Based Approaches

On Android devices, rooting grants administrative control, often referred to as "superuser" access. While Android's operating system includes restrictive safeguards to protect users, these limits can hinder comprehensive network analysis. Device APIs offer some access to network data, but detailed cellular information is particularly restricted. Root-based measurement apps bypass these restrictions by directly probing the cellular chipset. However, since the techniques for this are not publicly available, existing root-based tools are often expensive and complex. Therefore, we strategically employ root-based apps for focused cellular studies where detailed data is essential.

We strategically employ various root-based tools for detailed cellular network analysis, depending on their availability and features. All these tools capture extensive LTE and NR parameters, along with timestamps and GPS coordinates, enabling spatial and temporal studies. Our toolkit has evolved over time: Initially, we used **Network Signal Guru (NSG)** [87], which requires manual rooting but doesn't offer data extraction capabilities. We transitioned to **Accuver XCAL** [8] for its data export feature, though it requires tethering to a laptop and doesn't involve manual rooting. Currently, we utilize **QualiPoc** [100], which offers a streamlined experience with a bundled phone and tool, and allows data extraction via an HTML interface. Table 3.3 shows some of detailed cellular parameters available only in the root-based tools.

Table 3.3: Detailed Cellular Data Available in Root-Based Tools.

Parameter	**Radio Tech.**	**Explanation**
SSB (Synchronization Signal Block) SSB	5G	Identifier for a specific SSB (Synchronization Signal Block) within a cell. SSBs are used for initial cell discovery and synchronization and also denotes unique beam.
SCS (Subcarrier Spacing)	5G	The spacing between individual subcarriers within the transmission bandwidth. Smaller SCS allows for higher potential data rates but also increases complexity.
CSI-RSRP	5G	Measured power of the received CSI (Channel State Information) signal. An indicator of overall channel quality.
RB (Resource Block)	4G, 5G	A basic unit of resource allocation. Consists of multiple subcarriers within a specific time slot.
Modulation	4G, 5G	Specific technique used to represent digital data as a signal for transmission (e.g., QPSK, 16QAM).
MCS (Modulation and Coding Scheme)	4G, 5G	Combination of modulation techniqueand error-correcting code used for data transmission. MCS options offer trade-offs between data rate and robustness.
BLER (Block Error Rate)	4G, 5G	The percentage of resource blocks that are received incorrectly. An indicator of the quality of the received signal.
MIMO Mode	4G, 5G	Configuration of the MIMO system, specifying the number of transmit and receive antennas used (*e.g.*,, 2x2, 4x4).
MIMO Layer	5G	The number of independent data streams transmitted or received simultaneously using MIMO techniques.
CQI (Channel Quality Indicator)	4G, 5G	Feedback signal from the UE to the gNB indicating the perceived channel quality. Used for MCS decision.
RI (Rank Indicator)	4G, 5G	Signal from the gNB to the UE indicating the preferred number of downlink layers for transmission.

CHAPTER 4

LTE AND WI-FI COEXISTENCE STUDIES

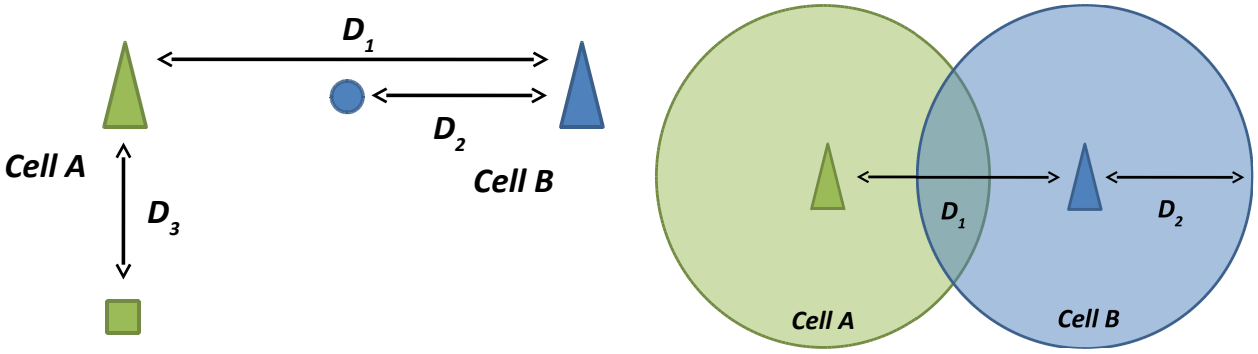
4.1 Overview and Related Works

The Licensed Assisted Access (LAA) is an extension to the 4G LTE specification for enabling access in the unlicensed 5 GHz spectrum which was previously dominated by Wi-Fi. To enable fairness in the unlicensed spectrum, LAA implements a listen-before-talk (LBT) scheme similar to Wi-Fi's collision avoidance (CSMA-CA) scheme. However, LBT is implemented with a -72 dBm energy detection threshold, while CSMA-CA uses -62 dBm energy threshold for non-Wi-Fi nodes. This asymmetry of energy threshold leads to a hidden node problem which then causes a lower throughput performance for Wi-Fi. In this works, we used both controlled simulation and measurement using real devices to demonstrate such problems.

There are theoretical analyses [74, 119] and limited experiments [126, 75] that studied the fairness of LTE and Wi-Fi coexistence. The ns-3 simulator has also been used to study the coexistence fairness between LTE and Wi-Fi [57], but the analysis does not show in detail what the impact on different threshold values is and how the channel gains access by LAA once the medium is won. We explored in detail the important role of energy detection threshold to improve coexistence. The main results obtained from our extensive simulation study is that Wi-Fi, LAA and LTE-U all have improved throughput and latency performance when the energy detection threshold used by Wi-Fi in the presence of LTE is lowered to -82 dBm, *i.e.*, if Wi-Fi treats LTE-LAA and LTE-U as another coexisting Wi-Fi cell instead of as an interfering noise source. Furthermore, we confirm this observation using device-based measurements on LAA and Wi-Fi deployments.

4.2 Impact of Energy Detection Threshold to the Coexistence Between LTE and Wi-Fi in the Unlicensed Spectrum

To measure the coexistence between LTE and Wi-Fi, ns-3 simulator [93] is used due to the early stage of LTE specification on unlicensed spectrum access. At the time, there are two competing standards on unlicensed access: LAA and LTE-U. The former is developed by the 3GPP alliance [1] and uses sensing scheme namely Listen Before Talk (LBT), while the latter is developed by the LTE-U forum [71] and uses duty cycle (on-off cycle). The LTE and Wi-Fi coexistence module is developed as an extension to the ns-3 simulator to bridge between the Wi-Fi and LTE module, ensuring coexistence in the simulation [83].



(a) Experiment #1

(b) Experiment #2 & #3

Figure 4.1: ns-3 experiment setup.

We assume a simulation system model where the cellular network (either LTE-LAA or LTE-U) will be using the unlicensed spectrum for downlink only data transmissions, which will be shared with a co-channel Wi-Fi Access Point (AP). The control information and any uplink data is always transmitted using licensed spectrum. To access unlicensed spectrum LAA Base Station (BS) and clients will use LBT scheme which is based on Wi-Fi's CSMA. On the other hand, LTE-U will follow the fixed duty cycle mechanism based on a fair sharing scheme (*i.e.*, $\frac{1}{N}$, N is the total number of unlicensed AP/BS deployed nearby) among operators. We assume there is no coordination between the different LTE BSs and Wi-Fi APs. Hence, our approach is distributed in nature. The traffic is assumed to be

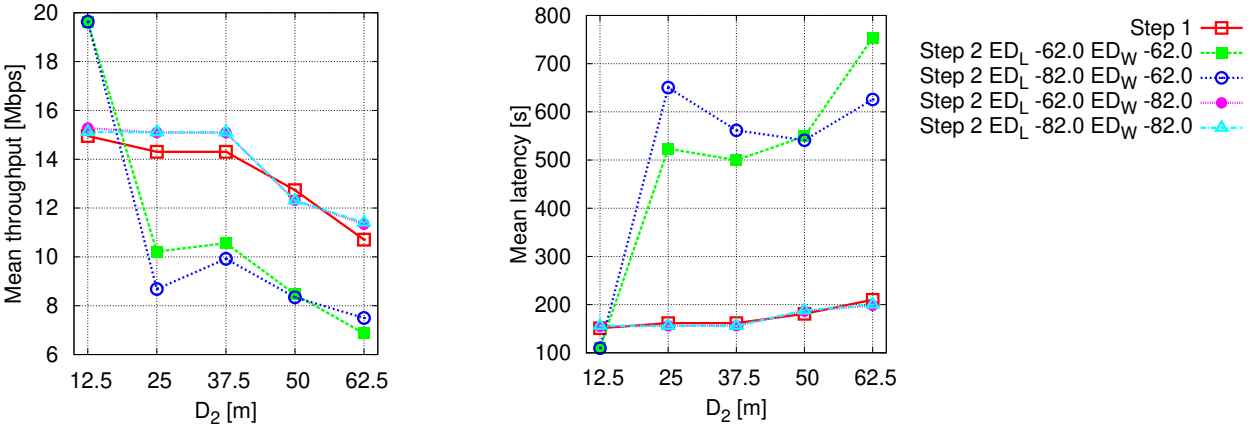
Table 4.1: ns-3 simulation parameters.

Parameters	**Experiment # 1**	**Experiment # 2**
ED_L	-62, -82 dBm	-62, -72, -82 dBm
ED_W	-62, -82 dBm	-62, -72, -82 dBm
D_1	75 m	25, 50, 75, 100, 125, 150 m
D_2	12.5, 25, 37.5, 50, 62.5 m	75 m
D_3	50 m	M/A
No. of users for each cell	1	20
BS transmit power	18 dBm	18 dBm
BS antenna gain	0 dB	5 dB
UE/STA transmit power	18 dBm	18 dBm
UE/STA antenna gain	0 dB	0 dB
Noise figure	5 dB	5 dB
RTS/CTS	Not enabled	-
A-MPDU	Not enabled	-
LTE & Wi-Fi antenna mode	SISO	SISO
Operating frequency	5.180 GHZ	5.180 GHZ
Wi-Fi rate control	Ideal Wi-Fi manager	Ideal Wi-Fi manager
LAA rate control	Proportional Fair (PF)	Proportional Fair (PF)
Traffic	UDP	UDP
Full buffer (saturation)	Yes	Yes
Simulation time	48 s	48 s

Poisson with parameter λ.

We define 3 experiment setups, as shown in Fig. 4.1, where Experiment #1 is is a "simple" experiment with only one user in each cell, where we define D_1 and D_3 as fixed and vary the D_2. We set up the experiment in this fashion in order to to highlight the effect of the hidden node problem on a single Wi-Fi user. Then, the position of both cells are switched to observe the opposite effect (*i.e.,* Cell A STA is in between Cell A and B BS, Cell B STA is perpendicular to its BS). On the other hand, Experiment #2 more appropriately reflects a real deployment by uniform-randomly deploying 20 clients on each cell. D_1 is varied while D_2 is fixed. The ns-3 framework also enables varying parameters such as Wi-Fi and LAA energy detection threshold (ED_W and ED_L, respectively) as shown in Table 4.1.

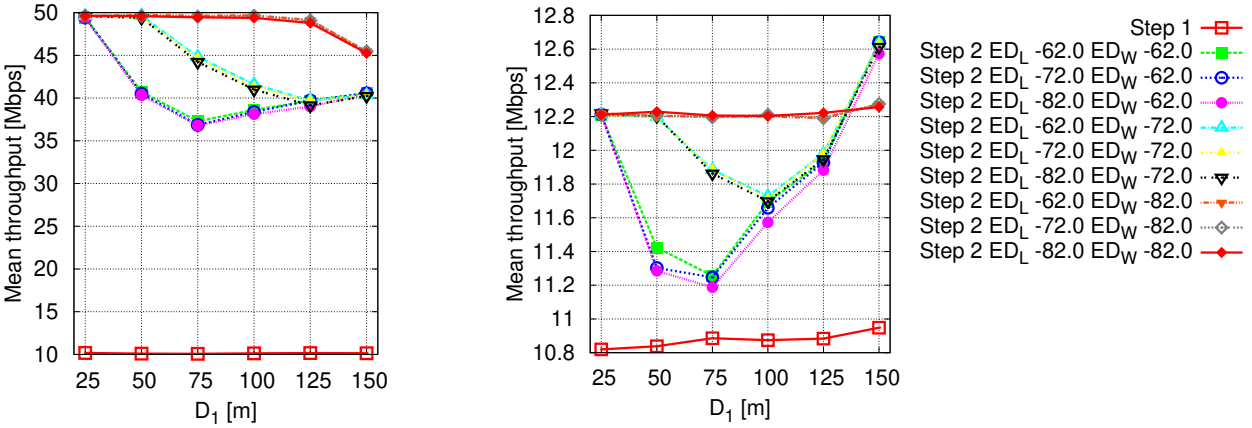
Using the various parameters, we also simulate two steps: Step 1 where Cell A and Cell



(a) Mean throughput of Cell B

(b) Mean latency of Cell B

Figure 4.2: Experiment #1, Step 1: Cell A uses Wi-Fi, Step 2: Cell A uses LAA.



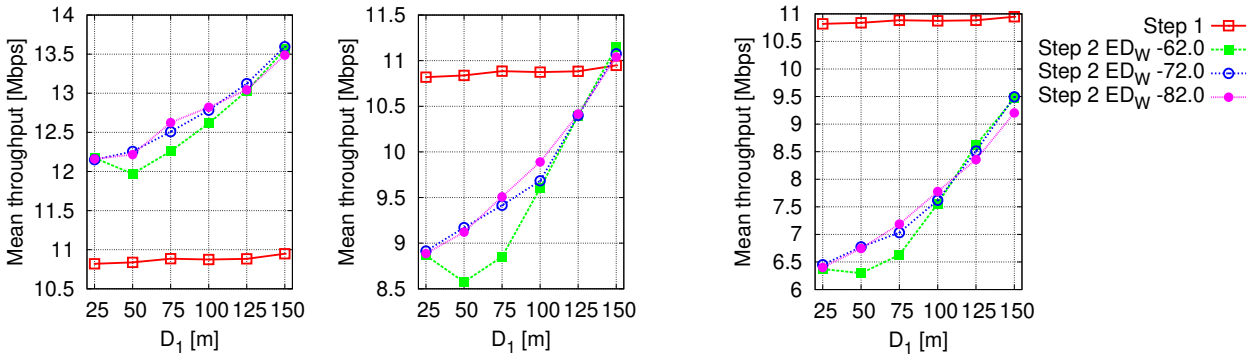
(a) Mean throughput of Cell A

(b) Mean throughput of Cell B

Figure 4.3: Experiment #2, Step 1: Cell A uses Wi-Fi, Step 2: Cell A uses LAA.

B both use Wi-Fi, and Step 2 where Cell A switches to LAA or LTE-U and Cell B continues using Wi-Fi. On Experiment #1 and #2 (Wi-Fi and LAA) as shown on Fig. 4.2 and 4.3, Cell B shows a performance decrease on the default energy detection threshold (Wi-Fi -62 dBm, LAA -72 dBm). Wi-Fi can only keep the same level of performance when both Wi-Fi and LAA uses the same threshold of -82 dBm, *i.e.*, Wi-Fi treats LAA as another coexisting Wi-Fi cell instead of as an interfering noise source. Experiment #3 shown on Fig. 4.4 also similarly shows a better performance when Wi-Fi uses a threshold of -82 dBm.

This methodology enables us to simulate LTE and Wi-Fi coexistence in a large scale



(a) Duty Cycle = 0.3 (b) Duty Cycle = 0.5 (c) Duty Cycle = 0.7

Figure 4.4: Experiment #3, Mean throughput of Cell B, Step 1: Cell A uses Wi-Fi, Step 2: Cell A uses LTE-U.

with dense deployments. However, the assumptions in our simulations may not accurately reflect the actual deployment. Therefore, a direct measurement of an actual deployment is required to further understand the performance impact of coexistence between LAA and Wi-Fi, specifically, and wireless networks in general.

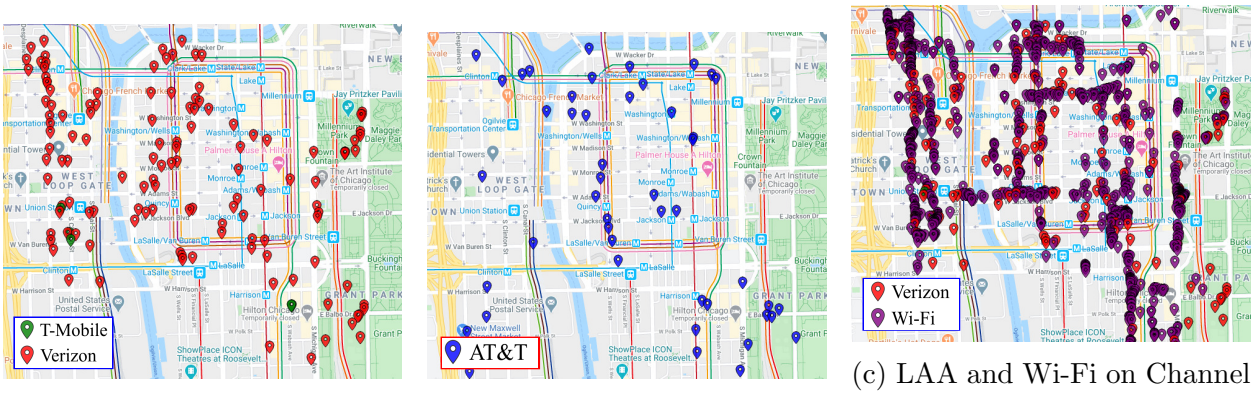
4.3 Coexistence Studies of Wi-Fi and LAA in the unlicensed spectrum at Chicago

Continuing from simulation of the Wi-Fi and LAA coexistence, we introduce our device-based measurement to conduct coexistence studies in deployments around University of Chicago (UChicago), Illinois Institute of Technology (ITT), and the Loop Area of Chicago [103]. As of March 2020, LAA has emerged as the dominant specification used by LTE for unlicensed spectrum access, and there are rapid deployment of LAA Base Stations (BSs) from the three major US operator (*i.e.*, AT&T, T-Mobile, Verizon). In addition of a wide deployment survey, we also conducted a focused experiments to study hidden node problem at UChicago [101] over the months of April and June-August 2021, and at ITT [108] over January 2020.

4.3.1 Survey of LAA and Wi-Fi Deployments

Experiment setup and deployment analysis. Using Google Pixel 3 phones equipped with SIMs from the three major US operators (*i.e.*, AT&T, T-Mobile, and Verizon), we collected SigCap data by walking on sidewalk, driving car, and riding public transportation. In this work, we defined a 10 second data interval to conserve power. As of March 2020, we observed LAA deployments from the operators with 57 unique LAA PCIs and 10639 unique Wi-Fi BSSIDs in the vicinity of the observed LAA deployments (we only report Wi-Fi measurements in locations where we also observe at least one LAA PCI). Furthermore, AT&T and Verizon's LAA cells are primarily deployed around the densely populated Loop area (as shown on Fig. 4.5a and 4.5b), while the T-Mobile deployments are in the less dense residential areas and on the IIT campus.

Statistics of overlapping LAA and Wi-Fi. Using frequency and RSSI data captured by



(a) LAA on Channel 36 (b) LAA on Channel 149 (c) LAA and Wi-Fi on Channel 36

Figure 4.5: Deployment of LAA by AT&T, T-Mobile and Verizon LAA and coexisting Wi-Fi on Channels 36 and 149.

SigCap, we compiled the number of overlapping LAA and Wi-Fi deployment and its RSSI statistics, as shown on Table 4.2. We observe a huge number of Wi-Fi AP overlapped LAA BS in terms of channel deployment. Moreover, a larger number of Wi-Fi APs deployed in 40 and 80 MHz bandwidth compared to 20 MHz, thus a single Wi-Fi AP may overlap with multiple LAA BSs. Most of prior works only consider the coexistence scenario where Wi-Fi and LAA uses 20 MHz bandwidth. Thus, we focused on the multi-channel coexistence problem, where LAA that deployed in aggregate of three 20 MHz channels would create an interesting coexistence scenario with 80 MHz Wi-Fi.

4.3.2 Impact of Hidden Node Problem in LAA and Wi-Fi Coexistence

As a supplement to the SigCap methodology, we employ root-based tools, namely Network Signal Guru (NSG), to further extract signal information that are hidden to SigCap. These information are (but not limited to) physical layer throughput, TXOP, signal-to-interference-and-noise ratio (SINR), block error rate (BLER), and allocated resource blocks (RB) for each channel. However, to analyze the data collected by NSG requires manual works of directly transcribing the values from the UI. Thus, we only reserve this methodology for a focused analysis that requires a deeper level of signal information.

Table 4.2: LAA and Wi-Fi deployment and RSSI statistics.

Wi-Fi-equivalent Channel Numbers	LAA Deployment			Overlapping Wi-Fi
	AT&T	T-Mobile	Verizon	
Channel 36	4	49	209	3089
Channel 40	5	38	222	2750
Channel 44	4	38	205	3009
Channel 48	0	0	0	3189
Channel 149	104	0	2	2673
Channel 153	119	1	4	2569
Channel 157	131	1	22	2648
Channel 161	38	0	25	2601
Channel 165	27	0	20	105

(a) LAA and Wi-Fi deployment statistics

RSSI Metrics	LAA	Wi-Fi		
		20 MHz	40 MHz	80 MHz
Mean (dBm)	-84.49	-82.19	-82.87	-83.65
Variance	63.92	46.41	34.55	19.3
Range (dBm)	[-105, -45]	[-95, -47]	[-95, -56]	[-95, -51]

(b) LAA and Wi-Fi RSSI statistics

Using NSG, we set to answer two questions: (1) What is the effect of multi-channel coexistence between 80 MHz Wi-Fi and 3×20 MHz LAA? And, (2) what is the effect of TXOP and traffic types on the coexistence? Table 4.3 shows access categories for different types of traffic on LAA and Wi-Fi, which shows the same four categories on both specifications, *i.e.*, voice, video, best effort, and background. However, there is a difference in the values of the channel sensing parameters (*i.e.*, initial CCA/channel sensing, minimum/maximum Contention Window, and TXOP). This may lead to unfairness in terms of time needed for medium access and time spent to hold the medium.

Experiment setup. To answer the two research questions posed, we constructed a co-existence experiment at two LAA deployments near two university campuses: T-Mobile at IIT [108] and AT&T at UChicago [101]. At both locations, we deployed multiple Wi-Fi APs and 5 smartphones as Wi-Fi and LAA clients, equipped with SigCap and NSG. There are two coexistence scenarios: (1) Wi-Fi/Wi-Fi coexistence, with all phones as Wi-Fi clients, and (2)

Table 4.3: Access categories in LAA and Wi-Fi.

Access Class # (DL)	**Initial CCA**	**CWmin**	**CWmax**	$TXOP$
1 (Voice)	25 μ s	30 μ s	70 μ s	2 ms
2 (Video)	25 μ s	70 μ s	150 μ s	3 ms
3 (Best Effort)	43 μ s	150 μ s	630 μ s	8 ms or 10 ms
4 (Background)	79 μ s	150 μ s	10.23 ms	8 ms or 10 ms

(a) Downlink LAA

Access Category	**AIFS (Initial CCA)**	**CWmin**	**CWmax**	$TXOP$
Voice (AC_VO)	18 μ s	27 μ s	63 μ s	2.08 ms
Video (AC_VI)	18 μ s	62 μ s	135 μ s	4.096 ms
Best Effort (AC_BE)	27 μ s	135 μ s	9.207 ms	2.528 ms
Background (AC_BK)	63 μ s	135 μ s	9.207 ms	2.528 ms

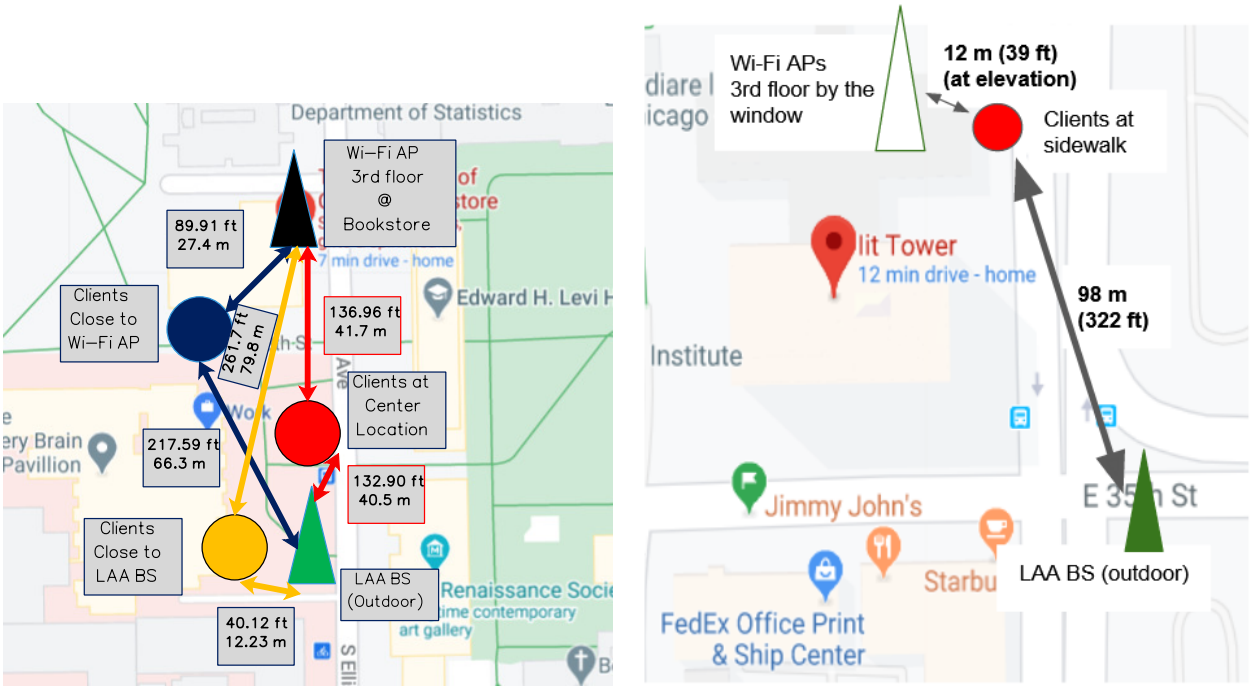
(b) Wi-Fi (802.11ac)

LAA/Wi-Fi coexistence, with 4 phones as Wi-Fi clients and 1 phone as an LAA client. We also used laptops with Wireshark to capture Wi-Fi packets in monitor mode. Fig. 4.6 shows the location of AP, BS, and clients on each site. For the brevity of the analysis, we only present the analysis at UChicago site (Fig. 4.6a) for clients at the center location (distance to LAA BS: 40.5 m, distance to Wi-Fi AP: 41.7 m).

At the UChicago site, there is an LAA BS on the Wi-Fi-equivalent channel number 149, 154, and 157, with each 20 MHz bandwidth (combined: 5.735-5.795 GHz). To overlap this, we set three Wi-Fi APs to primary channel 149, 153, and 157 with 80 MHz bandwidth (5.735-5.815 GHz), but for brevity we only include the analysis of one AP in primary channel 157. At the IIT site, the LAA BS is set to channel 36, 40, 44 (combined: 5.17-5.23 GHz), while we set 5 Wi-Fi APs in varying bandwidths and primary channels, but for brevity we only present the results for all Wi-Fi APs on primary channel 36 and 20 MHz bandwidth (5.17-5.19 GHz).

To observe the impact of access categories to fairness, we generated multiple types of traffic:

- **Data (D):** Downlink data traffic assumed as a full buffer, generated by downloading



(a) Experiments at UChicago

(b) Experiments at IIT

Figure 4.6: Experiment locations.

a large YUV dataset (>10 GB) using HTTP (TCP) protocol from Derf Test Media Collection [26].

- **Video (V):** A Youtube video is downloaded, with a resolution of 1920×1080 and bit-rate of 12 Mbps.
- **Data + Video (D+V):** Combination of data and video traffic as described above.
- **Streaming (S):** A live stream video on Youtube is loaded, with a resolution of 1280×720 and a bit rate of 7.5 Mbps.
- **Data + Streaming (D+S):** Combination of data and streaming traffic as described above.

LAA: RB allocation, TXOP, and baseline throughput. At both locations, we all RB are allocated to the phones indicating that our phones are the only one using the channel. We

observed 8 ms TXOP for **D**, **D+V**, and **D+S** traffics, indicating that the data transmission enables the maximum TXOP. Next, **V** traffic is transmitted using 3 ms TXOP, as shown in Table 4.3a. Lastly, **S** traffic is transmitted only through licensed primary channel (with the LAA channels disabled), indicating traffic prioritization for QoS. Table 4.4 represents baseline LAA throughput at the UChicago site. We observe a similar baseline throughput at IIT.

Table 4.4: Baseline throughput of LAA alone (no Wi-Fi) at UChicago site.

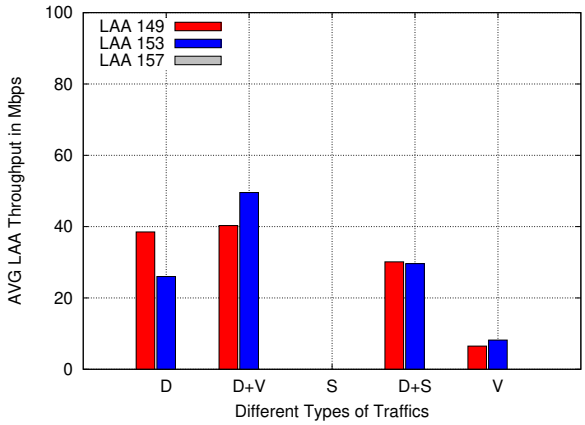
Channels	**D**	**D+V**	**S**	**D+S**	**V**
Licensed	26.3 Mbps	32.7 Mbps	8.4 Mbps	12.2 Mbps	10.9 Mbps
LAA 149	53.5 Mbps	58.6 Mbps	-	44.1 Mbps	8.1 Mbps
LAA 153	60.4 Mbps	67.1 Mbps	-	52.9 Mbps	9.8 Mbps
LAA 157	61.5 Mbps	61.9 Mbps	-	49.4 Mbps	8.3 Mbps

Table 4.5: Average LAA SINR at UChicago site under coexistence.

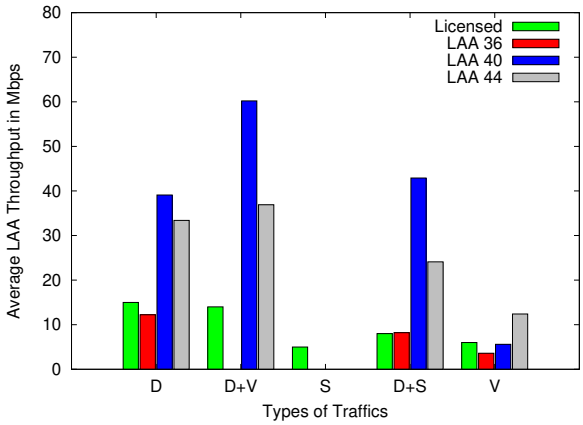
LAA Channel	**D**	**D+V**	**S**	**D+S**	**V**
LAA 149	14 dB	12.6 dB	-	9.7 dB	12.8 dB
LAA 153	10 dB	11.4 dB	-	8.2 dB	14.2 dB
LAA 157	-2 dB	-3.2 dB	-	-1.9 dB	-2.9 dB

Impact of Wi-Fi interference to LAA. As Wi-Fi interference is introduced, we observed lower SINR and downlink throughput on LAA transmission. Table 4.5 shows the average SINR of LAA client under coexistence at the UChicago site. We observe lower SINR for LAA channel 157, which is also the primary channel of the deployed AP at UChicago site. This is reflected on the throughput of LAA client, Fig. 4.7a shows no downlink throughput on LAA channel 157 compared to the baseline (Table 4.4. Similarly, Fig. 4.7b shows little to no throughput on LAA channel 36, which is also the primary channel of the deployed AP at IIT site. This results clearly shows the impact Wi-Fi primary channel selection to LAA throughput.

Impact of LAA interference to Wi-Fi. Similarly, Wi-Fi clients' throughput are also

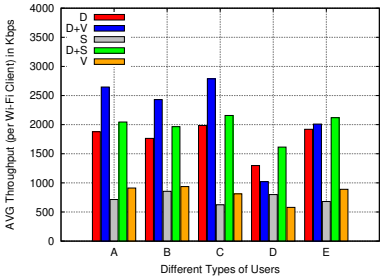


(a) Experiments at UChicago

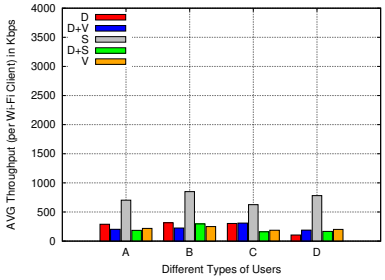


(b) Experiments at IIT

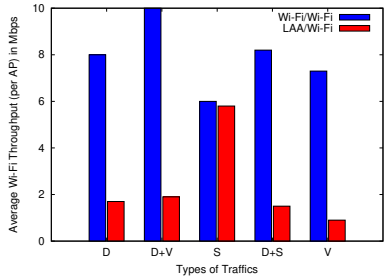
Figure 4.7: Average downlink throughput of LAA client on LAA/Wi-Fi coexistence at different sites.



(a) Wi-Fi/Wi-Fi Coexistence at UChicago

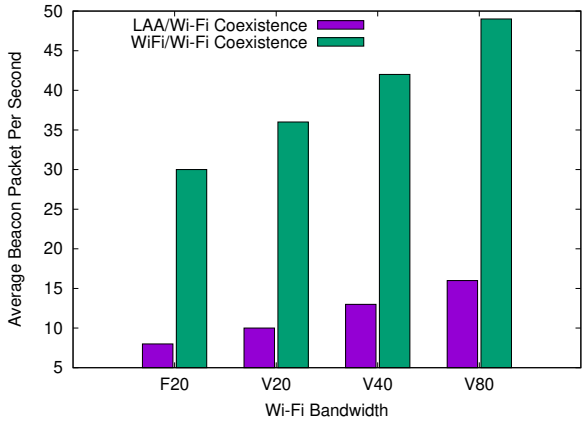


(b) LAA/Wi-Fi Coexistence at UChicago

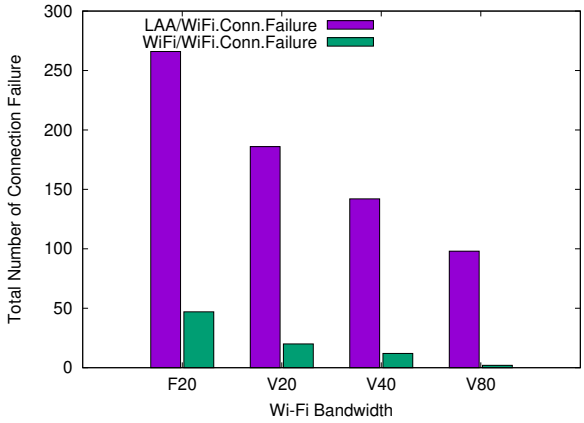


(c) Wi-Fi/Wi-Fi and LAA/Wi-Fi Coexistence at IIT

Figure 4.8: Average downlink throughput of Wi-Fi clients on LAA/Wi-Fi coexistence at different sites.



(a) Number of Wi-Fi beacon



(b) Number of failure connection (disassociation packet)

Figure 4.9: Impact of LAA interference to Wi-Fi control packets.

impacted by LAA interference. Fig. 4.8a illustrates the average throughput of 5 Wi-Fi clients (labelled A to E) on Wi-Fi/Wi-Fi coexistence, while Fig. 4.8b shows a similar values on LAA/Wi-Fi coexistence (client E was used as LAA client). Both Fig. 4.8a and 4.8b shows a throughput degradation for all Wi-Fi clients when interfered by LAA, with the exception of **S** traffic due to the client exclusively using primary LTE licensed channel. Likewise, Fig. 4.8c shows an average throughput degradation for all Wi-Fi clients (average over all clients) when interfered by LAA, except on **S** traffic.

In addition to throughput degradation, we discover an increasing number of connection failure when LAA is interfering Wi-Fi at the IIT site. Using a laptop with Wireshark to capture Wi-Fi packets, we observe a decrease in captured Wi-Fi beacon as shown in Fig. 4.9a, and an increase of Wi-Fi connection failure (*i.e.*, number of disassociation packets), on LAA/Wi-Fi coexistence scenario. With the throughput degradation and increasing connection failure, we have demonstrated a higher impact on Wi-Fi when coexisting with LAA. While the impact on LAA is lesser, and even lessened due to having a licensed spectrum as a fail-over. Thus we concluded so far, a fair coexistence is not achieved in our coexistence studies.

4.4 Summary and List of Accomplishments

This chapter shows our first step in developing the device-based measurement. To validate our simulation findings and gain insights into real-world network behavior, we developed a device-based measurement methodology which aims to be quick and scalable. Our extensive simulation studies revealed potential throughput and latency improvements in Wi-Fi and LAA networks when Wi-Fi's energy detection threshold in the presence of LTE is lowered to -82 dBm. This approach allows Wi-Fi to treat LTE-LAA and LTE-U as coexisting Wi-Fi cells rather than interfering noise sources. We validated this discovery through a device-based measurement methodology applied to real-world LAA and Wi-Fi deployments. Results confirmed that the default asymmetrical energy detection threshold between LAA and Wi-Fi leads to decreased Wi-Fi throughput and connectivity issues. These problems are particularly noticeable when the Wi-Fi primary channel and LAA channel overlap.

The following papers has been published in the topic of LTE and Wi-Fi coexistence:

- Muhammad Iqbal Rochman et al. "Impact of changing energy detection thresholds on fair coexistence of Wi-Fi and LTE in the unlicensed spectrum". In: *2017 Wireless Telecommunications Symposium (WTS)*. IEEE. 2017, pp. 1–9.

- Vanlin Sathya et al. "Measurement-based coexistence studies of LAA & Wi-Fi deployments in Chicago". In: *IEEE Wireless Communications* (2020).

- Vanlin Sathya et al. "Hidden-nodes in coexisting LAA & Wi-Fi: a measurement study of real deployments". In: *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE. 2021, pp. 1–7.

- Vanlin Sathya et al. "Impact of hidden node problem in association and data transmission for LAA Wi-Fi coexistence". In: *Computer Communications 195*. 2022, pp. 187–206.

Additionally, we presented our findings to the wireless industry, namely to the 802.11 Coexistence Steering Committee. We presented our findings on the energy detection threshold in 2019 [53] and on the impact of hidden nodes problem in 2021 [102]. Our findings has been used as a consideration by the European regulation body to set the same energy detection threshold of -72 dBm for all radio technologies accessing the 6 GHz spectrum [37].

CHAPTER 5

THE WI-FI 6E (6 GHZ) DEPLOYMENT STUDIES

5.1 Overview and Related Works

The 6 GHz band, currently utilized by Wi-Fi 6E, includes four U-NII bands (U-NII-5 to U-NII-8) which are shared with incumbent users (see Table 5.1). To protect incumbents, unlicensed devices operate under two power classes: Low Power Indoor (LPI) and Standard Power (SP). LPI allows indoor access points (APs) to use the entire 6 GHz band without Automatic Frequency Control (AFC). SP APs, while offering wider coverage, are currently limited to U-NII-5 and U-NII-7 and require AFC (still under development) to avoid interference. Wi-Fi 6E devices gain 14 additional 80 MHz channels and 7 additional 160 MHz channels across the 1200 MHz spectrum. We focus on LPI deployments due to the ongoing development of AFC for SP deployments.

Table 5.1: Unlicensed Operation over 6 GHz.

Band	**Incumbents**	**Use Cases**	**Chann. No.**	**Freq. (MHz)**
U-NII-5	Fixed, Satellite Uplink	LPI, SP	1-97	5925-6425
U-NII-6	Satellite uplink, BAS, CTRS	LPI	101-117	6425-6525
U-NII-7	Fixed, Satellite uplink/downlink	LPI, SP	121-185	6525-6875
U-NII-8	Fixed, Satellite, BAS	LPI	189-233	6875-7125

Unlike the 5 GHz band regulations, Wi-Fi 6E APs operating under LPI rules in the 6 GHz band must adhere to a maximum power spectral density (PSD) of 5 dBm/MHz, regardless of the channel bandwidth [109]. This corresponds to maximum transmit (Tx) powers shown in Table 5.2. While APs are limited to indoor use, client devices (STAs) can be anywhere, including outdoors, and are therefore required to transmit 6 dB less power than the AP.

While the academic literature explores various coexistence scenarios in the 6 GHz band, there's a lack of research analyzing potential interference to incumbent systems. Current studies focused on incumbent coexistence are primarily conducted by industry stakeholders,

Table 5.2: Max. Tx Power for 6 GHz LPI.

Device Type	**Maximum TX Power**				
	20 MHz	40 MHz	80 MHz	160 MHz	320 MHz
STA	12 dBm	15 dBm	18 dBm	21 dBm	24 dBm
AP	18 dBm	21 dBm	24 dBm	27 dBm	30 dBm

particularly fixed-link operators and unlicensed proponents. These studies often analyze contrived scenarios, such as intentionally placing Wi-Fi 6E APs near windows to directly interfere with incumbent links [34, 35, 69, 38, 39]. Such setups may not accurately represent real-world deployments. Hence our goal is to understand the statistics of interference based on a dense real-world deployments at the University of Michigan and the University of Notre Dame, instead of worst-case scenarios.

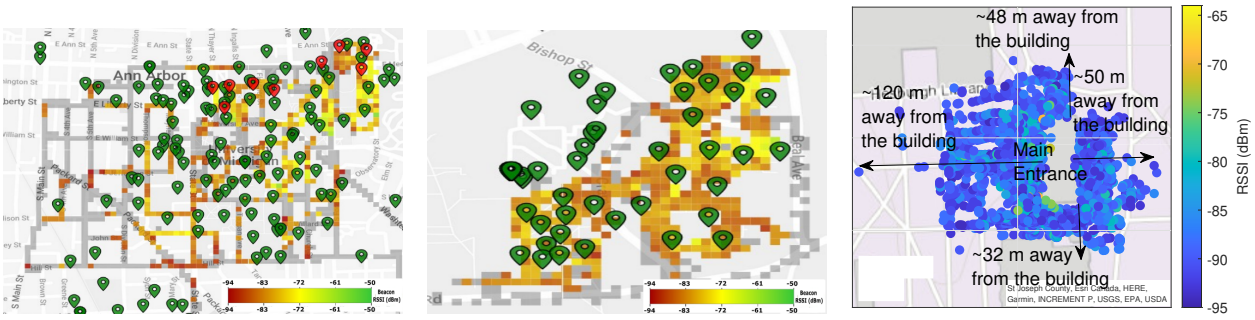
5.2 Indoor and Outdoor Measurement Studies of Wi-Fi 6E Deployments

5.2.1 Measurement Tools

Client devices were used to capture signal information in various environments, using two tools, SigCap and Wireshark, on smartphones and laptops respectively, to extract various signal parameters as shown in Table 5.3.

Table 5.3: Measurement tools and devices.

Tool	**Wi-Fi Parameters**	**Devices**
SigCap	Time-stamp, location, frequency, RSSI, BSSID, SSID, #STA, Channel Utilization	1 × Google Pixel 6, 1 × Samsung S21 Ultra, 3 × Samsung S22+
Wireshark	Source/Destination, SSID, BSSID, Frequency, RSSI, Tx Power, beacon and data packets	Laptop: ThinkPad P16 Gen 1, Wi-Fi Card: Intel(R) Wi-Fi 6E AX211 160 MHz, OS: Ubuntu 22.04 LTS
Ookla (MC3 only)	Time-stamp, location, download & upload speed	1 × Google Pixel 6, 3 × Samsung S22+



(a) Main campus area (MCA) at UMich (MC1, MC2).

(b) Residential area (RA) at UMich (MC2).

(c) Measurement building at UND (MC3).

Figure 5.1: RSSI heatmap for Outdoor Measurements at UMich and UND. Green pins: buildings with Wi-Fi 6E APs. Red pins: Drone experiment locations.

SigCap is utilized to passively collects time and geo-stamped wireless signal parameters (cellular and Wi-Fi) through APIs without root access. Wi-Fi parameters, such as RSSI, channel, BSSID, etc. are collected from the beacon frames every 5 seconds. Optional beacon elements with information on Tx signal power, number of stations connected to each BSSID and channel utilization (percentage of time that the AP senses the channel to be busy) are also collected: fortunately, all the Wi-Fi 6E APs deployed in UMich broadcast these optional elements, thus facilitating our analysis. **Wireshark** is an open source tool that we used for capturing both beacon and data frames using a Lenovo ThinkPad P16 Gen1 with the Intel(R) Wi-Fi AX211 Wi-Fi adapter.

5.2.2 Methodology

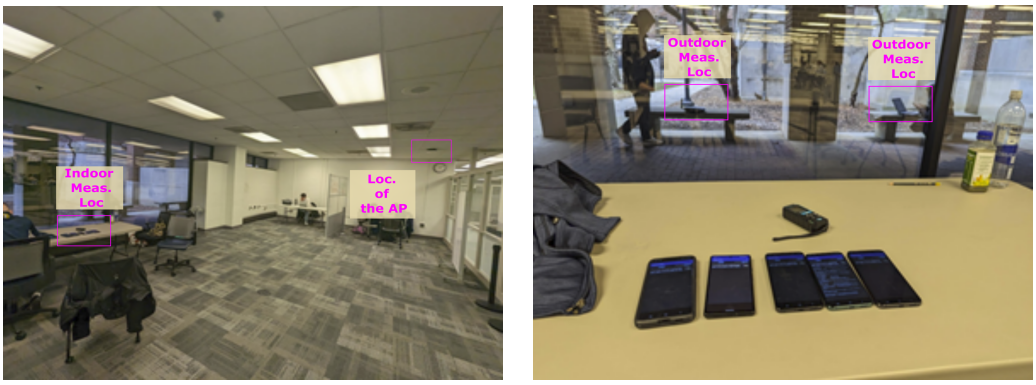
The measurements were conducted in three campaigns, as described below.

Measurement Campaign 1 (MC1): MC1 took place on January 7-9, 2023, during which measurements were conducted while driving and in a fixed location on the University of Michigan (UMich) campus.

Driving Measurements were conducted in the Main Campus Area (MCA) of UMich as shown in Fig. 5.1a between 9:50 pm and 00:50 am, at a speed of 20 miles per hour. Data

was collected with SigCap running on the five smartphones listed in Table 5.3. Due to the cold weather, walking measurements were not conducted in MC1.

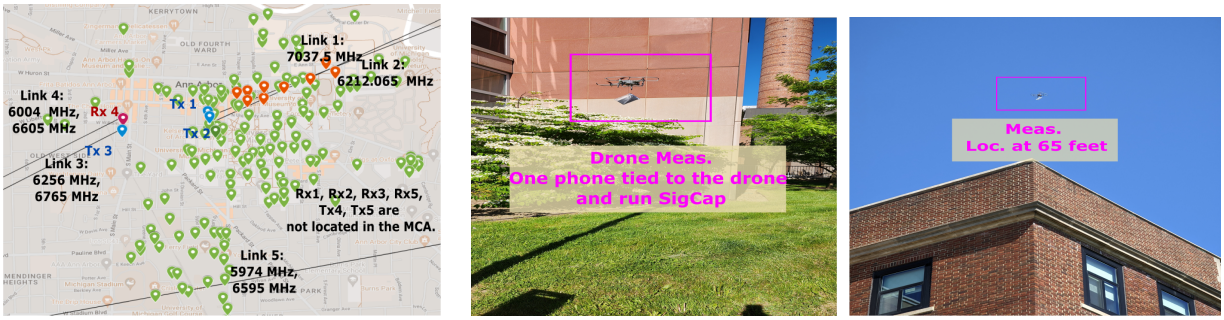
Fixed Location 1 (FL1) measurements were taken inside and outside a building with an open indoor area with high occupancy. Fig. 5.2a shows the position of the Wi-Fi 6E LPI AP in the space. The AP is positioned 6 meters away from double pane low-E windows. The indoor measurements were taken by placing the phones near the window while the outdoor measurement location is 1.5 meters from the window. Wireshark and Sigcap were both used for measurements, as shown in Fig. 5.2b. The AP transmit power was 15 dBm over a 160 MHz channel bandwidth, which is considerably lower than the regulatory limits specified in Table 5.2. This reduction in transmit power is due to the dense deployment of LPI APs, since many users need to be supported in this area.



(a) Indoor location and Wi-Fi 6E AP. (b) Outdoor locations.

Figure 5.2: Measurement and AP locations for FL1 (MC1).

Measurement Campaign 2 (MC2): MC2 was conducted on May 24-27, 2023 at UMich with drone, driving, walking, and fixed location measurements. The deployment had been changed from mostly 160 MHz channels observed in MC1 to mostly 80 MHz channels during MC2. This was done by UMich Information and Technology Services (ITS) to serve more users with a higher quality of service. However, since our analysis depends on measurements of the 20 MHz beacon channel RSSI, this change did not affect our results or comparisons.



(a) 6 GHz fixed links.

(b) Drone measurement scenario.

Figure 5.3: 6 GHz fixed links and drone meas. scenario at UMich (MC2). Orange pins: drone meas. locations, Blue: Tx locations, Red: Rx location.

Drone Measurements: There are five active, fixed links in the MCA, as shown by the black lines in Fig. 5.3a. Three of these links have their transmitters (*i.e.*, Tx1, Tx2 and Tx3 in the figure) located within the MCA, while the transmitters of the other two links (Tx4 and Tx5) are positioned at a significant distance away from the campus. Rx4 is the only receiver (Rx) on campus but the link direction is away from the buildings with dense deployments. Nine buildings, indicated by the orange pins in Fig. 5.3a, were chosen for drone measurements due to their proximity to Links 1 and 2, operating at center frequencies 7037.5 MHz and 6212.065 MHz with bandwidths of 25 MHz and 56 MHz respectively [42, 41]. Table 5.4 provides information on the height of these buildings and the number of Wi-Fi 6E LPI APs deployed in each. On average, we assume two BSSIDs per AP in 6 GHz as determined by UMich ITS. The drone measurements were conducted during daylight hours over a period of three days. As shown in Fig. 5.3b, a Samsung S22+ smartphone with SigCap was tied to the drone for data collection. The drone moved vertically up and down, parallel to the wall of a given building.

Driving Measurements: In order to validate the driving measurements conducted in MC1 (Fig. 5.1a), we replicated the same route as closely as possible. The measurements were carried out between 10:00 pm to 12:00 am, mirroring the timeframe of MC1 using the same 5 phones with SigCap.

Table 5.4: Building information for drone measurements.

Building Name	Height (ft)	No. of AP/BSSIDs
Building 1 (BLD1)	58	43/86
Building 2 (BLD2)	40	184/368
Building 3 (BLD3)	45	44/88
Building 4 (BLD4)	47-65 wrt. upper and lower levels	400/800
Building 5 (BLD5)	58	39/78
Building 6 (BLD6)	65-85 wrt. upper and lower levels	46/92
Building 7 (BLD7)	75	40/80
Building 8 (BLD8)	70	40/80
Building 9 (BLD9)	70	40/80

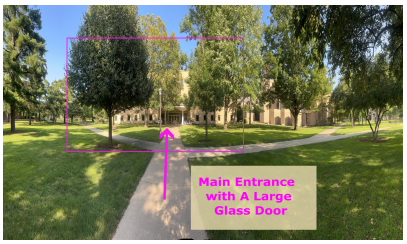
Walking Measurements: The center of the campus, where Wi-Fi 6E is densely deployed, offers only pedestrian access. Hence RSSI measurements were collected in this area by walking with hand-held phones running SigCap. The walking and driving measurements are combined (also with MC1) to produce heatmap as shown in Fig. 5.1a. We similarly measured the Residential Area (RA) of UMich, as shown in Fig. 5.1b, between 12:00 pm and 3:00 pm.

Fixed Location 2 (FL2): The measurement area is a conventional classroom on the first floor of a building, shown in Fig. 5.4. The single AP in the room is center-mounted on the ceiling, and the room has a north facing exterior wall. The outdoor measurement location is 7 meters away from this wall due to trees obstructing closer access.

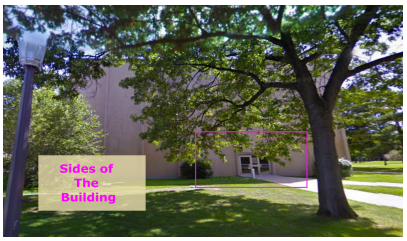
(a) Indoor locations and Wi-Fi 6E AP. (b) Outdoor locations.

Figure 5.4: Measurement and AP locations for FL2 (MC2).

Measurement Campaign 3 (MC3): MC3 was conducted on during June and July 2023 at the UND with walking and fixed location measurements around and inside the building



(a) Frontside of the measurement building: With a large glass door.



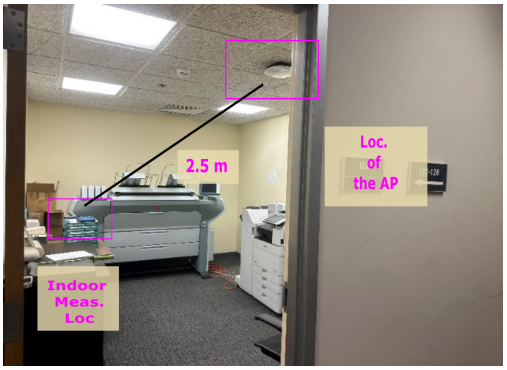
(b) Sides of the measurement building: With a glass door, no windows.

(c) Backside of the measurement building: No windows on the first floor.

Figure 5.5: Measurement environment at the UND.

shown in Figs. 5.1c and 5.5. The number of deployed Wi-Fi 6E LPI APs is 70, with 15 dBm Tx power and 80 MHz channel bandwidth. The number of unique BSSIDs is two for each AP.

Walking Measurements: Walking measurements are conducted at the front, side, and back of the building. As seen in Figs. 5.5a and 5.5b, the front of the building has a big glass door and multiple wide windows, while the side walls have only a glass door and no window. The back wall has no window in the first floor, while small windows are present in the upper floors as shown in Fig. 5.5c. Data was collected with SigCap running on the 4 phones given in Table 5.3 (omitting the use of S21 Ultra phone).



(a) FL3.

(b) FL4.

Figure 5.6: Measurement and AP locations for FL3 and FL4 (MC3).

Fixed Location 3 (FL3): The measurement area of FL1 is a typical room with a single AP on the first floor of the building, as shown in Fig. 5.6a. The AP is center-mounted on

the ceiling, 3 m away from the exterior wall. The indoor measurement location is 2.5 m away from the AP and the outdoor measurements were carried out right outside the exterior wall.

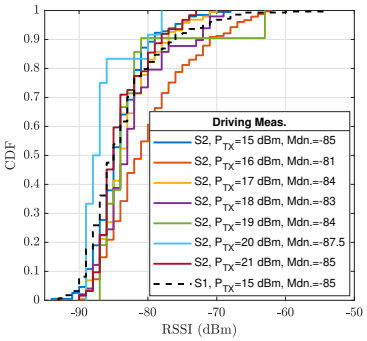
Fixed Location 4 (FL4): FL2 measurement area is a corridor on the same floor, shown in Fig. 5.6b. The AP is on the wall, with antennas pointing downwards, at a distance of 9 m from the exterior wall. Indoor measurements were conducted in front of the exterior wall, while outdoor measurements were performed outside the exterior wall.

5.2.3 Results and Discussions

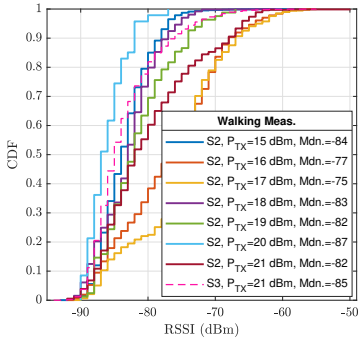
We present statistical analyses of the measurements under different conditions. The discussions are categorized into three main groups at the two measurement locations: (i) ground level driving & walking measurements (and the resulting analysis on C2C enabling level), (ii) aerial drone measurements (only at UMich), and (iii) indoor-outdoor building entry loss (BEL) measurements.

Driving and Walking Measurements at UMich (MC1 & MC2): The minimum and maximum RSSI values measured across the MCA are -94 dBm and -62 dBm for the driving measurements, and -92 dBm and -55 dBm for the walking measurements, respectively. Transmit power levels ranging from $P_{TX} = 15$ dBm to $P_{TX} = 21$ dBm were observed within the MCA, with $P_{TX} = 16$ dBm being the most frequently used. 73% and 95% of the RSSI measurements were with $P_{TX} \leq 18$ dBm for the driving and walking measurements in the MCA, respectively.

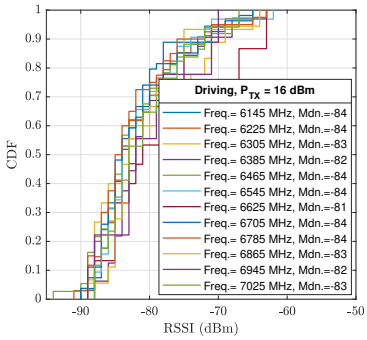
Statistical analyses of the measurements in the MCA and RA, using cumulative distribution function (CDF) plots of the measured RSSI at different transmit power levels, are shown in Fig. 5.7. Fig. 5.7a shows the CDF of driving measurements within the MCA for MC1 (S1) and MC2 (S2). While P_{TX} represents the transmit power for the AP, the maximum power of the 20 MHz beacon frames is 18 dBm for $P_{TX} \geq 18$ dBm as shown in Table 5.2. MC1 measurements showed a transmit power of 15 dBm: this changed when we returned



(a) Driving measurements.



(b) Walking measurements.



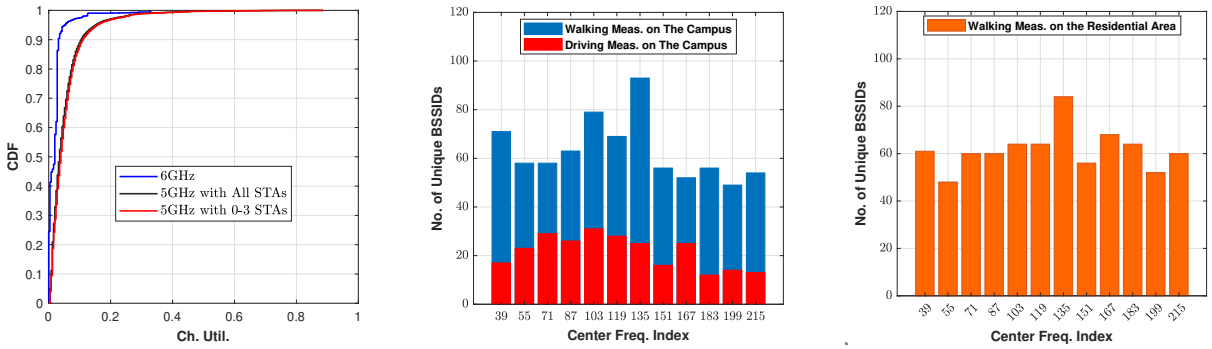
(c) RSSI for each 80 MHz channel, S2 (driving).

Figure 5.7: CDF of outdoor RSSI at UMich. S1: MCA in Jan., S2: MCA in May, S3: RA in May.

in May for MC2. The median outdoor RSSI level is -85 dBm for both S1 and S2 under $P_{TX} = 15$ dBm, while the highest median RSSI value is -81 dBm for S2 under $P_{TX} = 16$ dBm due to being the most frequently used.

Fig. 5.7b shows the CDF of outdoor RSSI levels recorded during walking measurements (only in MC2) in the MCA (S2) and the RA (S3). A single transmit power of $P_{TX} = 21$ dBm was observed in the RA deployment, which is less dense than the MCA and hence each AP can transmit at a higher power without interference. This is still 3 dB less than the maximum allowed power of 24 dBm for 80 MHz channels. Due to the proximity of the walking measurement locations to the buildings, an increase of 1-9 dBm is observed for the median RSSI values in the walking measurements compared to the driving measurements in the case of S2. Fig. 5.7c shows the results obtained for each of the 80 MHz channels with Tx power of $P_{TX} = 16$ dBm: all the channels exhibit similar behavior.

Channel utilization and number of unique BSSIDs observed outdoors help to understand the potential interference impact of a dense deployment. A higher channel utilization and larger number of unique BSSIDs on a particular frequency point to increased potential for interference on that frequency. Fig. 5.8a shows the CDFs of primary channel utilization at 5 GHz and 6 GHz for UMich SSIDs during walking measurements in the MCA. 6 GHz



(a) Primary ch. util. for S2. (b) # of unique BSSIDs at MCA. (c) # of unique BSSIDs at RA.

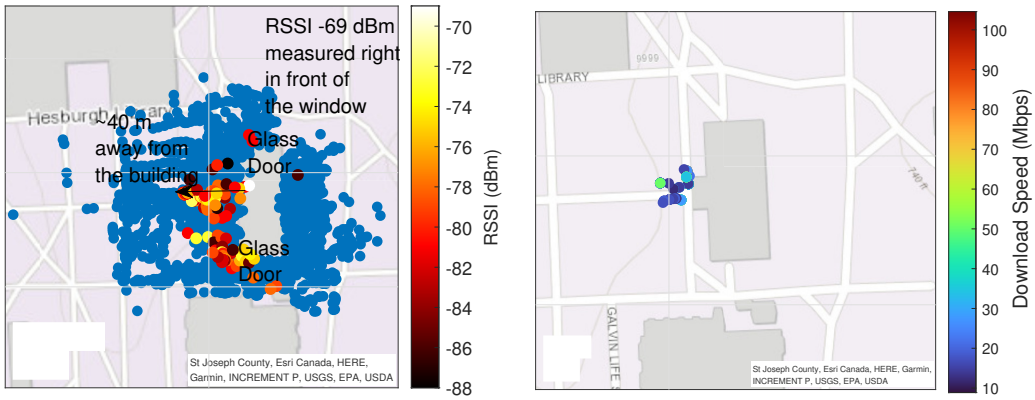
Figure 5.8: Channel utilization and # of unique BSSIDs the UMich.

usage is still sparse, and during our measurements, a maximum of 3 devices were seen connected to a single BSSID at a particular time instant. However, we observe from our 5 GHz measurements that primary channel utilization is not very dependent on number of connected devices since the main contributor to primary channel utilization is beacons and other management frames.

Figs. 5.8b and 5.8c shows the number of unique BSSIDs in each 80 MHz channel observed in the MCA and RA, demonstrating a similar pattern for the walking measurements in both areas and, as expected, a reduced number in the driving measurements in the MCA. The key takeaway from this result is that while there is a slightly higher number of unique BSSIDs observed outdoors on channel 135 in both areas, overall, all channels are used relatively uniformly, thus reducing the probability of interference to an outdoor fixed link that overlaps with a particular 80 MHz channel.

Walking Measurement Campaign at UND (MC3): Fig. 5.1c shows the outdoor RSSI range measured on 20 MHz beacon frames around the measurement building. RSSI measurements were collected by walking with hand-held phones running SigCap. The measured minimum and maximum RSSI around the building are -95 dBm and -64 dBm, respectively. The glass door and dense windows on the front of the building create a small region with high RSSI, so beacon frames were captured at a distance of 120 m from the building. On

the back of the building, however, we observed lower RSSI levels compared to the front as there are no windows on the first floor. The beacon frames were captured at a distance of up to 50 m, potentially transmitted by Wi-Fi 6E LPI APs on upper floors with windows. The distance reduces up to 32 m for the sidewalls of the building with glass doors, but no windows.

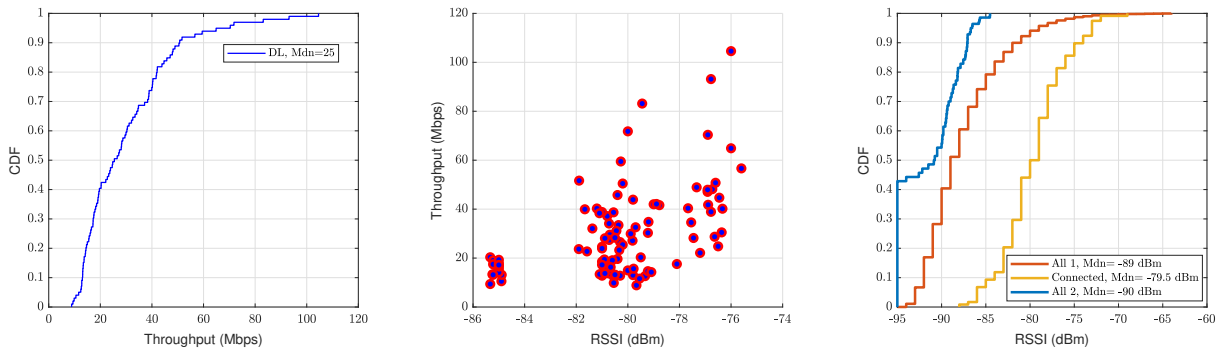


(a) 6 GHz connection outdoors. (b) 6 GHz downlink tput. outdoors.

Figure 5.9: 6 GHz connection and downlink throughput outdoors at UND.

Fig. 5.9 shows the measured outdoor RSSI and DL throughput ranges when phones outside were connected to indoors Wi-Fi 6E LPI APs. As shown in Fig. 5.9a, phones were connected to 6 GHz mostly right outside the glass doors, existing on three sides of the building. Due to sporadic connections between phones outside and LPI APs, we were able to run the speed test only at the front of the building, *i.e.*, less than a meter away as illustrated in Fig. 5.9b. To provide a detailed analysis of 6 GHz connection outdoors, Fig. 5.10a shows the CDF plot of DL throughput, while Fig. 5.10b shows the relation between the throughput and RSSI values. The observed range of DL throughput ranges from 8 Mbps to 104 Mbps with a median level of 25 Mbps. Throughput levels greater than 60 Mbps were observed at high RSSI levels, *i.e.*, -80 dBm and above. However, we were not able to run the speed test at RSSI levels less than -86 dBm. Thus, even though the phone may be connected to a AP, if the RSSI is very low, speedtests do not complete.

Statistical analyses of the campaign are shown in Fig. 5.7 via CDF plots of the mea-

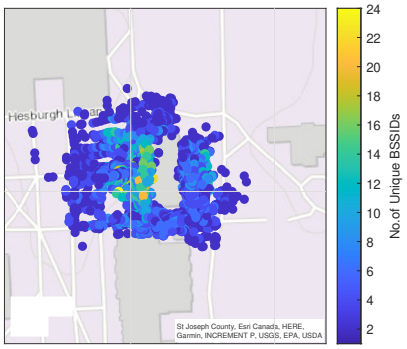


(a) CDF of downlink tput. (b) Downlink tput. vs. RSSI. (c) CDF of outdoor RSSI.

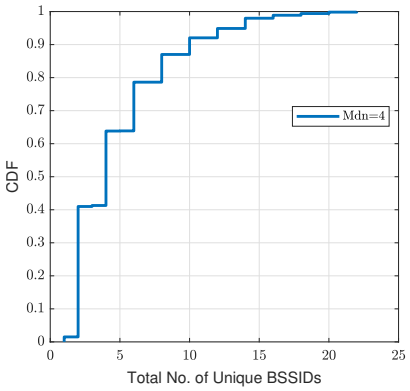
Figure 5.10: Downlink throughput and RSSI in outdoors walking measurements at UND.

sured RSSI. We observed median outdoor RSSI level of -89 dBm during walking experiments (labelled All 1). Specifically, 80 out of the 140 unique BSSIDs were observed during this outdoor measurements. To further evaluate potential interference from the Wi-Fi 6E deployment to fixed microwave links, we compute average RSSI for each BSSID observed outdoors, and assign the RSSI value of -94 dBm for the BSSIDs not detected outdoors (labelled All 2). Although median RSSI level remains similar, we observed a considerable decrease in the 90th percentile, indicating a greatly reduced potential for interference. The median RSSI level increases to -79.5 dBm when the outside phones are connected to the indoor Wi-Fi 6E APs.

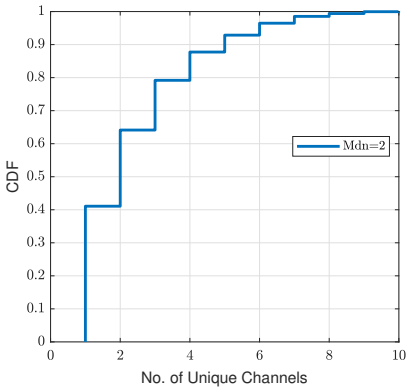
Fig. 5.11 focuses on the analysis of the number of unique BSSIDs and 80 MHz channels measured outdoors during walking measurements to provide insights into the potential interference impact of a typical Wi-Fi 6E deployment. Fig. 5.11a shows the outdoor heatmap of the number of unique BSSIDs during walking measurements. Although we observed 80 unique BSSIDs outdoors, a high number of BSSIDs were received only outside the front glass door. Figs. 5.11b and 5.11c show the CDF plot of the number of unique BSSIDs and unique 80 MHz channels measured at a specific location. Median number of BSSIDs received outdoors is 4 out of 140 deployed BSSIDs, while the number of unique channels ranges from 1 to 10 with a median value of 2. The lower number of unique BSSIDs and channels indicates



(a) Number of unique BSSIDs measured at a given location.



(b) CDF of the number of unique BSSIDs measured at a given location.



(c) CDF of the number of unique channels measured at a given location.

Figure 5.11: CDF plots for walking measurements: Number of unique BSSIDs and channels at UND.

a reduced potential for interference from Wi-Fi 6E LPI APs to existing incumbents.

C2C Enabling Level Based on Measurements at UMich and UND: In the proposed C2C mode, clients that can receive an enabling signal from any Wi-Fi 6E AP can directly communicate with each other, at STA LPI power levels, bypassing the need for data transmission through the AP. Device sharing is an example application that benefits from the C2C mode, reducing air time occupancy and latency. While the intended use of C2C is to improve indoor performance, care must be taken to set an appropriate level for the enabling signal so that client devices that are outdoors do not transmit to each other. The proposals submitted to the FCC recommended using -86 dBm/20 MHz and -82 dBm/20 MHz as enabling signal levels [60]. Based on our walking results at UMich, where the median outdoor RSSI level varies between -75 dBm and -85 dBm, even a level of -82 dBm could trigger ¿ 50% of outdoor devices to communicate with each other, which is not desirable. Furthermore, the walking measurements at UND shows a median RSSI of -79.5 dBm. Hence, further measurements and analyses should be performed to determine an appropriate enabling signal level for C2C that minimizes the probability of interference.

Drone Measurements at UMich (MC2): Driving and walking measurements obtained at ground level alone do not offer a comprehensive understanding of the interference potential in the 6 GHz band since most outdoor fixed links are deployed at higher altitudes. Hence, the drone experiments provide insights into the RSSI levels as a function of altitude.

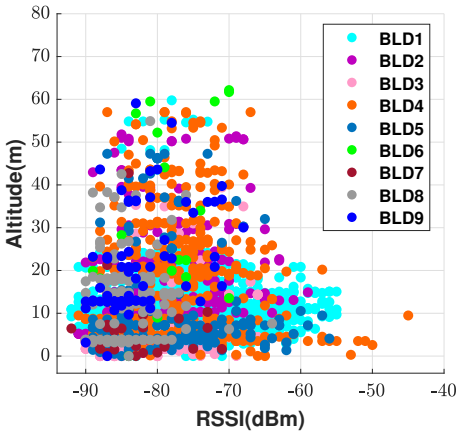
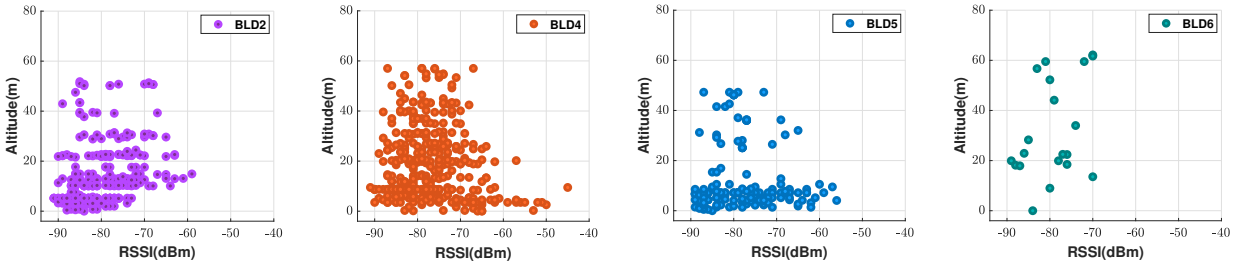


Figure 5.12: RSSI vs. altitude for drone measurements.

Fig. 5.12 summarizes the RSSI measured at different altitudes near the nine buildings listed in Table 5.4. The observed range of RSSI is between -93 dBm and -55 dBm. RSSI values greater than -60 dBm were not observed above a height of 20m. Above a height of 30m, the RSSI values are less than -68 dBm.

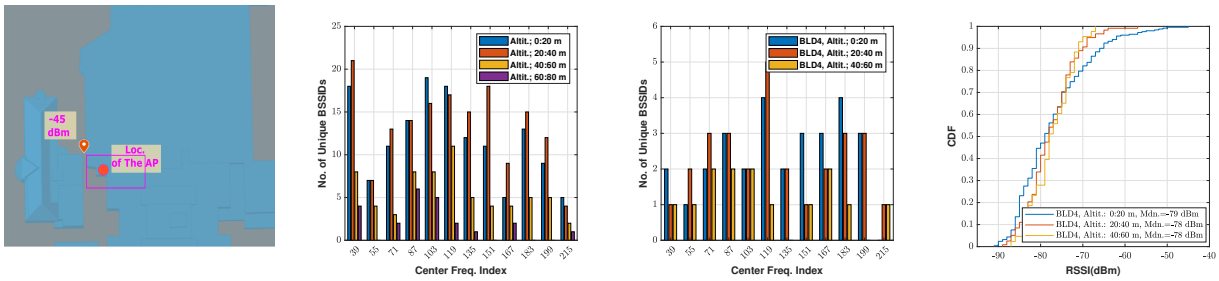


(a) $N_{BSSID} = 368$ (b) $N_{BSSID} = 800$ (c) $N_{BSSID} = 68$ (d) $N_{BSSID} = 92$

Figure 5.13: RSSI vs. altitude wrt. the number of BSSIDs at UMich.

In order to provide an in-depth analysis of the relationship between RSSI and factors such as number of Wi-Fi 6E APs, construction material, and altitude, Fig. 5.13 shows RSSI

vs. altitude for four representative buildings: BLD2, BLD4, BLD5 and BLD6 with 368, 800, 68 and 92 BSSIDs respectively, as shown in Table 5.4. BLD2 and BLD4 have many more APs compared to the other two. From Fig. 5.13a and Fig. 5.13b we see that the drone measurements near BLD2 and BLD4 provide a larger number of data samples up to 60m compared to BLD5 and BLD6 which have fewer APs. However, there is an uniform decrease in the number of samples and RSSI with increase in altitude for all 4 buildings. Despite having fewer APs than BLD6, there are more data samples observed near BLD5 with higher RSSI: this is because unlike most buildings on campus, BLD5 is a historical building with single pane windows, resulting in lower loss.

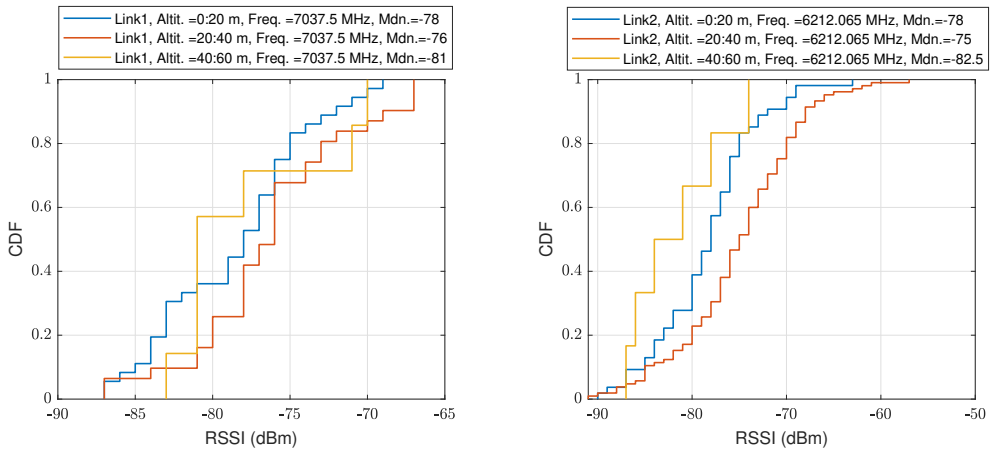


(a) -45 dBm RSSI. (b) All nine buildings. (c) BLD4. (d) CDF of RSSI.

Figure 5.14: Number of unique BSSIDs vs. altitude at UMich.

Fig. 5.13b shows a high RSSI value of -45 dBm obtained at 10m near BLD4 which we investigate further. Fig. 5.14a shows the relative location of this data sample and the corresponding BSSID/AP inside the building. The AP is in a room on the first floor and there is line-of-sight (LOS) through a corner window, resulting in the high outdoor RSSI measured at the outdoor location. It is important to note, however, that not all APs will contribute to significant signal emissions outdoors. In addition to the number of APs within a given building, the likelihood of these APs to LOS conditions through nearby windows plays a vital role in the resulting outdoor RSSI levels, and hence potential for interference. Figs. 5.14b and 5.14c illustrate the number of unique BSSIDs vs. altitude for the the nine buildings and for BLD4, respectively. Although the number of unique BSSIDs observed

within the altitude range of $0-20$ m and $20-40$ m is fairly comparable, there is a noticeable decrease in the number of unique BSSIDs as the altitude range extends to $40-60$ m and $60-80$ m, thus indicating reduced potential for interference at higher altitudes. Finally, Fig. 5.14d shows the CDF of RSSI for BLD4. While the median outdoor RSSI values remain consistent across the three altitude intervals, there is a decrease in the maximum outdoor RSSI level as the altitude increases.



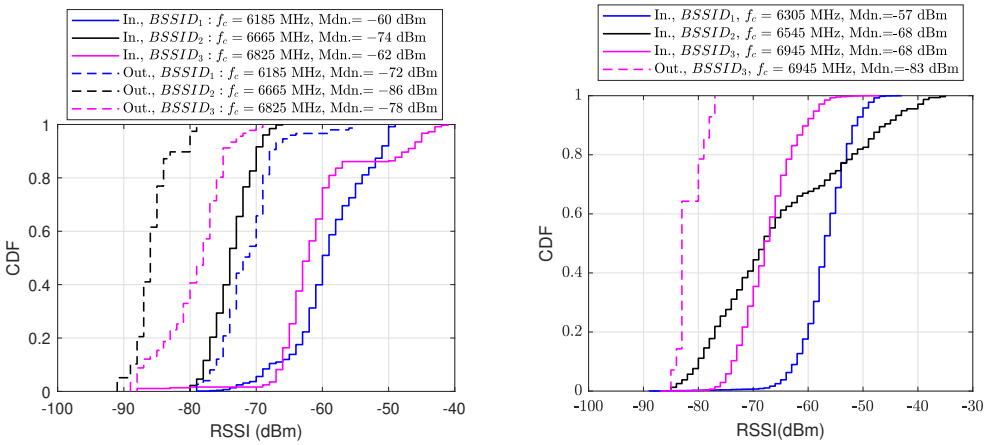
(a) Link 1: RSSI on Channel 215. (b) Link 2: RSSI on Channel 55.

Figure 5.15: CDF of drone RSSI measurements on channels overlapping Links 1 and 2 at UMich.

We evaluate the interference potential to Links 1 and 2 which overlap with Wi-Fi channels 215 and 55 respectively (Link 2 has < 1 MHz overlap with the edge of channel 39 which we ignore since the Wi-Fi signal drops off at the band-edge). Fig. 5.15 shows the CDF of the RSSI on these channels at different altitudes. As the altitude increases, RSSI level decreases, thus reducing the interference potential to these links. To further evaluate the interference level, we calculate approximately the ratio of interference to noise power (I/N) for these links as $I/N = 10\log_{10}(BW_i/20) + RSSI_{Outdoor} + G_{rx} - NF - PL$, where BW_i is the link bandwidth, G_{rx} is the Rx antenna gain, NF is the noise floor and PL is the free space path loss. These are computed from the link parameters in [42, 41]. We assume worst case conditions: highest outdoor RSSI measured of -68 dBm and -58 dBm for Links 1 and

2 respectively, in the main Rx beam. I/N is calculated to be -72 dB for Link 1 and -66 dB for Link 2, much lower than the harmful interference threshold of $I/N = -6$ dB. Although Rx4 is located in the MCA, the link points away from the densely deployed region and thus we did not calculate the interference level at Rx4.

Indoor-Outdoor BEL Measurements at UMich (MC1 & MC2): At UMich, we collected indoor-outdoor BEL measurements at two locations as described below.



(a) FL1: Double-pane low-E window. (b) FL2: Solid brick wall.

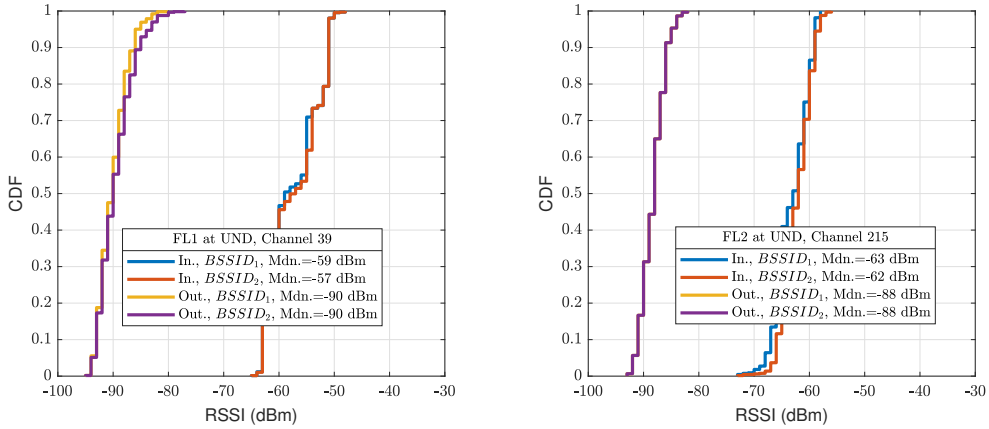
Figure 5.16: BEL for fixed locations at UMich.

BEL near a double-pane low-E Window (FL1): Fig.5.16a shows the CDF of indoor and outdoor RSSI values for the fixed location FL1 which is the open area shown in Fig. 5.2. We only consider RSSI measurements where the client devices are connected to the BSSID associated with the AP in the room, which is one of the few APs with three BSSIDs. A 12 dB BEL is observed for BSSID_1 and BSSID_2, while BSSID_3 exhibits a higher entry loss of 16 dB.

BEL near a solid brick wall (FL2): Fig. 5.16b shows the results obtained for the FL2 shown in Fig. 5.4. Inside the measurements room, the devices were able to connect to $BSSID_1$ and $BSSID_2$. However, these two BSSIDs were not detected outside due to the solid brick wall. $BSSID_3$ was observed outside since it is associated with the AP located

in the adjacent room, which has a window pointing out towards the outdoor measurement location. Moreover, 391 APs, corresponding to 782 BSSIDs, are deployed in the entire building of which only 159 BSSIDs are observed within the measurement room, and only 8 of these i.e., 5%, are observed outside in this location, indicating a very high loss through the brick wall.

Indoor-Outdoor BEL Measurements at UND (MC3): Fig. 5.17 illustrates the results for BEL near a solid brick wall in two different environments. Figs. 5.17a and 5.17b show the CDF of RSSI for two BSSIDs of the APs in FL1 and FL2, respectively. In FL1, we observed BEL ranging from 30 dB to 35 dB, while the BEL in FL is around 25 dB. We observed higher BEL in FL1 due to distance between indoor measurement location and the exterior wall.



(a) FL3: Solid brick wall. (b) FL4: Solid brick wall.

Figure 5.17: BEL for fixed locations at UND.

5.3 Summary and List of Accomplishments

This chapter demonstrates a significant advancement in our device-based measurement approach, specifically focusing on the API-based tool, SigCap. By utilizing SigCap, we conducted extensive measurement campaigns across two university campuses–the first studies

of this scale. Our findings provide compelling evidence of negligible interference from LPI APs. We observed outdoor RSSI values on driving and walking ranging from -64 to -95 dBm (median -89 dBm), indicating substantial signal attenuation primarily due to double-pane low-emission windows (12-16 dB loss) and solid brick walls (25-33 dB loss). Focusing on the walking measurements, we observe a median of -82 dBm and -79.5 dBm at UMich and UND, respectively. These median values are equal or higher than the two proposed C2C activation threshold of -86 dBm and -82 dBm, which may result in a high number of undesired C2C activation by outdoor Wi-Fi clients. The outdoor RSSI median is further increased to -78 dBm as we go higher where the fixed point-to-point links are located. But even with the highest RSSI of -45 dBm (representing the worst case of interference), we calculated the interference to noise ratio of -72 dB and -66 dB for two separate links, a value much lower than the harmful interference threshold of -6 dB. Furthermore, the mere 5% detectability of indoor BSSIDs outdoors underscores the negligible effect of LPI deployments to incumbents.

The following papers has been published in the topic of Wi-Fi 6E (6 GHz) deployments studies:

- Seda Dogan-Tusha et al. "Evaluating The Interference Potential in 6 GHz: An Extensive Measurement Campaign of A Dense Indoor Wi-Fi 6E Network". In: *17th ACM Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization (WiNTECH '23)*. 2023, pp. 56–63.

- Seda Dogan-Tusha et al. "Indoor and Outdoor Measurement Campaign for Unlicensed 6 GHz Operation with Wi-Fi 6E". In: *26th IEEE International Symposium on Wireless Personal Multimedia Communications (WPMC)*. 2023, pp. 1-6.

We also published a comment to the FCC's Ex Parte regarding our findings of the outdoor signal level from the LPI APs [52], and a comment to FCC's Further Notice of Proposed Rulemaking (FNPRM) regarding the appropriate signal levels for C2C mode in the 6 GHz spectrum [54].

CHAPTER 6

SURVEY AND ANALYSIS OF 5G DEPLOYMENTS

6.1 Overview and Related Works

In 2019, cellular operators has begun to acquire new spectrum while rapidly deploying 5G network all over the US. Among the three largest US operators, Verizon was notably acquired and deployed 5G mmWave (>20 GHz) in a rapid pace, while AT&T followed behind. The mmWave spectrum itself has been a subject of academic research for a number of years, most existing literature discusses the feasibility [121], design [63], and deployment challenges [82]. There are a number of contributions that perform theoretical studies, modeling and simulations on beam management [56, 9, 16] and beam selection algorithm [67, 123, 47]. On the 5G mid-band, T-Mobile has rapidly acquired and deployed the n41 band (2.496–2.690 GHz) [25], while AT&T and Verizon deployed in the newly released C-Band spectrum (3.7–4.2 GHz) [10, 111]. Simultaneously, VZW also uses the CBRS band (3.55–3.7 GHz) in its 4G network, using both Tier 2 Priority Access License (PAL) and Tier 3 General Authorized Access (GAA) modes [49]. Furthermore, ATT and VZW have further extended their 4G networks to the unlicensed 5 GHz spectrum through LAA [104]. Prior real-world deployment studies of commercial 5G did not delve into the fundamental reasons for performance enhancement or contrast the improvements to its 4G counterpart [18, 48, 77, 55]. Therefore, we focused our work on analyzing and quantifying the performance of these 5G deployments, while also comparing its improvements over the older 4G deployments.

6.2 A Comparison Study of Cellular Deployments in Chicago and Miami

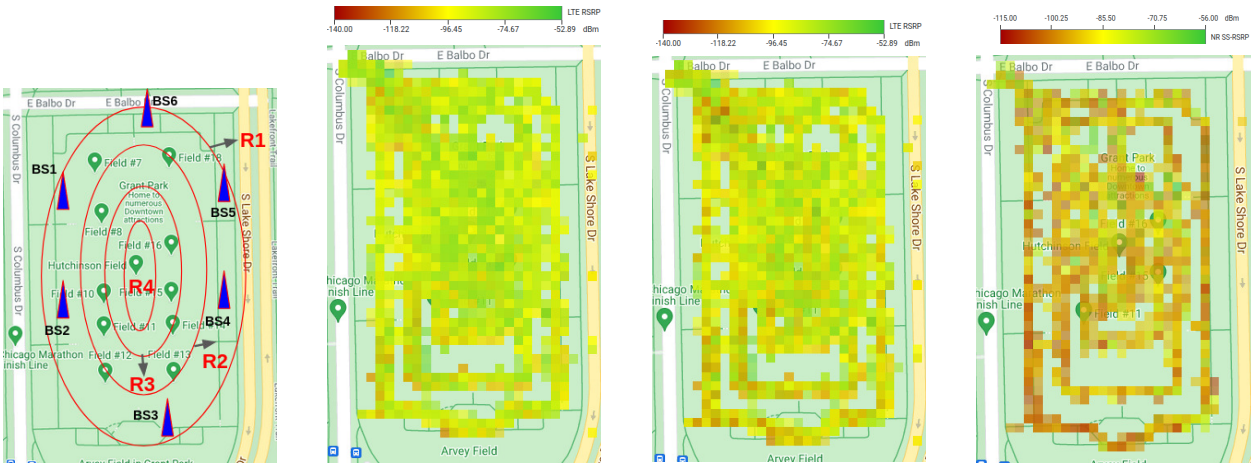
In this work [95], we present detailed comparisons of the three major cellular operators (*i.e.*, AT&T, T-Mobile, Verizon) in Hutchinson Field, an outdoor park area where there are dense cellular deployments in all the major bands and technologies described above to service the dense crowds that are common in the summer months when popular outdoor events are hosted. We also present an in-depth study of 5G mmWave performance in Miami, focusing on quantifying the performance of 5G mmWave as a function of body blockage, distance, and the number of devices connected to the base station. Table 6.1 shows the various technologies and frequency bands deployed: each operator has chosen a different mix of technologies and spectrum to deliver enhanced broadband speeds.

Table 6.1: Operator Deployment in Hutchinson Field, Chicago, and Downtown Miami (TDD bands in bold).

Operator	**Deployment**	**5G Freq.**	**5G Op. Bands**	**4G Op. Bands (LAA:46,CBRS:48)**
Verizon	4G+LAA & CBRS, 5G	Low, High	n5, **n260**	2, 4, 5, 13, **46**, **48**, 66
T-Mobile	4G, 5G	Low, Mid	**n41**, n71	2, 4, 7, 12, 66
AT&T	4G+LAA	Low	n5	2, 4, 12, 14, 30, 46, 66
Verizon (Miami)	4G+LAA, 5G	High	**n261**	2, 4, 13, **46**, 66

Table 6.2: Devices used for 4G and 5G Measurements

Location	**Mobile Device**	**Network Support**
Chicago	2 × Google Pixel 2	4G Licensed Only
	2 × Google Pixel 3	4G Lic., LAA, CBRS
	3 × Google Pixel 5	4G Lic., LAA, CBRS, 5G
Miami	2 × Google Pixel 5	4G Lic., LAA, CBRS, 5G



(a) Experiment Location (b) 4G Licensed (c) 4G Lic., LAA and CBRS (d) 5G FR1 and FR2

Figure 6.1: Hutchinson Field Overview: Verizon, T-Mobile and AT&T 4G, 4G+LAA/CBRS, and 5G Coverage

6.2.1 Data collection methodology

4G and 5G measurements were collected over several months from the morning to the evening in 2020 and 2021 in various locations in Chicago and Miami, with the intent to (i) compare the performance of the three major carriers with the greatest diversity of deployment options, and (ii) perform an in-depth study of mmWave performance. Thus, we present results from one location, Hutchinson Field, in Chicago for the former and one location in downtown Miami for the latter. In this work, we further improve our device-based measurement methodology to gather detailed network information. Table 6.2 shows all devices that used in the measurements. The devices are equipped with three Android applications, each of which supply varying degrees of information: SigCap, FCC Speed Test, and Network Signal Guru.

SigCap and its improvements. Similar to the previous methodology, SigCap is used to passively collect 4G and 5G cellular data from the device every 10 seconds. A new 5G cellular handler is implemented to collect 5G data from device's Android API (as shown on Table A.3). However, the state of the art smartphones at the time (*e.g.*, Google Pixel 5,

Samsung S21 Ultra) did not correctly implement the API, leading to missing signal strength (*e.g.*, RSRP, RSRQ) and cell identity (*e.g.*, PCI, frequency) information. To solve this, we also implement a workaround that captures partial signal information and additional NR state information as shown on Table A.4. This allows us to at least decode SS-RSRP, SS-RSRQ, and whether the 5G channel is mmWave or not, but without detailed cell identity information. Using the above data, we generate heat maps of 4G and 5G RSRP as shown in Fig. 6.1b, 6.1c, and 6.1d, by defining 10 m square grids and averaging the collected RSRP of the deployment we are interested in (4G Licensed, LAA, CBRS, 5G FR1, and 5G FR2) over the grid.

FCC Speedtest (FCC ST) [45] measures uplink/downlink throughput, and round trip latency to the speed test server with the lowest latency. Our measurements went through two servers in Chicago and one server in Miami. We confirmed that both servers in Chicago exhibited similar performance. The throughput and latency numbers reported by the app are end-to-end and include losses introduced by the back-haul.

While the FCC ST app does measure uplink throughput, we only focus on downlink measurement. On each downlink and latency test, the app records signal conditions at the beginning and the end of the test similar to SigCap (our testing confirms that the collected signal data is similar to SigCap, since the same Android APIs are used by both). However, the information captured are limited (*e.g.*, only the primary 4G and 5G channel are recorded). Furthermore, FCC ST cannot be run more frequently than once every minute whereas SigCap can collect data every 10 secs and hence allows us to create maps with greater temporal and spatial detail. However, the data collected by both apps can be easily exported for analysis.

Network Signal Guru (NSG). Similar to the prior works, NSG is used in this work to provide extensive information on 4G and 5G, such as frequency, bandwidth, numerology,

duplex mode, throughput on several network layers, beam index, SINR, block error rate (BLER), modulation, and the number of allocated RBs, but requires root access, unlike SigCap and FCC ST. Also similarly, we use NSG to study a few cases in detail and use SigCap and FCC ST for heatmaps and statistical analyses.

6.2.2 Measurements in Chicago

Methodology and Overview Hutchinson Field is part of a large urban park called Grant Park in Chicago, which is often used in large outdoor events (*e.g.*, live concert). The area, spanning approximately 0.1 km^2, is shown in Fig. 6.1a. There are dense deployments of Verizon's 4G Licensed, LAA, CBRS, and 5G as shown in Table 6.1, with fewer deployments by T-Mobile and AT&T. As needed, each device is equipped with AT&T, T-Mobile, or Verizon SIMs with unlimited data plans[1]. Data was collected by walking with the devices in the four different regions, with different radii, as shown in Fig. 6.1a: Outer Region Round 1 (R1), Inner Region Round 2 (R2), Inner Region Round 3 (R3) and Inner Region Round 4 (R4).

We present only the latest data collected during May and June, 2021, during the afternoon hours with few people (around 20) in the park. In total, we collected 8,353 SigCap data points. Specifically, there are 44,683 4G, 22,620 LAA/CBRS, and 3,097 5G data points in the measurement set. In addition, we collected 1,333 FCC ST measurements (708 4G, 386 5G and 239 mixed, where the technology changed during the test), with each containing uplink/downlink throughput and latency results. Fig. 6.1b, 6.1c, and 6.1d shows coverage maps of 4G, 4G+LAA/CBRS, and 5G in the park, respectively, from the SigCap measurements.

Summary of 4G and 5G deployment in the Hutchinson Field. Table 6.1 shows that

1. Our subscribed Verizon plan stated that there is a throttling after 50 GBytes for 4G data, and no throttling for 5G data. For AT&T, there is a throttling after 100 GBytes to 4G and 5G data. For T-Mobile, 50 GBytes for 4G and 5G data. In our experiments, we used multiple SIMs to avoid data cap throttling.

all of the operators that we studied have extensive deployments of 4G in low-band (Bands 5,12,13,14) and mid-band (Bands 2,3,4,7,30,46,48,66). We found no AT&T and T-Mobile BSs deployed inside Hutchinson Field; their 4G bands are mostly deployed on macro-cells located in the greater Grant Park area. Only Verizon has deployed 4G and 5G within Hutchinson Field: three CBRS (Band 48) channels in 3.56, 3.58, and 3.6 GHz, using General Authorized Access (GAA) [128]; and LAA (Band 46) channels on two sets of Wi-Fi-equivalent channels: {36, 40, 44} in U-NII-1 and {157, 161, 165} in U-NII-3. AT&T has also deployed LAA on two sets of channels: {149, 153, 157} and {157, 161, 165} in U-NII-3. Both LAA and CBRS were mostly aggregated in groups of three 20 MHz channels with a total bandwidth of 60 MHz, excluding to the primary licensed carrier.

We identified six lampposts inside the field that are used as Verizon's mmWave BSs (blue triangles in Fig. 6.1a) using the Ericsson radio. There is no AT&T and T-Mobile 5G deployments inside the field; all 5G BSs are deployed outside the field. The average distance between the Verizon mmWave BSs is 140 m (460 ft). Each mmWave antenna panel has a separate PCI with multiple beam indices. Verizon and AT&T have deployed 5G in NSA mode only, while T-Mobile uses both SA and NSA mode. We "forced" the SA mode connection by using NSG to block all connections beside 5G.

As its 5G spectrum, T-Mobile and Verizon used the low-band n71 and n5, respectively, with the maximum 20 MHz bandwidth, while AT&T's 5G deployment used n5 but with only 5 MHz. These bandwidths are lower than the possible 40 to 100 MHz in mid-band. Additionally, due to the limitation of the Pixel 5 being able to aggregate only one 5G channel in FR1, the low-band 5G performance is worse than the mid-band 4G at the present time, since 4G has up to four CA.

On the other hand, T-Mobile and Verizon have deployed 5G on mid-band and mmWave, respectively[2]. T-Mobile's mid-band deployment is in Band n41 using 20 and 80 MHz band-

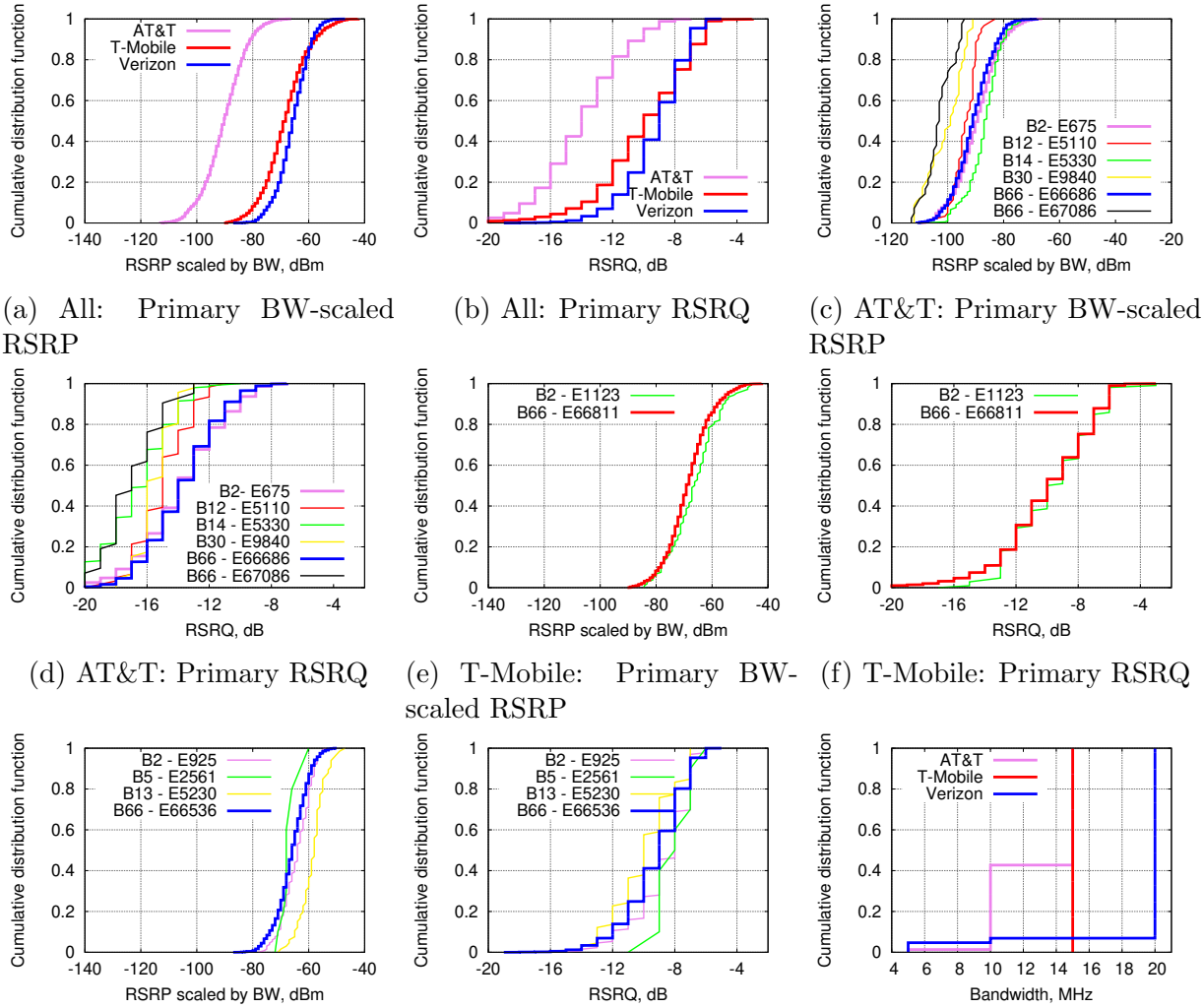
2. We measured AT&T 5G mmWave in other areas of downtown Chicago but not in Hutchinson Field as of June 2021.

widths. However, the Pixel 5's limitation of only one secondary 5G carrier in FR1 still applies, leading to a diminished performance compared to 4G at the present time. On the other hand, Verizon has deployed mmWave 5G densely in n260 (39 GHz) using at most four carriers, each 100 MHz wide. The higher bandwidths and number of channels being aggregated leads to a vastly improved throughput compared to mid-band 5G. Using NSG, we observed that Verizon aggregates mmWave channels only if they were transmitted from the same mmWave panel, *i.e.*, they have the same PCI.

Statistical Analysis of RSRP and RSRQ. We use RSRP and RSRQ values for all primary and other channels from SigCap to create cumulative distribution function (CDF) plots for each operator. Fig. 6.2a, 6.2c, 6.2e, and 6.2g show the CDF of primary channel RSRP scaled by bandwidth, as an indicator of coverage and throughput performance. The bandwidth scaling is calculated as $RSRP_{dBm} + 10 * log_{10}(BW_{MHz})$. We only present the primary channel bandwidth since the API has no reliable information on the total aggregated bandwidth.

Fig. 6.2a shows that the BW-scaled RSRP of T-Mobile and Verizon are comparable, while AT&T's is around 20 dB lower. Similarly, Fig. 6.2b shows a higher RSRQ for T-Mobile and Verizon, with AT&T around 4 dB lower. These CDFs indicate that the 4G performance of T-Mobile and Verizon is better than AT&T's, which is borne out by throughput analysis presented in the performance analysis section.

Sorted by Band (B) and EARFCN (E), we focus on the occurrence of the Bands on our measurements: (1) AT&T uses 5 LTE Bands (2, 12, 14, 30, 66) as its primary channel, with highest occurrence of B2 (E675, 57% of data) and B66 (E66686, 33% of data); (2) T-Mobile uses two primary channel Bands (2, 66), with B66 (E66811, 92% of data) as the majority, and; (3) Verizon uses four primary channel Bands (2, 5, 13, 66), with B66 (E66536, 93% of data) as the majority. Of all operators, the primary channel is selected by optimizing RSRP and RSRQ, as shown on Fig. 6.2c-6.2h where the primary channel with



(a) All: Primary BW-scaled RSRP

(b) All: Primary RSRQ

(c) AT&T: Primary BW-scaled RSRP

(d) AT&T: Primary RSRQ

(e) T-Mobile: Primary BW-scaled RSRP

(f) T-Mobile: Primary RSRQ

(g) Verizon: Primary BW-scaled RSRP

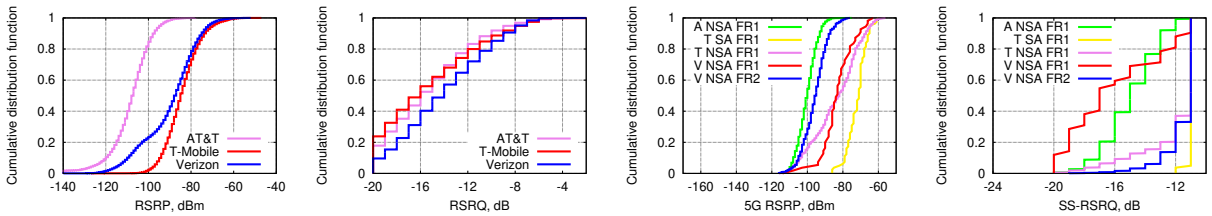
(h) Verizon: Primary RSRQ

(i) All: Primary BW

Figure 6.2: AT&T, T-Mobile, and Verizon in Hutchinson Field: CDF of Primary Channel RSRP, RSRQ, and Bandwidth

most occurrence (highlighted as a bold line) has the best BW-scaled RSRP and RSRQ. However, we observed a slight exception on Verizon: B13 has a better BW-scaled RSRP but worse RSRQ compared the most occurred B66, thus B66 is arguably the best choice of primary channel in our measurements.

Fig. 6.2i shows the CDF of the primary channel bandwidth. Verizon has the highest available bandwidth for its primary channel, followed by T-Mobile and AT&T. Note that the primary channel bandwidth, RSRP, and RSRQ may not be a good indicator for throughput



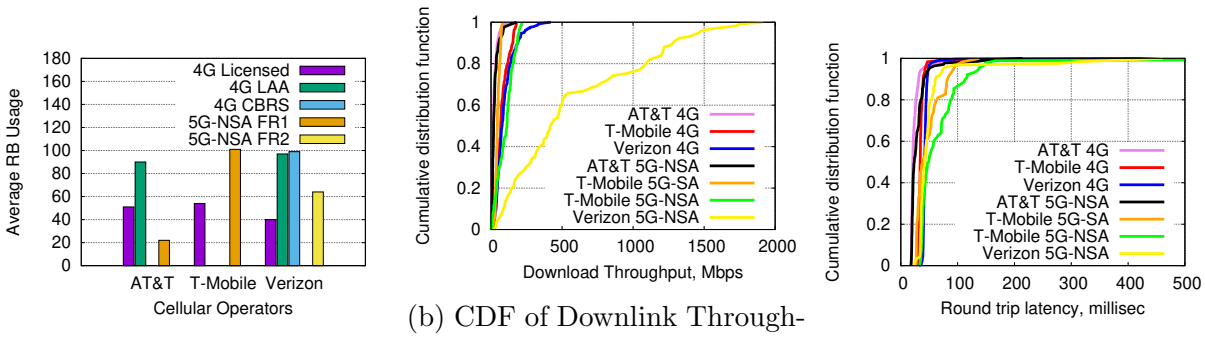
(a) All 4G Channels' RSRP (b) All 4G Channels' RSRQ (c) 5G RSRP (d) 5G RSRQ

Figure 6.3: AT&T (A), T-Mobile (T), and Verizon (V) in Hutchinson Field: CDF of 4G and 5G RSRP, RSRQ

performance due to carrier aggregation, but does provide insight into the deployment quality: the higher the primary bandwidth and RSRP, the more likely that the operator will have good coverage and throughput. This is corroborated by the throughput analysis in the next subsection.

Fig. 6.3a and 6.3b show the CDF of RSRP and RSRQ for all 4G Licensed carriers (*i.e.*, primary, secondary, neighboring) in Hutchinson Field. Based on this, T-Mobile has the best 4G licensed coverage, followed closely by Verizon and AT&T. The RSRQ CDF shows Verizon has a better overall channel quality compared to T-Mobile. On the other hand, AT&T's RSRP and RSRQ values indicate inferior coverage, which is probably due to the fact that the cells are mostly deployed outside Hutchinson Field.

Fig. 6.3c and 6.3d show the 5G-RSRP and 5G-RSRQ CDF of 5G when the device is connected to 5G. We do not scale the 5G-RSRP with bandwidth since the app does not provide this information for each data record. There are four observations we conclude from comparing the CDF of 5G-RSRP and 5G-RSRP: (1) Overall, the 5G-RSRP of the FR1 bands is higher than FR2 due to the difference in operating frequency and the resultant propagation. (2) The 5G-RSRP of T-Mobile NSA FR1 deviates from the Gaussian distribution since the values are combined from the low-band (n71) and mid-band (n41), (3) T-Mobile only connects to the low-band n71 in SA mode, thus its 5G-RSRP is higher. (4) AT&T shows a very low 5G-RSRP and 5G-RSRQ in FR1, indicating inferior 5G coverage.



(a) RB Usage

(b) CDF of Downlink Throughput

(c) CDF of Round Trip Latency

Figure 6.4: AT&T, T-Mobile, and Verizon in Hutchinson Field: RB Usage, Downlink Throughput, and Latency

Verizon 5G FR1 occurs the least over all categories, with a lower 5G-RSRP and 5G-RSRQ values. When the device was blocked from connecting to 5G mmWave (using NSG's root access), the device would connect more often to 4G+LAA/CBRS rather than mid-band 5G, perhaps because the former configuration provided higher throughput. While LAA and CBRS information was collected, we do not include them in the comparisons since there is a substantial difference in transmit power compared to the licensed channels: the U-NII-3 spectrum used by LAA only allows a maximum of 30 dBm transmit power, while CBRS allows a maximum of 47 dBm in outdoor deployments.

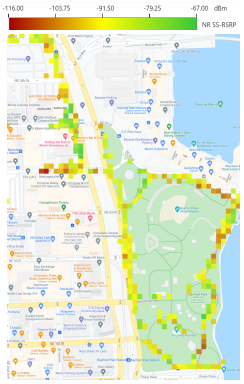
From NSG, we show the average RB allocation per device as an indicator of network load in Fig. 6.4a. There are slightly fewer RBs allocated on Verizon's licensed carrier compared to the other operators, indicating a higher load or higher resource allocations on the secondary LAA/CBRS/5G carriers. However, the difference is insignificant, and we can conclude that the network load is similar for all operators during the measurements.

Downlink Throughput and Latency Performance, using FCC ST. The data was sorted based on the cellular technology reported by FCC ST and we removed data where the technology switched between 4G and 5G during the test. Fig. 6.4b shows the downlink throughput CDF of AT&T, T-Mobile, and Verizon in 4G and 5G. The average download throughput recorded in the Hutchinson Field region for all operators are as follows: (i)

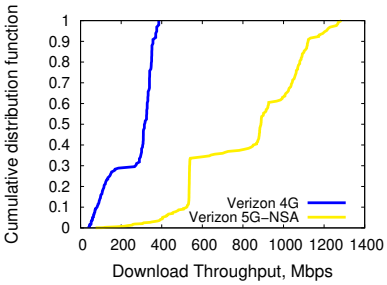
AT&T: 20.7 Mbps and 27.1 Mbps in 4G and 5G-NSA, respectively; (ii) T-Mobile: 77.2 Mbps, 46.2 Mbps, and 101.3 Mbps in 4G, 5G-SA, and 5G-NSA, respectively and (iii) Verizon: 95.8 Mbps and 574.4 Mbps in 4G and 5G-NSA, respectively. Verizon achieved the best throughput performance in 4G and 5G, due to its usage of CBRS/LAA and mmWave, respectively. AT&T had the worst 4G and 5G throughput in Hutchinson Field due to low coverage and low bandwidth (5 MHz) of Band n5. Both Verizon and T-Mobile achieved a very similar performance in 4G, which correlates to the similarity of their 4G RSRP, RSRQ, and primary bandwidth distribution. However, Verizon delivered a maximum 4G throughput of 421 Mbps due to LAA/CBRS usage: better than the highest 5G throughput in FR1 of 219 Mbps, achieved by T-Mobile 5G-NSA. Due to device limitations, only a maximum of one 5G FR1 carrier can be aggregated. Thus, there can be a diminished throughput increase when the device is switched from 4G to 5G FR1. This is demonstrated clearly by the low throughput values of T-Mobile 5G-SA which is limited by the single 5G channel usage.

Fig. 6.4c shows the CDF of the round trip idle latency of the three operators over 4G and 5G. The median values are: 30.5 ms and 30.7 for AT&T 4G and 5G-NSA, respectively; 44.1 ms, 48.4 ms, and 74.8 ms for T-Mobile 4G, 5G-SA and 5G-NSA, respectively; 44.1 ms and 54.4 ms for Verizon 4G and 5G-NSA, respectively. Generally, the latency performance is poorer in 5G-NSA compared to 4G. This may be due to non-optimal deployment of 5G-NSA [78, 125], causing additional overheads due to dual connectivity. It should be noted that the latency measurement is end-to-end, however, since all the latency tests were conducted via the same two servers, the effects of back-haul on the latency are the same for all the operators. We did not notice any significant difference in throughput and latency between tests conducted over the two servers.

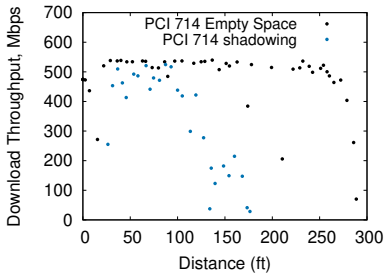
It is clear that 5G mmWave provides a significantly improved throughput performance, but the latency performance could be improved. In spite of the directional nature of mmWave transmissions, the dense deployment of 6 BSs over 0.1 km^2, with average distance of 140 m



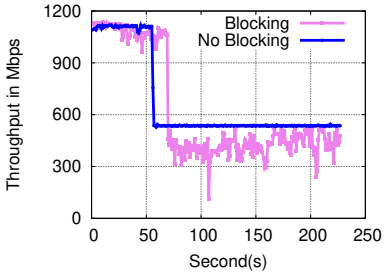
(a) 5G Coverage map in Miami downtown



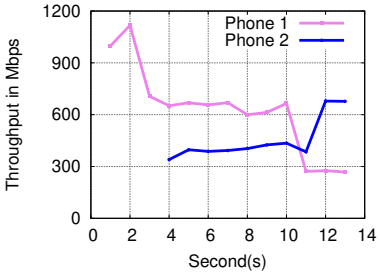
(b) Throughput of 4G+LAA Vs 5G



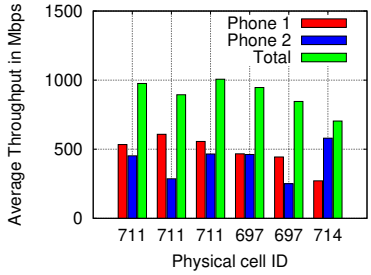
(c) Impact of distance and shadowing



(d) Impact of human body blocking



(e) Throughput between 2 phones



(f) 2 phones throughput on multiple PCI

Figure 6.5: mmWave Deployment at Miami, Florida

between BSs provides very good 5G mmWave coverage in Hutchinson Field. However, the directional nature also results in a higher variance of 5G mmWave throughput as seen in Fig. 6.4b. Hence, in the next section, we focus on a single Verizon 5G mmWave BS to better quantify mmWave performance as a function of distance, body loss, and number of clients.

6.2.3 Measurements in Miami

We utilized two Pixel 5 phones as summarized in Table 6.2. We measured the Verizon network while walking in the park and city streets within the downtown area shown in Fig. 6.5a. The measurements were done between January and June 2021. Verizon has a diverse deployment in downtown Miami with a mix of 4G, 4G+LAA, and 5G mmWave, as was previously summarized in Table 6.1. Unlike Hutchinson Field in Chicago where CBRS has been widely

deployed, CBRS was not detected in Miami[3]. The Verizon mmWave operating band is n261 (28 GHz) unlike Chicago where it was n260 (39 GHz) with a bandwidth of 400 MHz (aggregated over four carries, each 100 MHz).

First, Fig. 6.5a shows the *coverage map* of 5G deployment in downtown Miami, we focus on 7 locations labelled M1-7. 4G+LAA is also widely deployed in the same area. Fig. 6.5b the throughput distribution of 5G compared to 4G+LAA on all locations. The 5G throughput gain is in the range of 4× to 14×, compared to 4G. Also, we observe a similar 5G throughput distribution between Miami and Hutchinson Field. However, 4G throughput at Miami is higher due to high occurrence of LAA aggregation. Second, Fig. 6.5c shows the impact of **distance** on the 5G mmWave coverage. As shown, the maximum throughput is achieved up to 250 feet before it dramatically drops down at 300 ft. Furthermore, having trees (*i.e.*, shadowing effect) reduces the coverage range down to 125 ft (*i.e.*, 50% drop in coverage). Third, Fig. 6.5d depicts the impact of *human body blocking*, in which 2 different trials were conducted. One trial had the user's body blocking the phone, while the other did not. The trials were conducted at a fixed distance to the tower with no other obstructions, both phones were connected to the same PCI 714, and the same beam number throughout the trial. We observe a lower throughput and a higher variance on the blocked phone. The average degradation due to human body blockage is about 20%.

Finally, Fig. 6.5e shows the impact of having *two simultaneously* served phones. In this experiment, we use two Google Pixel 5 phones. The two phones were held within arms-length of one another near a cell tower, and phone-2 starts four seconds after phone-1. Fig. 6.5e depicts the throughput achieved by each of the two phones over time. As shown, phone-1 starts with a high throughput, indicating that all RBs are allocated to phone-1. Once phone-2 starts, the throughput of phone-1 drops given that the total resource blocks are now shared between the two phones. Such an experiment was repeated multiple times,

3. According to the FCC database, Verizon has 30 MHz PAL license in the Miami-Dade county area. However, we did not observe CBRS deployment at the time of measurements.

and Fig. 6.5f shows the outcome of 6 such trials over different PCIs. In most cases, the throughput values of both phones are comparable.

6.3 Analysis of 5G mmWave Deployments and Beam Management in Chicago

In this work [76], we focus on another facet of a 5G mmWave deployment: beam management in terms of coverage, selection, and propagation. Our analysis of beam management in commercial deployments will answer research questions that most of the analysis and theoretical modeling in the literature do not adequately answer: what should the practical inter-distance between two mmWave BSs be, what role does path loss play in beam selection mechanism, what is the trade-off between number of Tx and Rx beams, do more antennas imply higher throughput, do more beams lead to more inter/intra-beam handover or latency?

As of the time of the measurement (June 2021), two 5G operators have densely deployed mmWave-based 5G service (in non-standalone/NSA mode) in the area: OpX (**Verizon**) and OpY (**AT&T**). We chose two regions in the Chicago Loop that represents Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS) deployments: (1) BP– the Upper Hutchinson Field **B**aseball **P**ark (*near E Balbo Dr & S Columbus Dr*) representing an open field space, and (2) DT– **D**own**T**own Chicago (*W Adams Blvd & S Lasalle St to W Jackson Blvd & S State St*) representing an urban canyon surrounded by tall buildings on both sides of the road with high pedestrian and vehicular traffic.

6.3.1 Data collection methodology

To ensure that the end user's smartphone device does not become a bottleneck in supporting such high bandwidth, we use 3× state-of-the-art Samsung Galaxy S21 Ultra 5G (S21) smartphones as (SM-G998U1) the user equipment (UE). This model is equipped with the

Table 6.3: Fields captured in the dataset.

Field	**Description**
Latitude, Longitude	UE's geographic coordinates and estimated accuracy from the Android API
PCell PCI	Primary cell PCI for LTE/NR cell
SCell[x] PCI	Secondary cell PCI for LTE/NR cell [$x = 1 \sim 7$]
RSRP/RSRQ*	Signal strength values for LTE and NR PCell/SCell
Pathloss	Path Loss b/w Tx and Rx for NR PCell/SCell
UL, DL NR-ARFCN	Absolute radio-frequency channel number used in uplink and downlink for NR PCell/SCell
PDSCH/PUSCH Throughput	UL/DL physical throughput for LTE and NR PCell/SCell
Beam SSB Idx*	SSB (Secondary Synchronization Block) Tx/Rx beam index for NR Cell
Best Beam Idx	Tx beam index of dominant beam (highest RSRP) on serving cell
Best Beam State	Status of whether serving beam has the best RSRP over all possible beams (serving + neighbor)
Beam Switch Delay	Delay time when switching between beams on the same or different PCI

** these fields are also captured for neighbor (non-serving) cells and per beam for mmWave NR*

Qualcomm Snapdragon 888 (SM8350) chipset with X60 modem [116] to handle 5G in the low, mid, and mmWave bands. On the mmWave bands, it is capable of receiving up to 8 Tx beams using 2 Rx beams, utilizing up to 8 $\times$ 100 MHz wide channels.

Root-based tool: Accuver XCAL. Accessing lower-layer information requires access to Qualcomm *Diag* (or the diagnostic interface), which needs special licenses and tools. We therefore rely on a professional tool called *Accuver XCAL* [8] which has access to Qualcomm Diag. Similar to NSG, this tool provides access to *PHY*, *MAC*, *RRC* layer messages by accessing the control plane messages and chipset logs using root privilege, which in turn provides insights on the beam management aspects. XCAL provides an easier data extraction compared to NSG. However, the phones still need to be tethered to a laptop to enable the tool, with up to 4 smartphones connected concurrently. Table 6.3 provides a summary of a

subset of fields captured by XCAL which are relevant to our analysis.

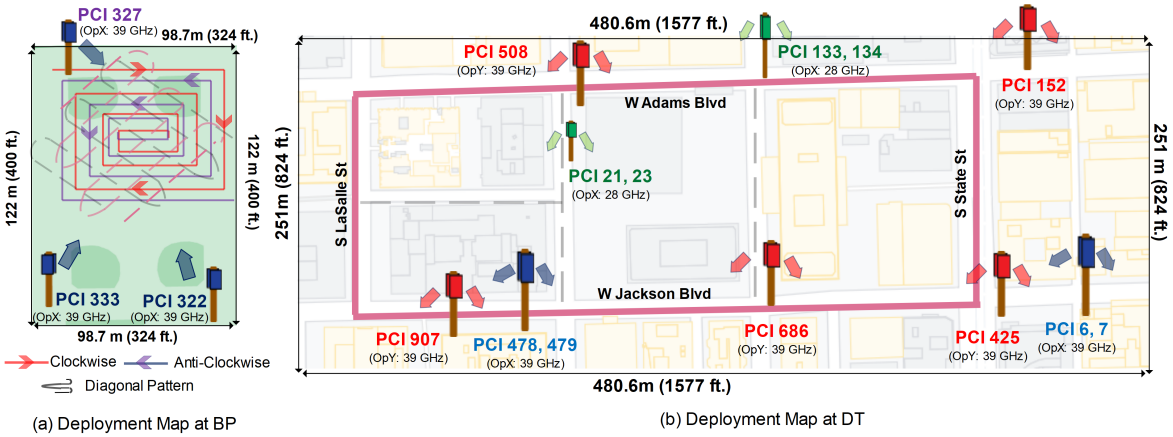


Figure 6.6: Map of 5G mmWave BS deployments and walking route/trajectory.

Overview of measurement locations We focus our measurement campaign on two regions. The first region is BP, a baseball park with large open fields spanning an area of approximately 17,170m^2. Fig. 6.6a depicts this park where OpX has deployed 3 mmWave BSs. Each BS was equipped with 3 directional mmWave transceivers. In order to understand the coverage of OpX within the baseball park area, we constructed two patterns of walking trajectory (see Fig. 6.6a): (1) a rectangular spiral pattern and (2) a zig-zag pattern which respectively took ∼27 mins (∼2.2km long) and ∼55 mins (∼4.6km) to complete a single route. We repeatedly walked pattern (1) in a clockwise and anti-clockwise directions for 3 times each, and pattern (2) in two opposing diagonals (*i.e.*, NW↔SE and NE↔SW) for 2 times each. The second region is DT, a section of downtown Chicago region that is surrounded by tall buildings, restaurants, tourist hot-spots, *etc.*, with high pedestrian as well as vehicular traffic. Both OpX and OpY have fairly dense 5G mmWave deployments in this area. We pick a 970m walking route in this region that passes through the coverage of both operators. We completed 9 walking loops of the route in an anti-clockwise direction. Fig. 6.6b depicts the walking route in DT as well as the location of the BSs. These two

Table 6.4: Dataset statistics collected from real world deployments with mmWave 5G coverage at Chicago Loop area.

Dataset Statistics	
Cumulative distance	73.76 km+ (walk), 69.1 km (drive)
Cumulative time of traces	1260 minutes+
# of commercial operators	2
# of unique 5G PCIs	OpX: 265, OpY: 105
Total area covered	2.3 km^2
mmWave 5G-NR bands	n260/39 GHz and n261/28 GHz

regions are particularly useful for this study from two perspectives. First, it allows us to compare the two and understand the impact of the environment characteristics on beam management and signal propagation. Second, the DT region allows us to compare the same between the two operators who have different deployment parameters as described in the next section.

In both regions, we use XCAL to passively collects all the lower-layer information, and run two types of active experiments: **(1)** *Ping* – measures the round trip latency every second with the target set to a Google DNS server (8.8.8.8), and **(2)** `HTTP` – download a large YUV data blob over HTTPS [26] (and repeat if the download is complete). For understanding beam management and coverage, the *Ping*-based measurements helped us ensure the 4G and 5G radios always remain in the RRC_CONNECTED state, thus avoiding any fallback to 4G due to data inactivity. `HTTP`-based measurement is used to understand the implications of beam management and configuration over network performance (*e.g.*, downlink throughput). Table 6.4 provides a statistical summary of our collected dataset over the full campaign at Chicago. In this work, we particularly only focused on data collected on foot.

6.3.2 Overview of mmWave deployment parameters

Table 6.5 summarizes several parameters observed in the data collected from our coverage analysis of Chicago city for both OpX and OpY. The key differences between the two operators

Table 6.5: mmWave Deployment Parameters (as of June'21).

Parameter	**OpX**	**OpY**
Radio Make	Ericsson	Samsung
Radio Model	AIR 5121/6701	HT5H01-60A
# of Antenna Panels	2 to 3 per BS	2 per BS
PCI Assignment	1 per panel	1 per BS
Max. Ch. Agg. (CA)	4 or 8 channels	8 channels
Max. # of Tx Beams	13 per PCI	56 per PCI
5G Deployment Model	NSA	NSA
5G-NR Band	n261, n260	n260
LTE Anchor Band	Band 2, 5, 66	Band 2 & 66
Ch. Width	100 MHz	100 MHz
Sub-Carrier Spacing	120 kHz	120 kHz

include: *(i) PCI assignment:* OpX has a unique PCI for every directional panel (*e.g.*, if a single BS has 3 panels, we observe three unique PCIs) whereas OpY has one per BS; *(ii) number of Tx beam indices:* OpX uses fewer beam indices (13 per PCI or 26 for a BS with 2 panels) compared to OpY (56 per PCI/BS)[4]. This observation suggests OpX uses wider beams than OpY; *(iii) 5G-NR band:* OpX uses both 28 GHz and 39 GHz in DT and only 39 GHz in BP while OpY uses only 39 GHz in DT. All BSs of both operators in DT use carrier aggregation (CA) to aggregate a maximum of 8 mmWave channels (1 primary and up to 7 secondary channels), each 100 MHz wide. We also find that depending upon the location (or radio model and/or band), OpX might either aggregate a maximum of 4 or 8 channels. OpY was observed to support up to 8 aggregated channels. With majority of our HTTP-based experiments (that saturated the downlink capacity) focused in the DT and BP regions, we observe that OpX aggregated up to 4 channels in 28 GHz and up to 8 channels in 39 GHz. OpY was observed to support up to 8 aggregated channels.

Carrier aggregation (CA) in frequency can occur over a single beam or multiple beams. As shown in Fig. 6.7, each Tx beam can transmit on up to eight 100 MHz wide channels. In

4. We observe a maximum beam index of 29 and 63, per PCI for OpX and OpY, respectively. While we observe only a subset of the beam indices in our walking experiments, the unseen beam indices might either be deactivated or can be observed at other regions (*e.g.*, at higher altitude).

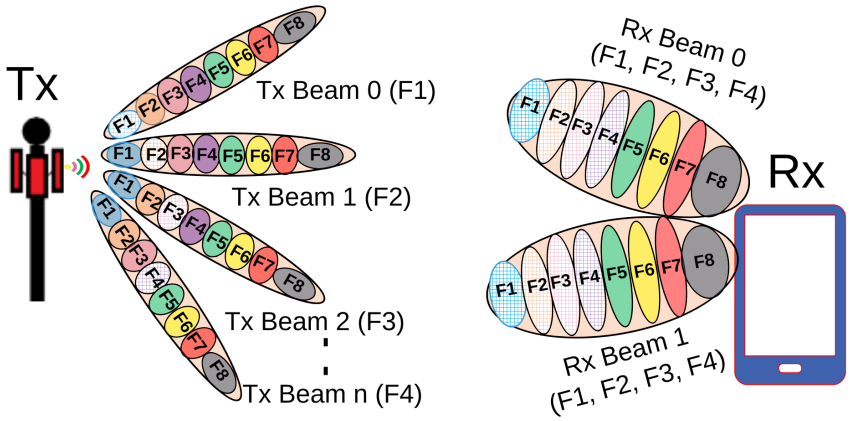


Figure 6.7: Carrier Aggregation (CA) in mmWave.

the deployments we measured, a particular frequency was transmitted only on one Tx beam, *i.e.*, there were no simultaneous data transmissions on the same frequency from multiple beams. On the Rx side, the phone has two beams, each of which can receive over all frequency channels. Thus, this is not a pure implementation of Multiple-Input-Multiple-Output (MIMO) where BS transmit the same signal over multiple frequencies, but an aggregation of different signals over space-frequency with receive combining. OpX and OpY exhibit differences in how they combine CA with beams as shown in Fig. 6.8. When more than 2 channels are aggregated, OpX uses a single beam most often in both 28 GHz and 39 GHz, whereas OpY uses two beams. This could be due to our earlier observation where we found OpX uses wider beams than OpY.

6.3.3 Beam coverage in LoS and NLoS environments

Line of Sight (LoS) Coverage. In an open field such as BP, mmWave beams have little to no scope to reflect off surfaces to establish non-line of sight (NLoS) path to the UE. Not surprisingly, OpX has densely deployed 3 mmWave BSs to cover the same geographic spot. For instance, as shown in Fig. 6.6a, the central region at BP falls in the coverage footprint

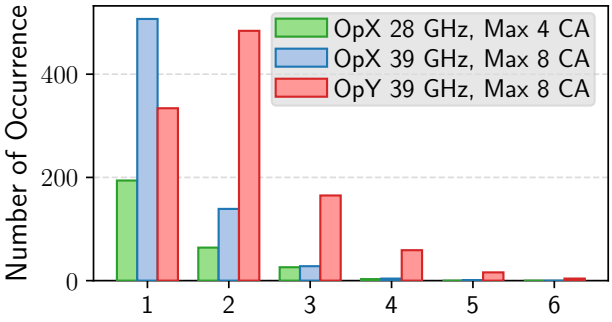
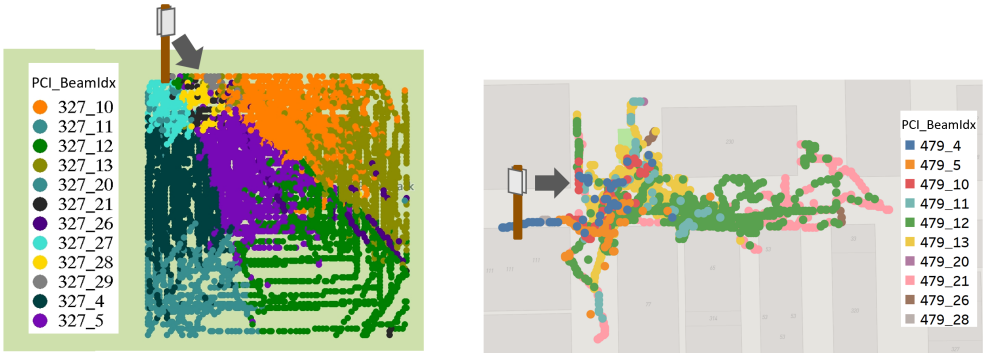


Figure 6.8: Number of beams used when CA >= 2.



(a) LoS: Serving Beams of PCI 327, OpX at BP.

(b) NLoS+LoS: Serving Beams of PCI 479, OpX at DT.

Figure 6.9: Coverage by different serving beams of a PCI (OpX).

of three different panels or PCIs (322, 327 and 333). We find that the UE typically gets connected to a PCI with LoS. We therefore use this location to understand and quantify the beam coverage. Fig. 6.9a shows OpX's PCI 327's beam coverage. This figure clearly shows each unique serving beam's demarcated geographical footprint under LoS conditions. Upon further investigation, we find that each unique beam associated with PCI 327 at BP location covers an area approximately between 1,800-4,000 m^2.

NLoS Coverage. We conduct similar analysis in the DT area that is surrounded by tall buildings. An urban canyon like this provides plenty of opportunity for the beams to reflect and establish NLoS path to the UE. Fig. 6.9b shows the coverage of OpX's PCI 479. Unlike the clear footprints observed under LoS conditions in BP, in NLoS, we find each beam's coverage can be highly dynamic and sparse. No doubt, coverage with NLoS is largely dic-

tated by two key factors: **(i)** the mmWave signal reflection characteristics provided by the surrounding environment, and **(ii)** the UE's contextual factors such as geolocation, moving speed, direction, *etc.*

6.3.4 Propagation analysis

Propagation measurements in mmWave have been conducted in multiple environments by a number of researchers, e.g. [51, 117, 91]. Most of these studies were carried out in a precisely controlled manner using high-fidelity channel sounding equipment that enables not only path loss measurements but also channel impulse responses when wideband channel sounding signals are used. These and many of similar measurements have formed the cornerstone of mmWave system development, including 5G. However, there is a dearth of measurement data on propagation in real-world environments using such as ones collected using commercial off-the-shelf (COTS) hand-held smartphones. Factors such as body-loss, hand obstructions on the receive antenna, foliage and building blockage have been considered in isolation but not in combination with real-world deployments and constraints. In this analysis, we use RSRP values recorded from the S21 smartphones running simultaneous *Ping* workload. Although the RSRP value may not be calibrated between the phones, they all uses the same modem chipset. Thus, RSRP values recorded by the modem are assumed correct within the smartphone model (*i.e.*, the same value will lead to the same behavior for all S21 smartphones).

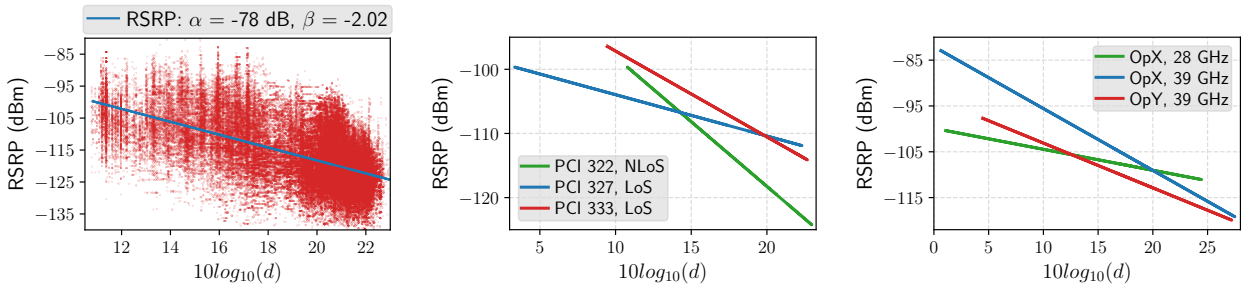
Primarily imposed by the both the tool and the UE/smartphone, there are two main limitations in the measurements available to us for analyzing propagation: **(i)** it is unclear as to how the "path loss" measurement obtained from the tool is being computed, since the transmit power could vary with the use of power control. We have observed that the RSRP of the primary channel is always higher than the secondary channels, indicating a higher transmit power. Furthermore, the combined RSRP from the two receive beams on

the phone is used to compute the path loss, not the RSRP on each individual receive beam, and **(ii)** we compute distances based on the GPS coordinates available from the phone, which have an inherent inaccuracy exacerbated by tall buildings in the DT location. With these constraints, it is impossible to "fit" the path-loss measurements to any of the well-known path-loss models [90]. Instead, since the RSRP calculation is well-defined, we focus on the RSRP measurements on a beam-pair level to perform relative comparisons of RSRP using the approach in [91] where a floating intercept model is used:

$$RSRP[dB] = \alpha + 10\beta \log_{10}(d) + X_\sigma \tag{6.1}$$

where d is the distance in meters, α is the intercept in dB, β is the slope, and X_σ is a zero mean Gaussian random variable with a standard deviation σ in dB. It should be noted here that β **should not** be considered as the path-loss exponent (PLE) since the intercept α is **not** the reference power at the reference distance of 1 m that is commonly assumed for mmWave propagation. Instead, α includes all contributions due to frequency dependence, Tx and Rx antenna gains, clutter, body loss, foliage, *etc.* However, β can be used to make relative comparisons as will be described later. The RSRP analysis in this section is based on observations made over the primary channel from the data collected using the *Ping*-based measurements. We fit the linear model described above to the RSRP for every Tx-Rx pair, where each Rx beam is considered separately.

RSRP vs. Distance for OpX in BP As shown in Fig. 6.6a OpX has deployed 3 BSs in the BP location, with PCIs 322, 327 and 333 providing coverage footprint to the inside of the baseball field. PCI 322 is partially obstructed by foliage (NLoS) while the other two PCIs are less obstructed. Fig. 6.10a shows the RSRP vs distance performance of PCI 322 where the scatter plot of all individual Tx-Rx beam pairs (not just the best beam pair) is shown, along with the best linear fit. Fig. 6.10b shows the best-fit line computed similarly for all



(a) RSRP vs. distance, OpX, BP, PCI 322.

(b) RSRP vs. Distance, OpX in BP.

(c) RSRP vs. Dist., DT, OpX and OpY.

Figure 6.10: Line fitting of RSRP vs. distance.

three PCIs in that location. As mentioned above, we can use the relative difference in the slopes, β, of these three PCIs in the same area to conclude that the obstructed PCI, PCI 322, has a higher PLE than the other two PCIs in the area.

RSRP vs. Distance for OpX and OpY in DT We combine the RSRPs for each Tx-Rx pair through the entire DT area for OpX in 28 GHz and 39 GHz and OpY in 39 GHz over all deployed PCIs. Fig. 6.10c shows the performance. OpX at 28 GHz has a lower slope (smaller PLE) compared to 39 GHz, due to the frequency difference, while OpX at 39 GHz exhibits a slightly higher slope (larger PLE) compared to OpY which could be due to the use of wider Tx beams leading to less power received at the same distance. However, overall there is not a significant difference at 39 GHz between the two operators since the deployment environment is basically the same.

6.3.5 Beam selection analysis

To better understand the impact of environmental features (*e.g.*, open-space vs. urban canyon), Fig 6.11 compares the RSRP of the serving beam between BP (LoS) and DT (NLoS+LoS). Overall, we find the RSRP at BP (which, except PCI 322, mainly propagates via LoS to UE) is higher by 3 to 4 dBm when compared to DT which is a mix of LoS and NLoS.

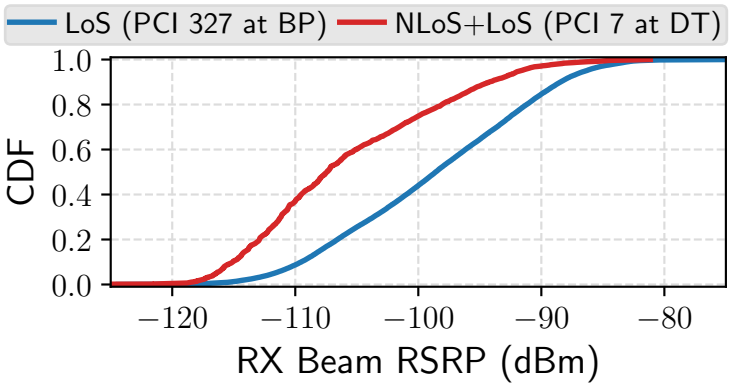


Figure 6.11: CDF: LoS vs. NLoS

When selecting the serving beam especially under situations where multiple PCIs (or beams) can cover the same geographic region or when the UE is on the move, operators have to track the UE's location and perform beam switching. To better understand the beam selection strategy used by the operator, we select several metrics (*e.g.*, RSRP, RSRQ, CSI, *etc.*) of the serving beam and compare it against that of the *neighboring beams* (up to 3, which can be from same or different PCI) as seen by the UE. We find that in general, operators use RSRP to make beam selection. We therefore use RSRP for further analysis on evaluating the beam selection strategies deployed by both the operators. We also compare the *Serving Beam*'s RSRP with the *Best Beam*[5] as reported in the Qualcomm chipset's `ML1 Searcher Measurement` log messages.

As discussed earlier, BP represents an open field (with high density of people during events) providing less opportunity for establishing NLoS paths between the BS and UE. Not surprisingly, in BP we find OpX has deployed multiple PCIs with overlapping coverage footprint and depending upon the UE's moving direction, the UE gets connected to the PCI with LoS. For instance, the patch illustrated in Fig. 6.12a falls under the footprint of all the three PCIs. The bearing (or azimuth) angles which represents the direction of UE's mobility shows distinct density distributions when connected to PCI 327 versus PCI 333. In terms

5. Details on how Qualcomm decides which beam is the best is not fully known. Our correlation analysis suggests this to be chosen from the beam with the highest instantaneous RSRP measured by the chipset.

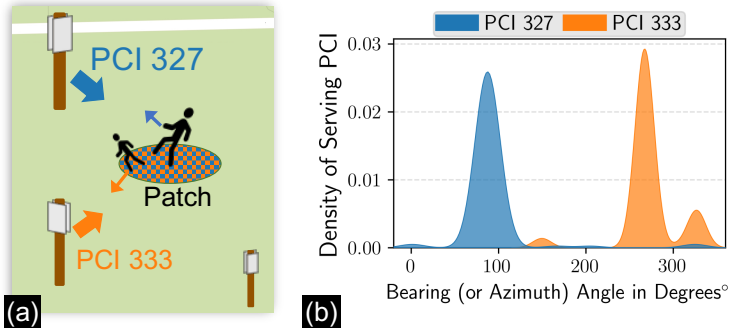


Figure 6.12: OpX: UE @ BP prefers PCI (and Beam) with LoS.

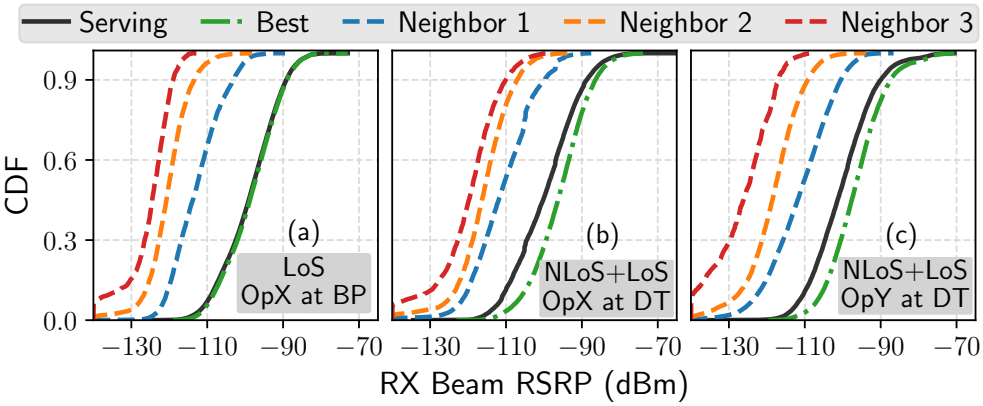


Figure 6.13: CDF of OpX RSRP: serving beam vs. best beam vs. top {1, 2, 3} neighbor.

of how well an operator performs in selecting the best beam as the serving beam, Fig. 6.13a shows that in BP (or under LoS conditions), the *Best* beam clearly match the *Serving* beam. On an average, the selected beam is also 14.4 dBm higher than the *Neighbor Top 1* beam. This suggests, operators show the ability to in general select the best beam under LoS. Note, selecting the best beam does not always result in better coverage especially in open space settings with limited to no scope of signal reflection.

On the other hand, Fig. 6.13b (and Fig. 6.13c) show the RSRP at the DT (*i.e.*, LoS + NLoS environment), on an average there is a degradation of 3.6 dB of the *Serving* beam's RSRP when compared to that of the *Best* beam. Nonetheless, our study highlights and quantifies the challenges faced by operators which could have several implications on network and application performance. Clearly, differences in the environmental features has an impact

Table 6.6: Beam switching statistics at DT.

Operator	Intra-BS Beam Switch			Inter-BS Beam Switch		
	Swtch. interval	Delay (s)		Swtch. interval	Delay (s)	
		μ	σ		μ	σ
OpX-28 GHz	6.99 s	0.16	0.09	43.39 s	4.72	2.35
OpX-39 GHz	70.18 s	0.35	1.66	N/A	N/A	N/A
OpY-39 GHz	1.29 s	0.2	1.12	85.03 s	24.03	73.14

of signal reflection and propagation. Such impact is known but challenging to quantify especially in-the-wild. we believe our initial analysis on beam selection as well as the dataset will establish a baseline for the research community as well as to track longitudinal insights.

Intra-BS and Inter-BS Beam Switching Statistics

We perform an analysis on OpX and OpY data collected at DT using the *Http* workload that activates more beams. Table 6.6 shows the statistics of beam switching within different beams in the same BS (intra-BS) and beam switching between different BSs (inter-BS) at DT. The phones are side-by-side during the measurement walk, thus enabling comparison of beam switching data from different phones.

OpY uses a larger number of narrower beams compared to OpX and hence we see that the switching interval is smaller, i.e. beams are switching more often within the BS. Since DT is a mix of NLoS and LoS, this is expected. The delay incurred by switching beams are varying between all operators. However, given that OpY has less switching interval and considerably low delay, it may demonstrated a more efficient beam management algorithm. For OpX in 39 GHz, we observe high beam switching interval and delay compared to 28 GHz, indicating that the 39 GHz BS holds on to a beam more due to its high delay. Over all operators, the 39 GHz beams shows a higher intra-BS beam switching delay compared to 28 GHz.

The deployment map in Fig. 6.6b shows that OpX's 28 GHz BSs are deployed closer together than OpY's, which results in a lower inter-BS switch interval for OpX compared to OpY. Meanwhile, OpX's 39 GHz BSs are deployed 340 m between each other, thus the UE

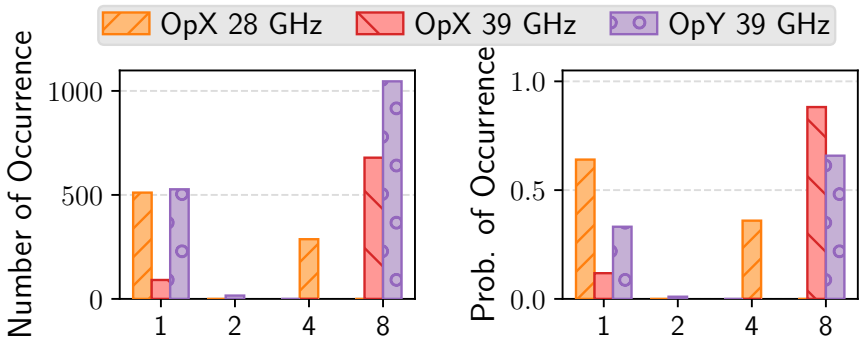


Figure 6.14: Number and prob. of frequency channels aggregated.

never switch between them. It is interesting that the inter-BS switch delay for OpY is much higher: it may due to a less optimized switching algorithm.

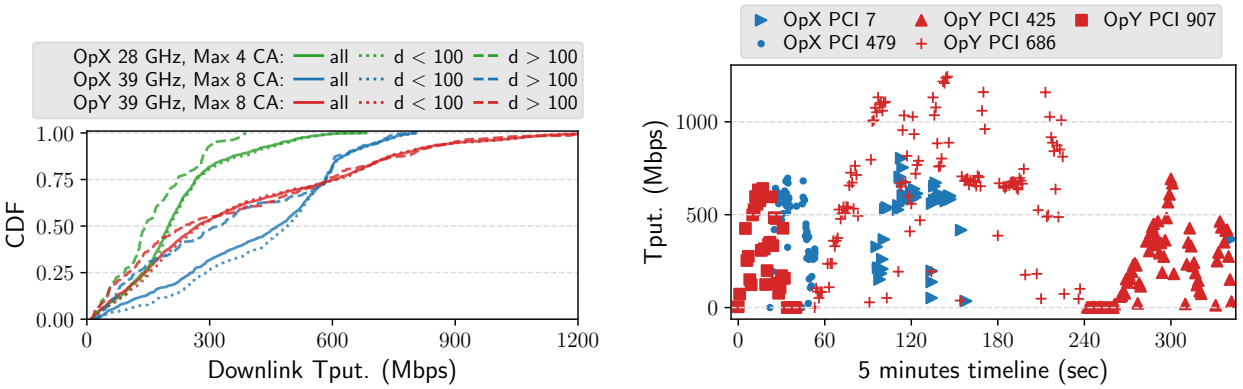
6.3.6 Performance analysis

Fig. 6.15a shows the throughput CDFs of OpX and OpY at 39 GHz and OpX at 28 GHz in DT for **all** data and separated by $d < 100$m and $d > 100$m, with d as the distance between BS and phone. There are a number of interesting observations we can draw from these results:

1) OpX's **maximum throughput over all data** is lower than OpY's in both bands. This is due to 2 reasons: (i) Fig. 6.14 shows that OpX aggregated a maximum of 4 channels at 28 GHz compared to 8 by both operators at 39 GHz, and (ii) we see from the deployment map in Fig. 6.6b that OpX's 39 GHz BSs are much farther apart than OpY's. In fact, it is rather curious that OpX has deployed their 28 GHz BSs closer together than the 39 GHz BSs: given the theoretical difference in path loss at these 2 frequencies (corroborated in Fig. 6.10c), it should have been the other way around.

2) OpX's **median throughput over all data** at 39 GHz is higher than OpY's. Fig. 6.14 show that this is due to OpX at 39 GHz aggregates 8 channels at 88% of the time compared to OpY at 62%. Also, OpX's median throughput is dominated by the data for $d < 100$m, *i.e.*, the increased carrier aggregation outweighs the reduced RSRP due to distance.

3) By comparing OpY's throughput between $d < 100$m and $d > 100$m, we see that



(a) Throughput comparison for different distances.

(b) Throughput vs. time

Figure 6.15: Throughput analysis at DT

the throughput distribution is relatively unaffected by distance. This is due to the average distance between their BSs being less than OpX at 39 GHz.

4) Fig. 6.15b shows throughput from a 5 minutes section of the measurements, which starts from LaSalle & Jackson and ends at State & Jackson. Clearly, the denser deployment of OpY (3 BSs) leads to more uniform and higher throughput over that region, with the best throughput achieved by OpY's PCI 686 due to the LoS environment surrounding the BS.

These measurement study of real-world 5G NR mmWave beam management has revealed the different deployment parameters used by the operators (*i.e.*, differences in channel frequency, beam width, number of beams), which in turn provide interesting insights on the mmWave signal propagation, coverage, beam management, and network performance.

6.4 Outdoor-to-Indoor Performance Analysis of a 5G mmWave Deployment

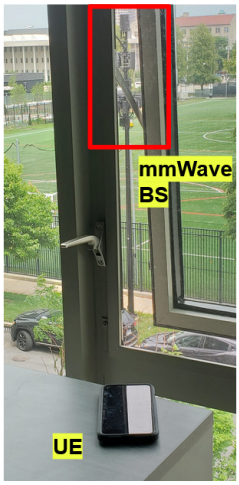
As the previous measurement campaigns were focused on outdoor measurements of 5G, there is a lingering research question regarding the performance of 5G indoors while the BSs are outdoors. To address this, we conducted indoor measurements at a University

of Chicago dormitory building which conveniently has a Verizon mmWave BS across the street. We first present an indoor performance analysis of 5G NR among the three US operators (*i.e.*, AT&T, T-Mobile, Verizon). Then we present a focused analysis of Verizon's 5G mmWave performance (in terms of downlink throughput, uplink throughput, and latency) under varying window opening gap sizes.

6.4.1 Methodology and Deployment Overview

Fig. 6.16a shows the indoor measurements site: Woodlawn Residential Commons, a 7 storied dormitory building at the University of Chicago. The building is located at 1156 E 61st St, conveniently beside (∼25 m) a Verizon mmWave BS deployment. The building has completed its construction in 2020, with an unknown type of glass used in the windows. However, we believe that the windows are most likely Low-E glass given the very recent construction of the building. We conducted indoor measurements in various rooms in July 2021, with special permission from the university.

(a) BS and UE location.



(b) Line-of-Sight (LoS) between BS and UE.

Figure 6.16: Outdoor-to-indoor (OtI) measurement location.

For the UEs, we utilized up to three Google Pixel 5 phones, equipped with AT&T, T-

Mobile, and Verizon SIMs with unlimited data plans. As with our prior works, we utilized multiple SIMs to avoid data cap throttling. Each phones passively ran SigCap and NSG on Google Pixel phones to collect detailed signal parameters. Conversely, the FCC ST app is utilized to actively run download, upload, and latency test on every minute.

Table 6.7: Indoor Cellular Reception at UChicago Dormitory. SA: standalone, NSA: non-standalone

Operator	**5G NR Mode**	**5G NR Band (Max. Bandwidth)**	**4G LTE Band (Max. bandwidth)**
AT&T	NSA	n5, 850 MHz (5 MHz)	2 (15 MHz), 12 (10 MHz), 14 (10 MHz), 17 (10 MHz), 30 (10 MHz), 66 (10 MHz)
T-Mobile	NSA	n41, 2.5 GHz (100 MHz), n71, 600 MHz (20 MHz)	2 (15 MHz), 66 (15 MHz)
Verizon	NSA	n5, 850 MHz (10 MHz), **n261, 28 GHz (400 MHz)**	2 (5 MHz), 13 (10 MHz), 66 (20 MHz)

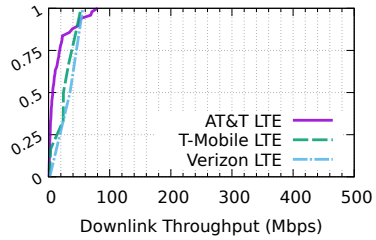
6.4.2 Comparison of 5G NR performance among different bands and operators

We surveyed 2nd - 7th floors of the building (the accessible floors for measurement) by placing three Pixel 5 phones on a cart. Each phone is equipped with AT&T, T-Mobile, and Verizon SIMs. We then turn the passive and active measurements, and wheeled the cart through corridors and rooms in the east side of the building which faces Verizon mmWave BS. All windows were shut during this survey. Table 6.7 shows the summary of indoor reception in the dormitory: there are a varying number of different 4G LTE and 5G NR channels, in low-, and mid-bands. First, all 5G deployments are NSA, and we were not able to "force" SA mode on T-Mobile by disabling LTE connection using NSG, possibly due to lack of SA deployment nearby. We were able to receive low-band n5 deployments by AT&T and Verizon indoors. On the other hand, T-Mobile has a more varying 5G deployment: a

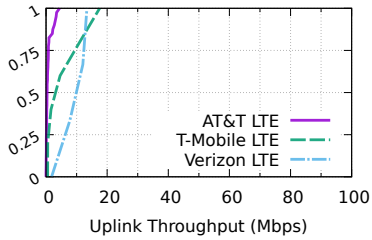
low-band n71 and and a mid-band n41 can be received indoors. For high-band/mmWave, we observed Verizon 5G mmWave reception indoors in 28 GHz with a maximum bandwidth of 400 MHz using 4-channel aggregation (CA). However, the reception was very limited and with poor RSRP. The mmWave signals are not available at all on the 7th floor possibly due to the downwards orientation of mmWave panels. While on the 2nd - 6th floors, there were only a handful of rooms that were LoS to the BS that could receive 5G mmWave signals when the window was open. This is likely due to the Low-E glass used in the windows. For AT&T and T-Mobile channels, we are uncertain about the exact location of their outdoor BSs. However, we confirmed from the PCIs that all indoor reception of Verizon's NR and LTE channels were being transmitted from the BS on the pole right outside the building. This particular Verizon BS also shows an outdoor availability of Bands 46 (LAA) and 48 (CBRS). However, we also did not detect both bands indoors, most likely due to the lower transmitted power allowed in these bands.

Since all 5G deployments are NSA, each 5G connection consists of LTE and NR channels. For AT&T and T-Mobile, the choice of LTE and NR channels are predictable based on the RSRP. However for Verizon, but there was a difference in the LTE primary channel used depending on the NR band. When NR Band n5 (low-band, bandwidth 10 MHz) was used, the LTE primary on the DL was always Band 66 with a bandwidth of 20 MHz, whereas when NR Band n261 (mmWave) was being used, the LTE primary carrier on the DL was either band 66 (20 MHz) or band 13 (10 MHz). This difference in choice of LTE primary channel has an effect on overall DL and UL throughput as shown on the later analysis.

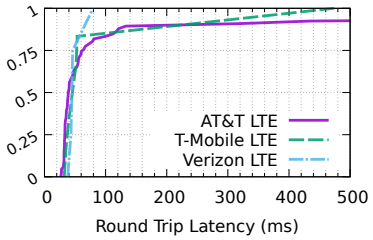
DL Throughput comparison: From Figs. 6.17a and 6.17d we see that NR clearly delivers significant DL throughput improvements over LTE, especially for T-Mobile and Verizon. AT&T NR performance is limited due to the low-band only deployment using only 5 MHz of bandwidth, compared to T-Mobile's 100 MHz at 2.5 GHz and Verizon's 10 MHz. Since Verizon 5G mmwave was not received during these tests, the DL throughput is solely



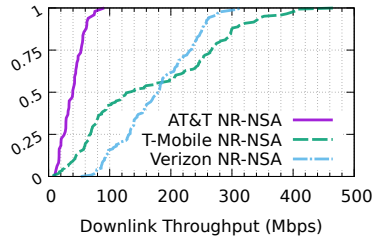
(a) LTE downlink throughput.



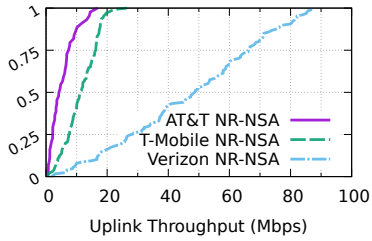
(b) LTE uplink throughput.



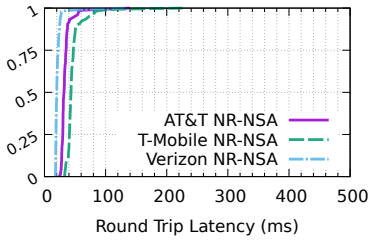
(c) LTE latency.



(d) NR-NSA downlink throughput.



(e) NR-NSA uplink throughput.



(f) NR-NSA latency.

Figure 6.17: Indoor survey of AT&T, T-Mobile, and Verizon in terms of throughput and latency performance.

via aggregation of LTE and low-band NR. With no mmWave reception, T-Mobile NR DL throughput is superior to Verizon's, even though the Verizon BS is very close to the building. Once again, this survey demonstrates the severe limitation of indoor 5G mmWave reception.

UL Throughput comparison: From Figs. 6.17b and 6.17e we see that here too NR clearly delivers significant UL throughput improvements over LTE, for all operators. There is a clear advantage of Verizon UL, most likely due to the aggregation with the 20 MHz band 66 LTE carrier and the proximity of the location to the BS enabling higher modulation-coding settings. For example, the 80 Mbps throughput is due to 65 Mbps over band 66 and only 15 Mbps over NR band n5.

Latency comparison: From Figs. 6.17c and 6.17f we see that there is not an appreciable reduction in latency with NR, though overall Verizon latency with NR is the lowest. However previous results already noted that NR latency was lower in the low-band compared to mmWave, and these results only include low-band NR. It should also be noted that since most of these measurements were over the NSA mode of NR, the latency could be higher

due to the dual connectivity, channel aggregation and the use of the 4G core network. As SA with the new 5G core begins to be deployed, we anticipate that the latency results will improve.

6.4.3 Performance of 5G mmWave as a function of window opening gap size

We first did a preliminary measurement where we open the window of each room facing Verizon 5G mmWave BS on all floors, and we observe the best 5G mmWave performance in room E206 on the 2nd floor. Therefore, we utilized the room for additional experiments to quantify performance as a function of the window opening gap size. The UE was placed on top a desk with line-of-sight (LoS) to the mmWave BS as shown in Fig. 6.16b. We then vary the width of the window opening as shown in Fig. 6.18, where Gap 1 is the widest gap and Gap 4 is a fully closed window. For each gap scenario, passive and active measurements were taken over 15 minutes.

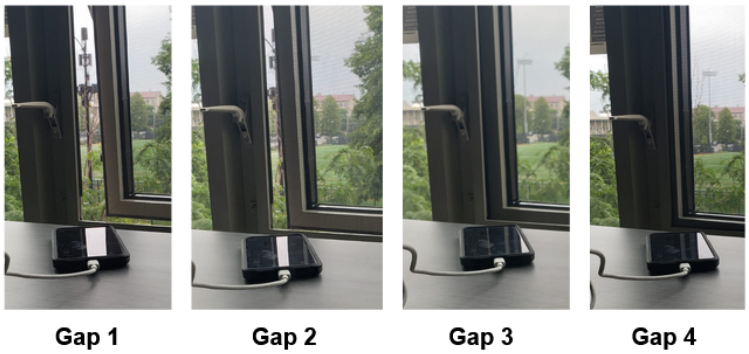


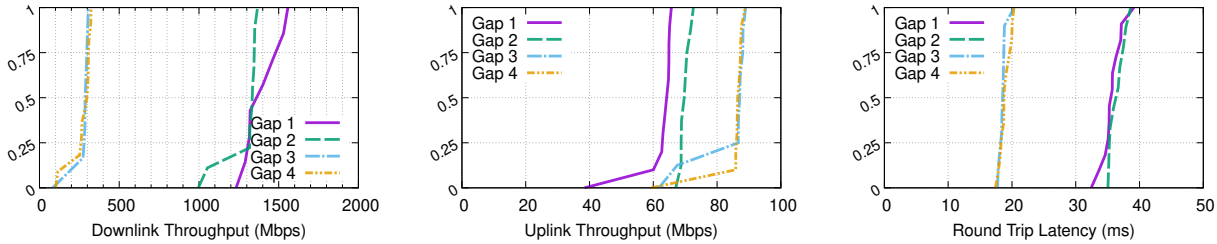
Figure 6.18: Window opening gap diagram.

First, we present coverage performance on each gap scenario, in terms of RSRP and RSRP as shown in Table 6.8. The phone was connected 5G mmWave for Gaps 1 and 2, then it was handed-over to 5G low-band for Gaps 3 and 4. Thus, the overall lower RSRP values in Gaps 1 and 2 are due to the shorter wavelength. While the average RSRQ stays constant

Table 6.8: NR Reception on Different Gaps

Gap #	NR Channels	Avg. RSRP	Avg. RSRQ
Gap 1	4 × n261 (400 MHz)	-89.52 dBm	-11 dB
Gap 2	4 × n261 (400 MHz)	-98.98 dBm	-11 dB
Gap 3	1 × n5 (10 MHz)	-74.34 dBm	-11 dB
Gap 4	1 × n5 (10 MHz)	-75.60 dBm	-11 dB

on all Gaps, we observe reduction of average RSRP from Gap 1 to Gap 2, and from Gap 3 to Gap 4. The decrease of RSRP by 10 dB from Gap 1 to Gap 2 illustrates the vulnerability of mmWave connections when encountering obstructions such as Low-e glass. While on Gaps 3 and 4, there is not much difference in the RSRP since Band n5 at 850 MHz propagates very well indoors and is less dependent on the window gap size.



(a) Downlink throughput. (b) Uplink throughput. (c) Round trip latency.

Figure 6.19: Throughput and latency performance as a function of window opening size

Fig. 6.19 show the throughput and latency performance on the varying window gap scenarios. For downlink throughput as shown by Fig. 6.19a, we observe a better performance on Gaps 1 and 2. This can be explained due to the high bandwidth of the 5G mmWave connection. Contrarily, Fig. 6.19b and 6.19c shows the best UL throughput and latency is achieved by Gaps 3 and 4, possibly due to the LTE channel aggregation of the NSA mode. These results shows that a true Gbps downlink throughput over 5G mmWave can only be delivered indoors with unobstructed LoS. On the other hand, the mmWave connection has worse uplink throughput and latency performance compared low-band NR.

While our work on the performance of OtI mmWave is comparable to a prior work by [64], the methodologies employed are very different, leading to different and contradictory

conclusions. First, the throughput results reported in [64] are based on predictions from signal strength measurements using a specific channel sounder that utilizes a continuous-wave tone at 28 GHz as the sounding signal, rotating horn antennas on the receiver and omni-directional transmit antennas: very different from actual operating conditions of 5G mmWave. On the other hand, we specifically conducted our measurements on deployed 5G mmWave systems using consumer handsets which captures real-world conditions such as beam-management using phased-arrays at both BS and UE, wide-bandwidth operation (400 MHz), and handset limitations. Additionally, our performance metrics are measurements of throughput and latency over all of the network stack, thus it includes overheads due to the MAC, transport, and network layers. Contrarily, we believe the prior work lack in accounting the effects of the intermediate layers in their prediction. These major differences in measurement methodologies and environment has lead to the contradictory results: the prior works [64] shows a prediction of 500 Mbps in a building with high-loss glass (*i.e.*, Low-e) windows for 90% of users located up to 49 m away from the BS, while our results demonstrate that in a building with Low-E glass windows located about 25m from a 5G mmWave BS, there is no 5G mmWave connectivity at all through closed windows and limited connectivity in a few locations with the window open. Further, the measurements over different bands and operators demonstrate that the low and mid-band 5G NR can still provide DL throughput of up to 400 Mbps even when 5G mmWave is unavailable in the building.

6.5 Impact of Device Thermal Throttling to 5G mmWave Performance

During many of our 5G mmWave throughput measurements, we noticed a repeated pattern of drastic throughput reduction after at least 1 minute of sustained downlink transmission. This reduction is due to the UE releasing connection of the maximum 4 mmWave channels to 1 channel, and finally a handover to 4G LTE in some cases. This pattern of failing to sustain 5G

mmWave throughput over an extended time is persistent over all of our smartphone models (*i.e.*, Pixel 5, S21 Ultra, S21+), but seemingly depends on time of the day, month of the year, and location (Chicago vs. Miami). From all of the possible causes, we narrow it down to a similarity of high ambient temperature at the time of measurement, which leads to higher device temperature and thermal throttling. The relationship between device temperature and sustained 5G mmWave throughput has not been explored in academic study and we aim to demonstrate it in this study [99]. In particular, we seek to demonstrate that the drop in throughput is indeed due to thermal. According to the 3GPP standard [6], a UE can provide information to the BS about its thermal state via the the RRC_CONNECTED message field. Upon receiving such a message from the UE, the BS will respond by temporarily reducing the number of aggregated data streams, in both component carriers and MIMO layers, for both downlink and uplink transmissions until the thermal warning messages are no longer received.

Thus, we present the following contributions: (1) We present results from detailed experiments conducted with consumer 5G smartphones operating over deployed 5G mmWave networks in multiple US cities to demonstrate that indeed this phenomenon occurs repeatedly on high ambient temperatures. (2) We demonstrate that as the skin temperature measured by the device increases, the number of aggregated mmWave channels drops from 4 to 1 followed by handover to 4G LTE, with the throughput dropping at each step. With external cooling, *e.g.*, using an ice-pack or low ambient temperature (*e.g.*, on a winter day in Chicago), high throughput can be sustained over several minutes. (3) We identify explicit message exchanges in the Radio Resource Control (RRC) layer between the user equipment (UE) and the base-station (BS) that confirm that the reason for handing over to 4G LTE is thermal and not network congestion or other considerations. (4) Lastly, we used an infra-red (IR) camera to further corroborate the effect of temperature rise at the mmWave antenna locations on throughput.

Table 6.9: Experiment Parameters

Parameter	**Value**
Operator	Verizon (Band n261/28 GHz)
# of experiment locations	Chi.: 2, Mia.: 1, SF: 1
Device model	Google Pixel 5
# of devices used	Chi.: 2, Mia.: 1, SF: 1
Cumulative # of meas. runs	32
Distance between BS and UE	∼2 meter
Average RSRP over all meas.	-92.63 dBm

(a) Chicago (b) Miami (c) San Francisco

Figure 6.20: Measurements locations in the three different cities (see Table 6.10).

6.5.1 Device methodology

In order to demonstrate the effect of device skin temperature on sustained throughput over 5G mmWave, the following requirements need to be met:

- A sustained download of a high-bandwidth data stream over ∼15 minutes while connected to a 5G mmWave BS.
- A method of measuring temperature while the download is occurring, and
- A method of extracting RRC messaging between the UE and the BS while the download is occurring.

Table 6.9 summarizes the parameters of the experiments conducted in two locations in

Table 6.10: Experiment Locations

Location	**#**	**Address**	**GPS coordinate**	**Traffic used**	**# of meas. runs**	**Ambient temp. at meas. time**
Chicago	1	61st St. & Woodlawn Ave.	41.7874024, -87.5965241	BG DL+FCC ST	16	Oct: $\sim 24^\circ$ C, Jan: $\sim -10^\circ$ C
	2	61st St. & Midway Plai.	41.7844559, -87.5962098	BG DL+FCC ST	9	
Miami	3	Bayfront Park	25.7753436, -80.1853549	BG DL	6	Sep: $\sim 31^\circ$ C
San Francisco	4	Pine & Stockton St.	37.7914117, -122.407218	BG DL+FCC ST	1	Sep: $\sim 15^\circ$ C

Chicago, one location in Miami and one location in San Francisco. Data was collected in all 3 cities over September - October 2021, and in Chicago in January 2022 for performance comparison under cooler ambient temperatures. All experiments were conducted using the same UE model and network: Google Pixel 5, running Android 11 on a Verizon network with an unlimited data plan[6]. Fig. 6.20 shows the specific measurement locations in Chicago, Miami and San Francisco, while Table 6.10 shows detailed information of each location. The Verizon 5G mmWave network at each location utilizes band n261 at 28 GHz.

Downlink throughput saturation is achieved using a combination of two methods:

- **Background Download (BG DL)** using HTTP download of a 10 GB dataset file [26].
- **FCC Speed Test (FCC ST)** app: the 5 sec downlink throughput test is run repeatedly to ensure that the link stays saturated continuously.

Thermal throttling was observed using either one of the above methods, but combining both methods ensures that the link is fully saturated. The Miami measurements used only the

6. Subscribed Verizon plan indicates a throttling after 50 GBytes for 4G and 5G low/mid-band data, and no throttling for 5G mmWave data.

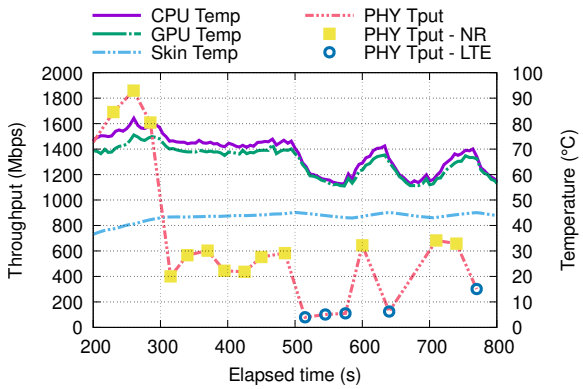
BG DL traffic, while BG DL + FCC ST was used in the Chicago and San Francisco measurements. Due to this minor difference in methodology, there are two separate throughput measurements: **PHY** level throughput collected by Network Signal Guru (NSG), and **APP** level throughput collected by FCC ST. Using all the measurements reported in this paper, we verified that, as expected, the APP throughput is always lower than the PHY throughput. APP throughput values are easier to extract from FCC ST than PHY throughput from NSG (requiring manual data input). Thus, these different types of throughput measurements are carefully separated and only the same type of throughput values are compared whenever needed in our analysis. To passively collect signal data on the smartphones, we utilized SigCap and NSG.

SigCap's temperature sensor implementation. SigCap is again utilized to primarily collect time and signal parameters (*e.g.*, 4G and 5G RSRP, RSRQ, RSSI, PCI, 4G frequency, etc) using APIs. To measure device's thermal, we implemented a new sensor handler that queries hardware temperature data from the sensor API [13] which includes instantaneous skin, CPU, and GPU temperature measurements. Details of collected parameters are described in Table A.6.

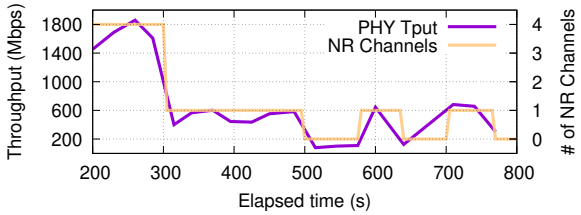
Network Signal Guru (NSG) [87]. NSG is also similarly used to provide more detailed information about the transmission such as operating frequency, number of carrier components, bandwidth, PHY throughput, and RRC messaging. The data collected are manually transcribed with 5 seconds interval and hence we use it only for certain analysis.

6.5.2 Impact of 5G mmWave on UE Temperature

5G mmWave throughput and UE temperature Vs. time. Using the tools and methodologies described in the previous section, we performed a total of 32 measurement runs over all locations, where each measurement run starts with a cool phone temperature.



(a) Throughput degradation correlated with device temperatures.



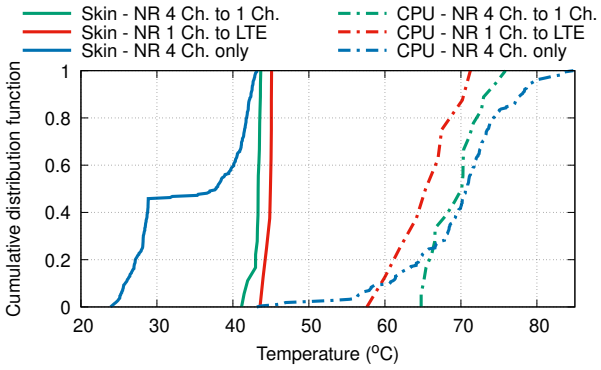
(b) Correlation of throughput with number of NR channels.

Figure 6.21: Representative results of throughput degradation.

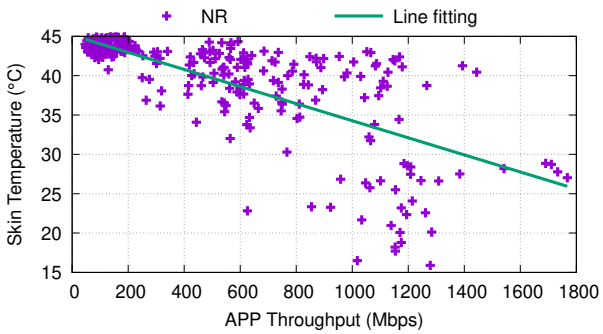
Fig. 6.21 shows a representative measurement at Location 1 in Chicago (taken on Oct 9, 2021) using the combined BG DL + FCC ST method. Data collected by NSG (*i.e.*, PHY throughput, NR channel) and SigCap (*i.e.*, temperatures) are synchronized using timestamps from both apps, while the PHY throughput values are shown only when the FCC ST is running (at ∼20 sec intervals) in order to display the saturated condition.

Fig. 6.21a shows that a PHY throughput of almost 2 Gbps was achieved soon after the experiment was started at the 200 sec mark, which is the result of aggregating 4 mmWave channels as shown in Fig. 6.21b. The throughput increase is accompanied by a rise on all three temperature measurements: skin, CPU and GPU. At the 300 sec mark, the number of aggregated mmWave channels reduces to 1 and the resultant throughput is reduced significantly. At this point, the CPU and GPU temperatures are reduced slightly, but the skin temperature does not reduce sufficiently to restore the throughput to the levels seen at the beginning of the experiment. The download was completed at 800 sec.

Analysis of skin temperature effect on throughput. We observe two events: **(1)** when the number of 5G mmWave channels is reduced from 4 to 1 (*i.e.*, 300 sec on Fig. 6.21a), and **(2)** when the device is handed over to the LTE network (500 sec). At both events, we recorded a "*Secondary Cell Group Failure*" signalling packet in the NSG log, which shows



(a) CDF of CPU and skin temperature at different states.

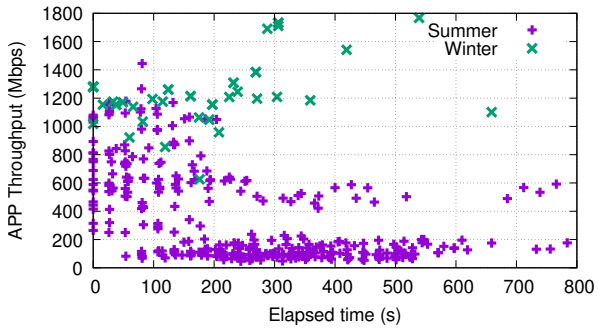


(b) Correlation between APP throughput and Skin temperature.

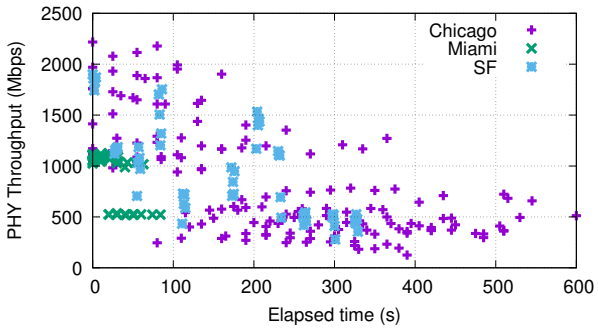
Figure 6.22: CPU and skin temperature.

compliance to the 3GPP standard [6]. Moreover, the temperature API [13] shown the static temperature threshold values: 96° C for CPU and GPU, and 43° C for Skin. Fig. 6.22a shows the skin and CPU temperature distribution of all our data from all locations for the following states: (i) the temperature when 4 mmWave channels are being aggregated, (ii) the temperature just after the switch from 4 mmWave channels to 1 mmWave channel, and (ii) the temperature just after the switch from 5G mmWave to LTE. The figure clearly shows that throttling to 1 mmWave channel happens mostly at skin temperature of ∼43° C, while throttling down to LTE happens mostly at skin temperature of ∼45° C. We omit GPU temperature since we observe that the CPU and GPU temperatures are similar. Moreover, the CPU temperature does not exhibit any correlation with the events since its threshold is never crossed. Hence, we infer that the skin temperature is the trigger that causes the throughput degradation. While it appears that there is some oscillation between states, on a larger time scale, we can still observe an on-off pattern as shown by Fig. 6.21 between the 500 to 770 sec mark.

Fig. 6.22b displays all 5G mmWave measurements collected at Chicago and San Francisco, using both BG DL and FCC ST to saturate the downlink transfer. Clearly, the higher skin temperature correlates to lower 5G mmWave throughput, with lower throughput values



(a) APP Throughput comparison between summer and winter in Chicago.



(b) PHY Throughput comparison between Chicago, Miami, and San Francisco in summer.

Figure 6.23: Throughput over multiple experiments, time-normalized to the first data

recorded mostly in summer (Sep-Oct) and the higher values recorded in Chicago in winter (Jan).

6.5.3 Thermal performance as a function of ambient conditions

Effect of ambient temperature over seasons and location. Fig. 6.23 shows the mmWave throughput versus time, where the time axis has been normalized *i.e.*, 0 sec is the timestamp of the first data point. Fig. 6.23a shows the comparison of APP throughput between summer (Sep-Oct) and winter (Jan) in Chicago. These measurements are from Location 1 and 2, using of FCC ST + BG DL traffic. It is clear from the figure that in the warmer months, when the ambient temperature was $\sim$24° C there is a degradation of throughput after 200 sec, while no such degradation is observed in the winter months when the ambient temperature was ~ -10° C.

Fig. 6.23b shows the comparison of measurements in Chicago, Miami, and San Francisco collected in summer. Since the data in Miami was captured using BG DL traffic only, PHY throughput from NSG is used in this analysis. The throughput in Miami data degrades faster (at $\sim$60 sec) than Chicago and San Francisco, which can be explained by the climate difference between these cities and the time of experiment. The Miami data was taken with ambient temperature of $\sim$31° C, while Chicago and San Francico data was taken with

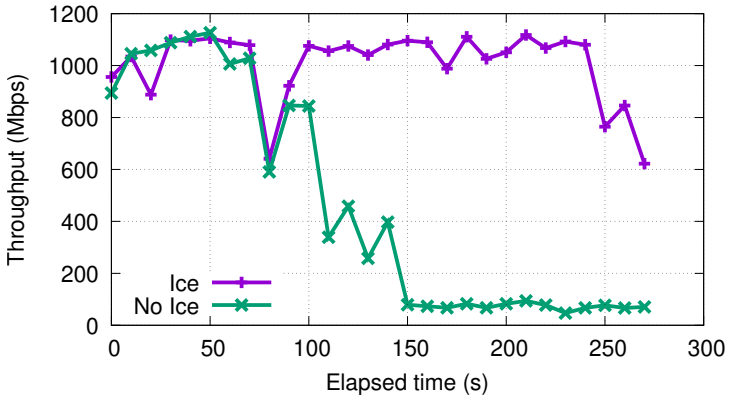
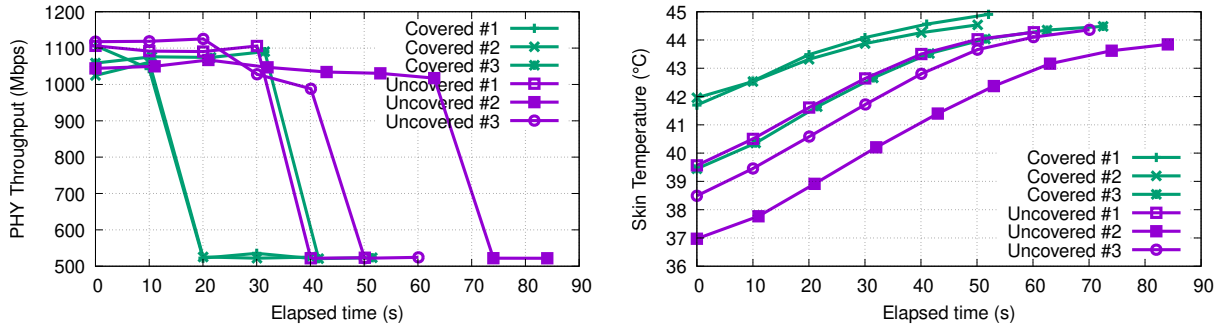


Figure 6.24: Prolonging high rate of 5G NR session via an ice bag.



(a) Throughput degradation between covered and uncovered phones.

(b) Skin temperature rise between covered and uncovered phones.

Figure 6.25: Phone cover experiments in Miami.

ambient temperature of ∼24° C and ∼15° C, respectively.

Effect of external cooling and phone cover. To further confirm the correlation between skin temperature and reduced 5G mmWave throughput, the following experiment was conducted in Miami in summer. Measurements were taken with the phone either held in the hand or placed on an ice-pack. Fig. 6.24 shows that a mmWave throughput above 1 Gbps is sustained when the phone is placed on top of an ice-pack.

Second, we investigate the impact of using a phone protective case on extending the 5G mmWave throughput. Using a standard commercially available case[7] to cover the phone, we compare throughput performance when the phone is with and without cover. Each

7. `https://www.spigen.com/products/pixel-5-case-tough-armor`

experiment type is repeated 3 times and both types were ran in Miami. Fig. 6.25a shows the achievable PHY throughput for all six runs. Without a phone cover, the phone can sustain up to 60 sec of a higher ∼1 Gbps 5G mmWave throughput using 4 channels. With the cover, the phone can only sustain the higher rate up to 30 sec.

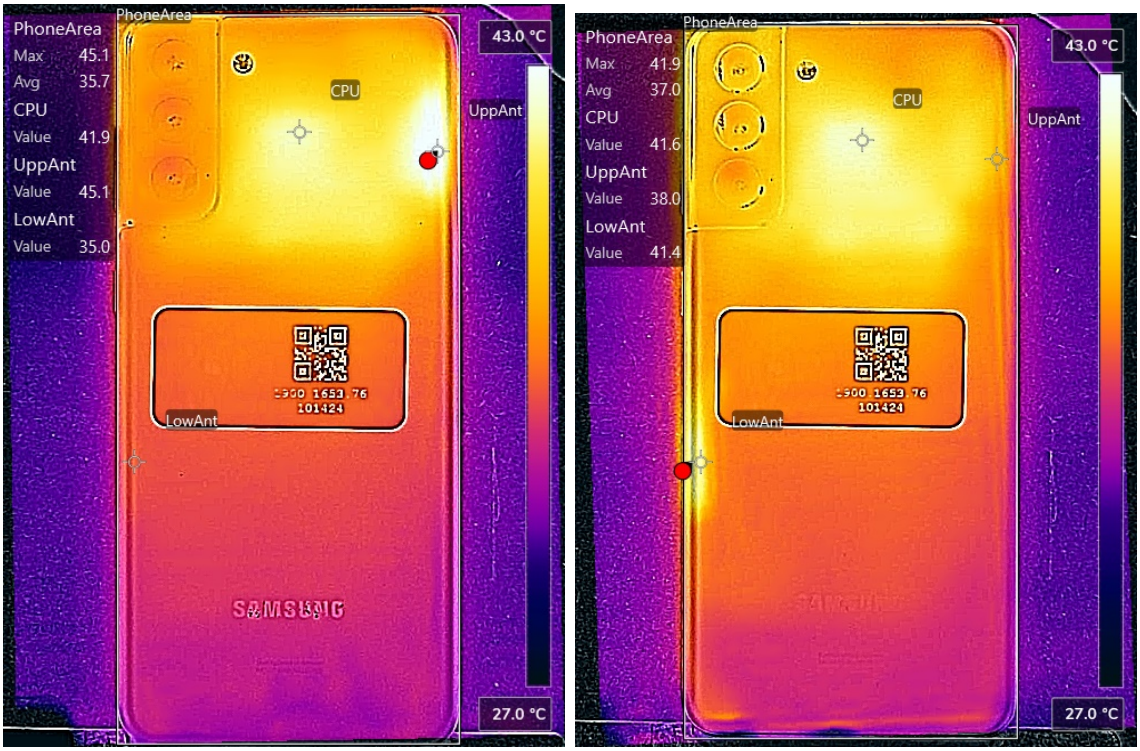
The lower throughput performance of the covered phone can be explained by Fig. 6.25b, which shows the corresponding skin temperature over all six runs. The covered phone breached the 43° C threshold at 20 sec, compared to the uncovered phone at 40 sec. Hence, the phone cover restricts heat dissipation and causes a higher skin temperature. While further experiments with more variables (*e.g.*, phone model, case type, climate) are needed, this experiment has demonstrated that faster heat dissipation allows for longer utilization of the 5G mmWave network at full capacity.

6.5.4 Thermal performance investigation using an IR camera

In addition to extracting the skin temperature from the API, we also performed IR camera measurements in May 2022. We set a FLIR One Pro LT IR camera up to mount stably ∼17.5 cm above a case-less Samsung S21+ phone with the Qualipoc measurement tool running[8]. The phone initiates BG DL traffic similar to prior experiments to capture PHY layer data (e.g., per channel SS-RSRP, SS-RSRQ, and throughput) and HTTP/application layer throughput. We captured 4 × 10 minutes runs, with the phone connected to the 5G mmWave BS at Location 1 in Fig. 6.20a with a good signal condition (∼90 dBm RSRP). The ambient temperature at the time of the experiment was 30° C.

We identified three spots on the phone with a high likelihood of heating up during the mmWave experiment: CPU and modem area (CPU), upper mmWave antenna (UppAnt), and lower mmWave antenna (LowAnt). x-y coordinates are defined for each spot, relative to the phone frame to ensure that the data is comparable between different experiment

8. https://www.rohde-schwarz.com/us/products/test-and-measurement/network-data-collection/qualipoc-android_63493-55430.html



(a) IR thermal capture on O1 (BS is to the right of phone).

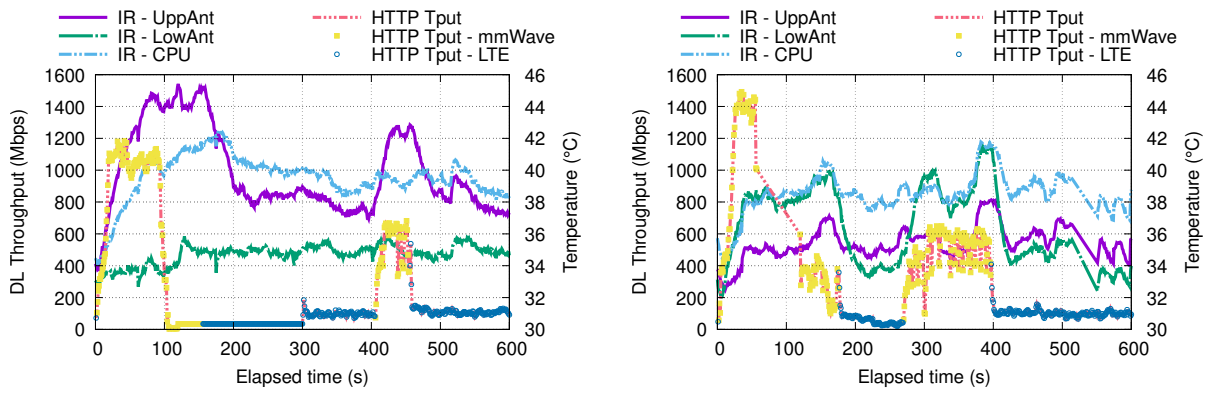
(b) IR thermal capture on O2 (BS is to the left of phone).

Figure 6.26: IR thermal captures in orientations O1 and O2.

runs. Note that none of these temperature spots directly translate to the CPU and skin temperature value collected by the Android API since the temperature API is not directly accessible on this phone.

Fig. 6.26a and Fig. 6.26b show representative thermal images[9], with two orientations, O1 and O2, w.r.t. the mmWave BS. In O1, the BS is located to the right of the phone, and both Fig. 6.26a and Fig. 6.27a shows a higher temperature on the UppAnt spot which indicates higher activity on this antenna. Conversely, Fig. 6.26b shows the O2 orientation where the BS is located to the left of the phone, and Fig. 6.27b shows higher LowAnt temperature when the phone is connected to mmWave. In both orientations, the phone started with 4 mmWave channels then throttled to 1 channel at the 95 sec and 85 sec mark for O1 and O2,

9. Full video available at `https://youtu.be/fm29QwdbVW8`



(a) Throughput and temperatures vs. time in orientation O1.

(b) Throughput and temperatures vs. time in orientation O2.

Figure 6.27: Throughput and temperatures vs. time.

respectively. Subsequently, LTE handover occurred at the 154 sec and 174 sec mark for O1 and O2, respectively. We observed a better overall throughput performance on O2 compared to O1 on all 4 runs. This is due to two reasons: location of each antenna w.r.t. the CPU (O1 is closer), and which antenna is activated during the experiment.

While we could not correlate the skin temperature to the spot temperatures, it is highly likely that the skin temperature sensor is located in the upper half of the phone, given that average temperature of the lower half was $\sim$35° C on all runs. Additionally, we performed UL traffic experiments using a similar setup and observed that the phone was connected to 1 mmWave channel during the entire 10-minute run, even as the temperature of the UppAnt spot increased to a maximum of 42° C. This observation further supports our hypothesis that fewer aggregated mmWave channels (and consequently, lower throughput) do not cause a significant rise in skin temperature, even with the additional power consumption due to transmitting, *i.e.*,**transmitting** over 1 mmWave channel caused less rise in skin temperature compared to **receiving** over 4 mmWave channels.

6.6 A Comprehensive Real-World Evaluation of 5G Improvements over 4G in Low- and Mid-Bands

While prior 4G mobile networks mainly operated on the low (<1 GHz) and mid (1–6 GHz) frequency bands (collectively referred to as frequency range 1, or FR1 [3]), initial 5G deployments in the US focused on the mmWave bands (>24 GHz), also known as FR2. We have shown that mmWave bands can provide a throughput performance of over 1 Gbps, but performance is limited by propagation loss, body loss, foliage, and thermal effects. The low-band, conversely, offers better coverage but with relatively lower bandwidth and hence throughput. Therefore, the mid-band which strikes a balance between coverage and performance has become a focal point for current 5G deployments. The novel features specified in 5G can theoretically improve throughput performance since network throughput is a function of channel bandwidth, modulation, code rate, and number of MIMO layers [5]. However, the reality is much more complex and presents numerous challenges. For example, receiver and transmitter hardware may limit the adoption of those new technologies; the regulator will constrain the transmission power in some locations; radio channels located at higher frequencies will further suffer from radio interference and fading; and poor channel quality will significantly reduce the efficiency of higher-order QAM due to increased transmission error. Therefore, there is a need of a real-world evaluation of 5G deployments and we believe that the following work is the first to comprehensively analyze the contribution of different physical layer techniques on the throughput performance of 5G as compared to 4G.

6.6.1 Measurement Settings and Methodology

The data analyzed in this paper was collected over three measurement campaigns. We conducted an initial campaign in Chicago during December 2022, followed by a campaign in Minneapolis during April-May and November 2023, with both focusing on the downlink and

uplink throughput performance of the three major US operators (ATT, TMO, and VZW). Additionally, a latency-focused campaign specifically targeting the T-Mobile network was conducted in Minneapolis in March 2024. To cover a large area, we conducted data collection while driving. Fig. 6.28 shows the setup of 5G probes and the driving routes: in Chicago, we measured in the downtown Loop area, Midway airport, and the interstate highway; while in Minneapolis, we surveyed the Downtown, Dinkytown, and the beltway. The statistics of the data collected are summarized in Table 6.11.

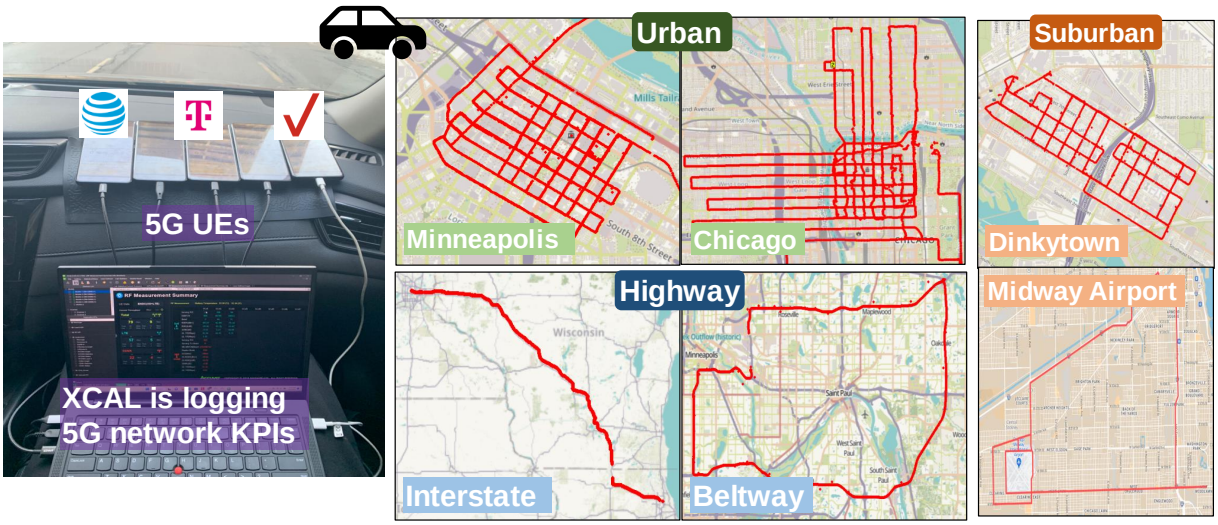


Figure 6.28: Setup of the 5G probes and driving routes of our measurements.

Table 6.11: Statistics of 4G/5G dataset.

Mobile Operators	AT&T, T-Mobile, Verizon
Radio Technologies	4G, 5G
Measurement Venues	Minneapolis, Chicago
Cumulative Data Traces	1200+km; Around 14 hours
XCAL Key Perf. Indicators	PCI-Beam idx; Freq.; SCS; RSRP; RSRQ; CQI; RI; BLER; MCS; #RBs; #MIMO layers; MIMO modes; PHY-layer throughput.

All the data were captured using Samsung Galaxy S22+ (Android 12), which can receive 5G signals in the low-band, mid-band, and mmWave channels. At the time, S22+ was

the only phone capable of capturing the TMO network's inter-band 5G Carrier Aggregation (CA). These state-of-the-art devices allowed us to measure the network's best possible performance. Three S22+ phones were used as user equipment (UE), each equipped with ATT, TMO, and VZW SIMs. All SIMs have unlimited data plans with no throttling of data rates. The S22+ phones were connected to a Lenovo ThinkPad X1 Carbon laptop running Accuver XCAL [8]. The XCAL application collects various 4G and 5G signal parameters by establishing a low-level interface to the modem chipset. To account for differences in parameter sampling intervals, the application processes the data over one-second periods, averaging numerical values and determining the most frequent (mode) for discrete values. Table 6.11 also summarizes the parameters (key performance indicators) collected by XCAL for our analysis. XCAL is also capable of actively creating traffic using iperf [61] tools: we generate full-buffer downlink (iperf server to UE) and uplink (UE to iperf server) transmission to cloud servers in Chicago and Minneapolis, whichever is closest to the measurement location.

6.6.2 Overview of the Observed 4G and 5G Deployments

Table 6.12 compares the 4G and 5G features we observed to the 3GPP specifications in Release 16 and 17. We believe that most deployments today are at most Release 16. Up to 256-QAM is observed in both LTE and NR networks, but not 1024-QAM. We also did not observe improvements in the number of MIMO layers/streams for low- and mid-band 5G over the 4G counterparts, even though 3GPP Rel-16 supports up to 8 layers. On the other hand, there are improvements in maximum channel bandwidth, as new spectrum has been released. This is reflected in the reduced number of aggregated channels: as bandwidth increases, there is less need to increase CA in 5G.

NR has two modes of network deployments: SA which only utilizes the 5G channels and network stack, and NSA which utilizes a combination of 4G and 5G channels and stacks with

Table 6.12: Highlight of features in 3GPP Rel-16 and Rel-17 compared to observed 4G and 5G in our dataset.

Parameters	**Observed 4G**	**Observed 5G**	**Rel-16 5G**	**Rel-17 5G**
Max. Modulation	256-QAM	256-QAM	256-QAM	1024-QAM
Max. MIMO Layer	4	4	8	8
Max. Channel BW (excl. mmWave)	20 MHz	100 MHz	100* MHz	100* MHz
Max. #CA	6	4	16	16

*mmWave channels can be up to 400 MHz wide

4G used as the primary carrier. In all campaigns, ATT and VZW deployed only NSA where NR and LTE channels are aggregated, but we did not observe two NR low- or mid-band channels aggregated in their network. On the other hand, TMO deployed both SA and NSA modes, with the SA mode aggregating up to 3 NR channels for a total bandwidth of 160 MHz. Table 6.13 shows the summary of captured NR and LTE bands/channels in the campaign. NR channels have the prefix "n" and LTE channels have the prefix "b" in the table. All three operators have deployed NR in low- and mid-bands. Notably, ATT-n66 and TMO-n25 are the newest bands detected only in our April-May 2023 campaign and afterward. AT&T and Verizon have also deployed NR mmWave bands (n260 and n261), but they are out of scope for this analysis. Among the NR low- and mid-band channels, all FDD channels are deployed with 15 kHz sub-carrier spacing (SCS) and lower bandwidth (*i.e.*, ATT-n5, ATT-n66, TMO-n25, TMO-n71, VZW-n5), while all TDD bands are deployed with 30 kHz SCS and higher bandwidth (*i.e.*, ATT-n77, TMO-n41, VZW-n77). These deployments suggest that the NR FDD bands are positioned as the "support" bands since the lower bandwidth and frequency result in lower throughput but greater coverage. It should be noted that TMO's mid-band deployment in 2.5 GHz has a 3.4 dB advantage over ATT and VZW in 3.7 GHz: this will be seen in performance results presented later. Most of the deployed LTE channels are FDD, except for the newer b46 (LAA) and b48 (CBRS) which are TDD, and b29 which is a supplementary downlink (SDL) band. The LTE bands are similarly used as the "support" bands to the NR TDD bands when aggregated in the NSA deployments.

Table 6.13: NR and LTE Bands Information

Operator-Band	**Duplex Mode**	**DL Band Freq. (MHz)**	**SCS (kHz)**	**BW (MHz)**
Representative Bands				
ATT-n5	FDD	850	15	10
ATT-n77	TDD	3700	30	40
TMO-n41	TDD	2500	30	40,100
TMO-n71	FDD	600	15	20
VZW-n5	FDD	850	15	10
VZW-n77	TDD	3700	30	60
ATT-b2	FDD	1900	15	20
ATT-b12	FDD	700	15	10
ATT-b46	TDD	5200	15	20
TMO-b12	FDD	700	15	5
TMO-b41	FDD	2500	15	20
TMO-b66	FDD	2100	15	20
VZW-b13	FDD	700	15	10
VZW-b48	TDD	3500	15	10,20
VZW-b66	FDD	2100	15	20
Other Bands				
ATT-n66	FDD	2100	15	5
TMO-n25	FDD	1900	15	20
ATT-b14	FDD	700	15	10
ATT-b29	SDL	700	15	5
ATT-b30	FDD	2300	15	5,10
ATT-b66	FDD	2100	15	5,10,15
TMO-b2	FDD	1900	15	10
TMO-b4	FDD	2100	15	20
TMO-b25	FDD	1900	15	10
TMO-b46	TDD	5200	15	20
TMO-b71	FDD	600	15	5
VZW-b2	FDD	1900	15	10
VZW-b4	FDD	2100	15	20
VZW-b5	FDD	850	15	10
VZW-b46	TDD	5200	15	20

6.6.3 Comparison of Low- and Mid-band Deployment

Preliminary analysis revealed negligible differences between the datasets collected in Chicago and Minneapolis. Consequently, we combined them for the analyses presented in this paper. For brevity, we selected a representative low-band and mid-band channel for each operator with substantial data points, regardless of their primary or secondary cell/channel designation. All mid-band channels are deployed with higher bandwidth compared to low-band channels. Table 6.14 shows the number of data points and deployment parameters of the selected representative bands. Due to PCI reuse, the number of unique Physical Cell Identifiers (PCIs) is calculated separately between Chicago and Minneapolis. For ATT NR, n77 (mid-band) and n5 (low-band) are selected. There are a larger number of data points and unique PCIs on n5, indicating a denser deployment in the low-band: this is in contrast to TMO and VZW which have a higher number of data points and unique PCIs in mid-bands (n41 and n77, respectively) compared to low-bands (n71 and n5, respectively). Moreover, TMO-n41 is very densely deployed with 464 unique PCIs compared to the NR channels from ATT and VZW. As we shall see later, the density of the TMO NR deployment and the lower NR mid-band frequency (2.5 GHz) significantly impact overall superior signal strength, spectral efficiency and throughput compared to ATT and VZW.

Similar to the NR bands, we observe a higher number of data points and unique PCIs on mid-band LTE channels compared to low-band. For ATT, b66 has the largest number of data points for mid-band. However, we chose the second-largest b2 for its wider bandwidth. For TMO, b12 is the only low-band channel beside b71, indicating the very sparse deployment of low-band LTE in TMO: b12 and b71 channels account for 10% of the total LTE data. The proportion of mid-band data in LTE and NR indicates that TMO and VZW have been focusing on mid-band deployments. Lastly, we selected ATT-b46 and VZW-b48 as representatives of the unlicensed/shared mid-band 4G channels. Additionally, TMO-b41 is chosen for comparison with TMO-n41. These bands exhibited fewer data points and unique

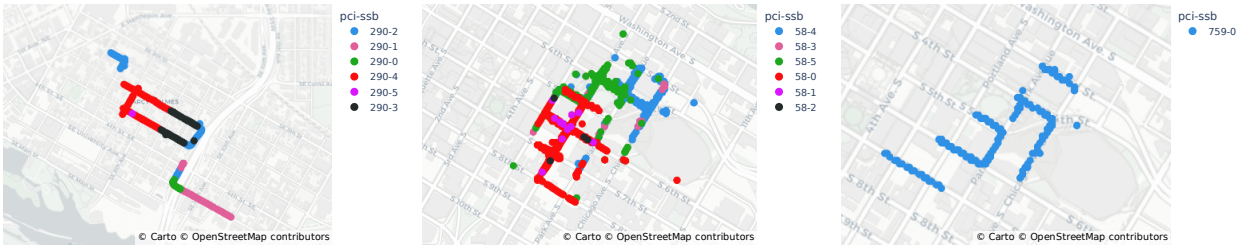
Table 6.14: Comparison of Rep. Bands' Deployment
(Bands in bold are mid-bands.)

Operator-Band	n data	% data	#SSB Inds.	#unique PCI
ATT-n77	8380	34	1,6*	152
ATT-n5	14444	58	1	217
TMO-n41	56606	90	6	464
TMO-n71	1981	3	1	60
VZW-n77	13049	96	1	147
VZW-n5	541	3	1	28
ATT-b2	31480	28	N/A	378
ATT-b46	7090	6	N/A	77
ATT-b12	12690	11	N/A	262
TMO-b66	19334	39	N/A	330
TMO-b41	7400	15	N/A	54
TMO-b12	2645	5	N/A	83
VZW-b66	31742	36	N/A	379
VZW-b48	8762	8	N/A	141
VZW-b13	16906	19	N/A	255

*ATT-n77 has 6 SSB indices in Minneapolis, but only 1 in Chicago.

PCI compared to other channels. This suggests localized deployments using small cells: at least b46 and b48 are limited in the transmit power.

Comparison of low- and mid-band NR beam deployment: Table 6.14 also shows the number of SSB Indices which denotes the number of beams available for each NR channel. We observe only index 0 (*i.e.*, single beam) per PCI for ATT channels in the Chicago campaign. However, we observe 6 SSB indices for ATT-n77 in the later Minneapolis campaign. Fig. 6.29a shows the coverage of the various SSB Indices for ATT-n77, PCI 290, in Dinkytown. Similarly, Fig. 6.29b depicts SSB Indices from 0 to 5 for TMO-n41, PCI 59, in downtown Minneapolis. All low-band NR channels, *i.e.*, n5 and n71, only use one SSB index, and the number of SSB indices did not change between the two campaigns. Unlike TMO and ATT, VZW always uses a single SSB index per PCI for all of its NR channels in both cities. Fig. 6.29c illustrates the coverage of one of VZW's n77 channels in downtown Minneapolis. Since more SSBs/PCI means more beams and hence beamforming gain, VZW with only one beam/PCI suffers from lower signal strength overall and poorer spectral efficiency, as will be shown later.



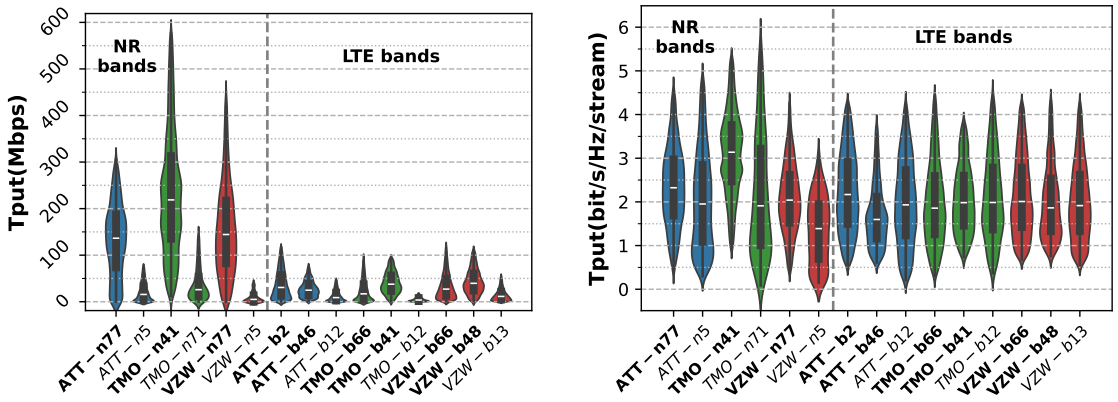
(a) ATT-n77 PCI 290 (b) TMO-n41 PCI 58 (c) VZW-n77 PCI 759

Figure 6.29: PCI-SSB index maps of mid-band channels.

6.6.4 Comparison of Throughput Performance Between Low- and Mid-Band Channels

Downlink throughput: Fig. 6.30a shows the comparison of downlink physical layer throughput between low- and mid-band LTE and NR, as reported by XCAL during all of our driving measurements. We observe a considerably higher downlink throughput on the mid-band NR channels compared to the low-band counterparts. As discussed in a prior section, this can be explained by the wider bandwidths. The highest median throughput of 218 Mbps is attained by TMO-n41 with a combination of two NR channels of 40 and 100 MHz bandwidth. For the LTE bands, we similarly observe higher throughputs on mid-band channels compared to the low-bands. The highest median throughput of 31 Mbps is achieved by ATT-b2 with 20 MHz bandwidth. Since the channels' block error rate (BLER) is similar (omitted for brevity), we conclude that the increase in median throughput in NR is due to the wider bandwidth.

For deeper analysis, we examine channel spectral efficiency. This involves normalizing the throughput of each channel by its bandwidth and number of MIMO layers, allowing us to directly compare how effectively each channel utilizes its allocated spectrum. We define normalized throughput: $Tput_{norm} = Tput_{bps}/(N_{RB} * SCS_{Hz} * 12)/N_{layer}$, where $Tput_{bps}$ is the throughput in bits/second, N_{RB} is the average number of resource blocks (RBs) allocated to the UE over one second, SCS_{Hz} is the subcarrier spacing (SCS) in Hz, and N_{layer} is the number of MIMO layers used. To determine the instantaneous bandwidth usage, we multiply N_{RB} by SCS_{Hz} and 12, given that there are 12 subcarriers in each RB.



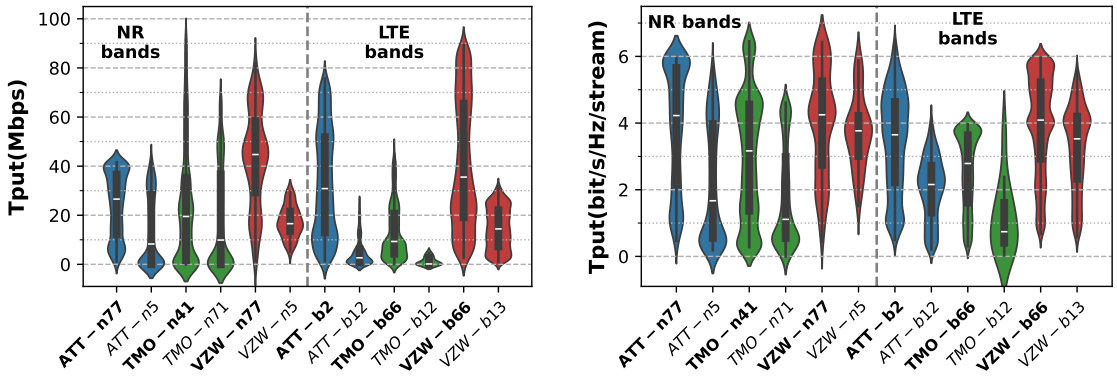
(a) Throughput (b) Normalized throughput

Figure 6.30: DL throughput comparison of NR and LTE in low-bands (normal) and mid-bands (bolded)

Since we use RB to normalize throughput, the difference between TDD configurations in the mid-band channels should not make a difference. However, we observe that all operators in the mid-band channels use the same TDD configuration of 7 slots for DL and 2 slots for UL, with a slot length of 0.5 ms. Note that when normalizing LTE throughput, RI is used due to the lack of the MIMO layer number KPI in LTE. This is viable since we observe a Pearson correlation of 0.95 between the RI and MIMO layers in our NR data, which is expected since RI is a part of Channel State Information (CSI) feedback to decide the number of MIMO layers.

As computed above, Fig. 6.30b compares the normalized throughput (spectral efficiency) of NR and LTE channels. VZW-n5 exhibits the lowest median throughput, while TMO-n41 achieves the highest (3.14 bit/s/Hz/stream). Other channels fall between 1.9 and 2.3 bit/s/Hz/stream, analogous to the theoretical capacity of uncoded QPSK of 2 bit/s/Hz. Since we previously observed a higher throughput from channels with higher bandwidth, this strongly indicates that the increase in throughput from LTE to NR can be attributed primarily to the wider bandwidth and number of MIMO layers. The exception being TMO-n41, which has a much higher spectral efficiency due to its dense deployment (compared to

both ATT and VZW) and larger number of beams (compared to VZW), both of which lead to improved overall signal strength and hence spectral efficiency. Furthermore, the stark contrast with TMO-b41, an LTE channel in the same frequency band, confirms that TMO-n41's superior performance stems from its denser deployment. Finally, we observe a lower normalized throughput in ATT-b46 compared to VZW-b48, where both are shared frequencies. In the next sections, we will further analyze the contribution of RSRP, modulation, and number of MIMO layers to the normalized throughput.



(a) Throughput

(b) Normalized throughput

Figure 6.31: UL throughput comparison of NR and LTE in low-bands (normal) and mid-bands (bolded)

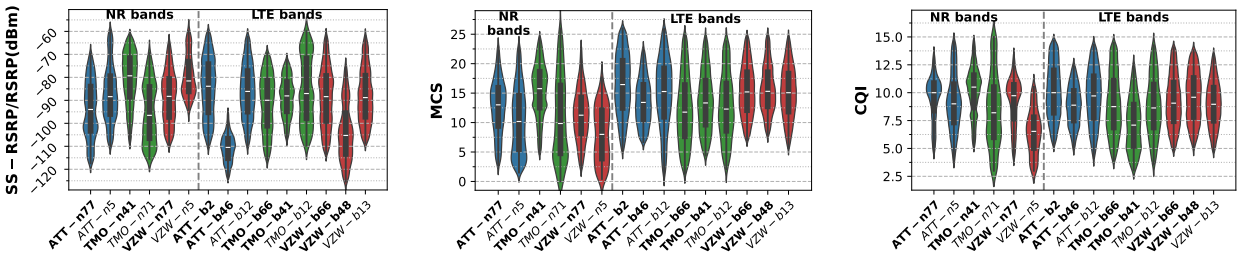
Uplink throughput: We omit the complete uplink throughput analysis due to limited new insights. Firstly, no uplink channel aggregation was observed within either LTE or NR deployments, even though aggregation is possible between one LTE and one NR channel in the NR-NSA deployment. Secondly, our data lacked information on the number of uplink MIMO layers parameter, and the NR RI did not correlate with the number of NR layers. Assuming LTE uses 1 stream (based on 97% of NR data using 1 stream), we see in Fig. 6.31a that overall uplink throughputs are lower than their downlink counterparts for all representative bands due to the fewer streams. All mid-band channels perform better than the low-band counterparts due to higher bandwidth, while all NR channels show marginal improvements over their LTE counterparts. We did not observe ATT-b46, TMO-b41, and VZW-b48 uti-

lized for uplink transmissions. Fig. 6.31b shows the normalized uplink throughput with mid-band channels perform better than the low-band counterparts. When combining all representative LTE and NR channels, we observe a median normalized uplink throughput of 3.4 bit/s/Hz/stream, which is higher compared to downlink. The lower number of uplink layers likely improves stream robustness against fading and errors.

6.6.5 Normalized DL Throughput Impact Factor Analysis

Contribution of RSRP, MCS, and CQI to normalized DL throughput: Fig. 6.32a shows a comparative analysis of the Synchronization Signal RSRP (SS-RSRP) on NR channels, and RSRP on LTE channels. Both ATT and VZW exhibit higher SS-RSRP values on their low-bands in comparison to their mid-band counterparts: this is due to better propagation characteristics of the low-bands. However, mid-band TMO-n41 displays higher SS-RSRP (median of -79 dBm) compared to its low-band counterpart, n71, which indicates a denser NR deployment to overcome the propagation loss at the mid-bands. Furthermore, TMO consistently displays RSRP values $\sim$12 dB higher than other operators in all of our NR data: this is due to a combination of dense deployment, multiple beams/PCI, and lower frequency. In LTE, we observe the similarity of RSRP distribution between the channels. The highest median RSRP of -83 dBm is achieved by ATT-b2, which is reflected in the normalized throughput: the highest median downlink throughput of 2.18 bit/s/Hz/stream over all LTE channels. On the other hand, ATT-b46 and VZW-b48 show lower RSRP due to the limitations of transmit power. Between NR and LTE, TMO-n41 stands out due to its denser deployment and higher number of beams.

Fig. 6.32b shows the distribution of allocated downlink MCS, which correlates well with the distribution of normalized downlink throughput in LTE and NR. For instance, the best and worst median MCS in NR are achieved by TMO-n41 and VZW-n5, respectively, which correspond to the best and worst median normalized downlink throughput. This is expected



(a) SS-RSRP/RSRP (b) DL MCS (c) CQI

Figure 6.32: Comparison of RSRP, MCS, and CQI of NR and LTE in low-bands (normal) and mid-bands (bolded).

since higher MCS delivers higher spectral efficiency but can only be used in good signal conditions. Further, we found RRC messages ("pdsch-Config > mcs-Table := qam256" in NR and "cqi-ReportConfig > altCQI-Table-r12 := all subframes" in LTE) which indicate that both LTE and NR used the MCS Table 2 as described in Table 5.1.3.1-2 of [4], making comparison feasible. We observe a lower median of MCS in NR channels compared to LTE, except for TMO-n41, again due to the excellent channel condition guaranteed by its denser deployment.

We further compare the CQI, which indicates channel conditions from the UE's perspective. Fig. 6.32c illustrates the comparison of CQI between the representative LTE and NR channels. Since the BS uses CQI to decide the MCS selection, the distribution of CQI aligns with its respective MCS values: the highest median CQI is attained by TMO-n41, similar to its median MCS, and vice versa with VZW-n5. On LTE, we also observe a similar distribution of LTE CQI with MCS. This further shows that normalized throughput is mainly influenced by the overall channel condition reported by UE, rather than just RSRP. However, since we cannot ascertain whether the CQI table used by NR and LTE networks are the same, we cannot make a direct comparison between them.

Comparison of DL modulation modes: We extend our analysis to examine the proportional utilization of each modulation mode, drawing a comparison with normalized throughput. It's worth noting that these modulation modes align with MCS indices, as each index

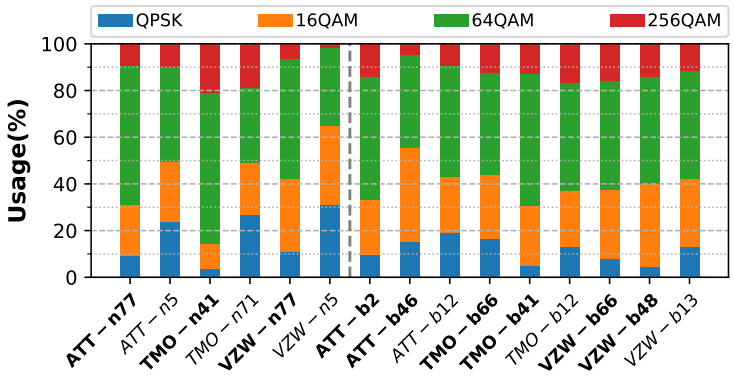


Figure 6.33: Proportional usage of modulation modes of NR and LTE in low-bands (normal) and mid-bands (bolded).

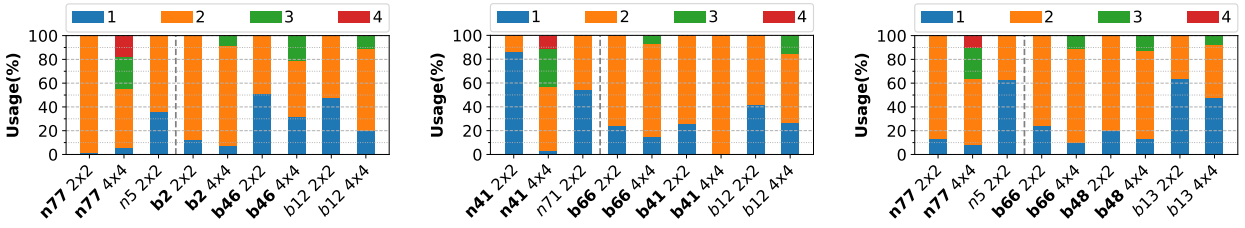
corresponds to a specific modulation mode. Fig. 6.33 shows the modulation modes used for the 12 representative low- and mid-band channels as defined in a previous section. Only modulation modes from QPSK to 256-QAM are observed in our campaign. TMO-n41 shows higher usage of 64-QAM and 256-QAM modulation, corresponding to the channel's high normalized downlink throughput. It is worth noting that the normalized throughput of TMO-n41 does not reach the theoretical capacity of 64-QAM due to MCS's code rate. Conversely, the VZW-n5 channel uses a higher proportion of QPSK and 16-QAM modes, which also explains the low normalized throughput of this channel. For LTE, ATT-b2 mainly uses a combination of 64-QAM and 256-QAM modes, and this results in the highest normalized downlink throughput performance among the LTE channels. Moreover, the resemblance in modulation usage among the other LTE channels corresponds to the similarity in their normalized throughput.

Comparing the modulation modes between the NR and LTE channels, we do not observe a significant improvement, *i.e.*, no indication that higher modulation is more available in NR compared to LTE, except for the TMO NR channels n41 and n71, which use 256-QAM more often than the other carriers. This is due to the fact that TMO exhibits better signal conditions in general, which confirms that spectral efficiency improvements are only possible if the overall signal strength improves, through a combination of dense deployments and

usage of more beams.

6.6.6 Comparison of MIMO Performance in NR and LTE

Analysis of MIMO performance in terms of RI and MIMO modes: In both LTE and NR, RI is the MIMO channel rank as calculated by the UE and transmitted back to the BS for MIMO layer decision. Fig. 6.34 shows the comparison of RI for the three operators on the representative low- and mid-band channels selected in a previous section. The data for each channel is categorized by MIMO modes (*i.e.*, 2x2, 4x4) as reported by XCAL. First, we observe that the NR low-band channels on all operators do not utilize 4x4 MIMO modes, while the LTE counterparts do. Fig. 6.34a compares the RI value between NR and LTE channels of ATT. We observe an RI value of 2 being the most common in all channels, even when 4x4 MIMO mode is available. For instance, less than 20% of data on ATT-n77 reported an RI of 4 even when the 4x4 mode is used, while RI 4 is not seen in the corresponding b2 and b12 channels. Fig. 6.34b similarly shows an RI value of 2 being most common for TMO, with the exception of n41 and n71 using 2x2 mode, where the majority of the data had an RI of 1. Fig. 6.34c also demonstrates an RI value of 2 being most used for VZW, except for n5 with 2x2 and b13 with both 2x2 and 4x4 modes.



(a) ATT (b) TMO (c) VZW

Figure 6.34: RI value for the operators, channels, and MIMO modes.

This result is very significant since it indicates that even though higher-order MIMO modes may be implemented, the physical channel rank may not support all available MIMO layers. This suggests that increasing MIMO order in future generations may not be the best

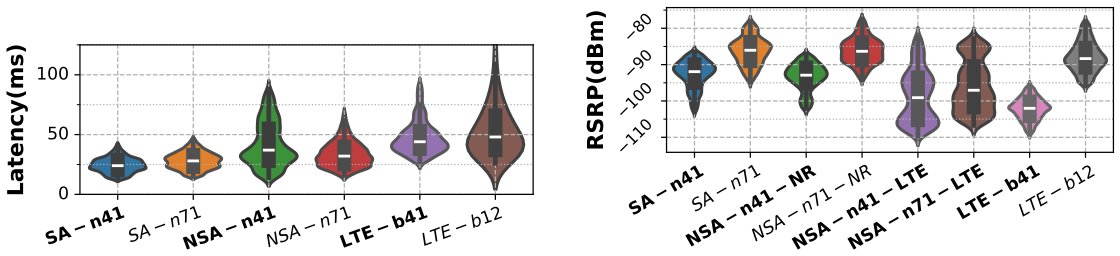
way to improve throughput in the real-world. In fact, TMO-n41 has the best throughput performance, but it achieves this with fewer MIMO layers on average compared to ATT-n77 and VZW-n77, which are all mid-band NR channels.

Analysis of MU-MIMO in NR: While operators claim to have implemented 5G MU-MIMO in test settings [11, 114], its widespread deployment remains uncertain. To address this question, we utilize the Precoding Matrix Indicator (PMI) which is a part of the CSI feedback to the BS. Moreover, it conveys information about the precoding matrix that should be used in the downlink transmission. Utilizing XCAL, we collected PMI values from all the UEs and observed PMI with indices: i(1;1), i(1;2), i(1;3), and i(2). This indicates the usage of Type 1-Single Panel codebook with 2–4 MIMO layers [4]. Further, we analyzed the RRC messages captured in all of our UEs and found "mimo-Parameters > codebookParameters > typeI > singlePanel > mode := mode1" message which further indicates the usage of the above codebook. Type 1 codebooks are used for Single User-MIMO (SU-MIMO) and only use a single beam to calculate CSI feedback [86]. Lastly, we did a stationary experiment in Minneapolis in November 2023, where we initiated downlink traffic with up to 4 UEs on the same operator, observing their exact RB allocation in the radio frame. Our hypothesis is that when MU-MIMO is enabled, at least one RB will be allocated in the same slot to two different UEs. We did not observe this in our data.

6.6.7 Comparison of Latency Performance in TMO Networks

We conducted a focused latency measurement in Minneapolis during March 2024, comparing the LTE and NR performance. Specifically, we focus on TMO, which is the only operator that has deployed NR in both SA and NSA modes. Similar to our throughput measurement campaigns, we collected data while driving, using 6×S22+. Using XCAL, we collected signal parameters and round-trip latency results using the included ping tool. We defined two ping targets: Google's cloud DNS server (8.8.8.8) and AWS Local Zone (server located in the

same city as the end-user) [17]. Additionally, we utilized XCAL to limit the phones to the following networks and bands: SA-n71, SA-n41, NSA-n71, NSA-n41, LTE-b14 and LTE-b41. This resulted in 12 distinct data categories, each containing an average of 1,774 data points (*i.e.*, ∼30 minutes of data collection per category).



(a) Latency performance

(b) SS-RSRP/RSRP

Figure 6.35: Comparison of latency performance and RSRP in TMO low-bands (normal) and mid-bands (bolded)

We observe higher latency to Google DNS compared to Local Zone, which is an expected behavior. Hence, Fig. 6.35a shows the combined latency results (ping to Google and Local Zone) across all bands for brevity. Among the network types, SA bands exhibit the best latency performance, likely due to their simpler architecture. NSA bands, which combine NR and LTE, achieve the next best results. Fig. 6.35b also combines the RSRP measured for the Google and Local Zone measurements. Since both NSA-n71 and NSA-n41 utilize either b2 or b66 as the anchor LTE band, we separate those categories with "LTE" or "NR" suffixes to indicate if the RSRP is from the anchor LTE or the secondary NR channel. As expected, we observe higher RSRP on lower-band channels. Interestingly, the LTE anchor channels in NSA bands exhibit a wider spread of RSRP values (-110 to -80 dBm). This lower and more variable RSRP in the LTE channels, combined with the overhead of using both NR and LTE, likely contributes to the slightly higher latency of NSA compared to SA bands. However, both SA and NSA offer significant latency improvements over traditional LTE.

6.7 Summary and List of Accomplishments

It is clear from all of the measurements and experiments conducted in multiple cities, we can draw the following conclusions:

1. Operator's choice of 4G primary channel is primarily determined by RSRP and RSRQ, as per our measurements.

2. 4G with the LAA and CBRS bands aggregation can deliver aggregated throughput in the mid-band that is comparable or even higher than mid-band 5G. However, there will be coexistence issues in LAA and synchronization issues in TDD deployment of CBRS, as both deployments continue to roll out.

3. We confirmed the dense deployments of 5G mmWave in downtown Chicago with significantly higher data rate compared to 4G+LAA/CBRS. We observed that higher channel aggregation and wider Tx beam contributed to an increase in median throughput. However, the throughput gain is reduced at a distance compared to narrower Tx beam which performs consistently at all distances.

4. While 5G mmWave offers the potential for higher performance, it is important to note that this is not guaranteed everywhere. Limitations such as distance, body blockage, thermal throttling, and obstructions like foliage and buildings can significantly degrade mmWave's performance.

5. We investigated beam selection mechanisms in 5G mmWave across open fields and urban canyons environments. In open fields, operators can generally select the optimal beam due to overlapping base station coverage. However, the complex signal environment in urban canyons often leads to the selection of sub-optimal beams, resulting in an average signal strength reduction of 3.6 dBm. This highlights the challenges of beam

selection in urban mmWave deployments and the associated potential for performance limitations.

6. We performed a comparative analysis of throughput over the representative low- and mid-band channels in NR and LTE. As expected, the 5G mid-band channels perform exceedingly well in downlink and uplink compared to other 5G and 4G channels. However, we further normalize the throughput and demonstrate that the higher channel bandwidth, dense deployments, and the use of more beams are a major factor in the increased throughput, rather than new 5G features.

7. The contribution of various signal parameters such as RSRP, MCS, and CQI to the normalized 4G and 5G throughputs are further analyzed. We demonstrated that these parameters in 5G perform similarly to their 4G counterparts. We also note the absence of 1024-QAM modulation, introduced in the latest 3GPP Release 17.

8. A comparative analysis of the RI value shows a marginal increase in 5G MIMO performance compared to 4G in terms of the actual channel rank and number of layers that the physical channel can support. We also note that Multi-User MIMO (MU-MIMO) has not yet been deployed in the cities we studied.

9. Since T-Mobile is the only operator with widely deployed NR-SA, we compared the latency performance of NR-SA, NR-NSA, and LTE. Mid-band NR-SA demonstrates the best latency performance due to the combination of lower signaling overhead (compared to NR-NSA) and denser mid-band deployments.

The following papers has been published in the topic of 5G cellular measurements:

- Muhammad Iqbal Rochman et al. "A Comparison Study of Cellular Deployments in Chicago and Miami Using Apps on Smartphones". In: *Proceedings of the 15th ACM Workshop on Wireless Network Testbeds, Experimental Evaluation & CHaracterization (WiNTECH'21)*. New Orleans, LA, USA, 2022, 61–68.

- Arvind Narayanan et al. "A Comparative Measurement Study of Commercial 5G mmWave Deployments". In: *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. 2022, pp. 800–809.

- Muhammad Iqbal Rochman et al. "Outdoor-to-Indoor Performance Analysis of a Commercial Deployment of 5G mmWave". In: *IEEE Future Network World Forum Workshop (FNWF).* 2022.

- Muhammad Iqbal Rochman et al. "Impact of Device Thermal Performance on 5G mmWave Communication Systems". In: *IEEE Communications Quality and Reliability Workshop (CQR).* 2022.

- Muhammad Iqbal Rochman et al. "A Comprehensive Analysis of The Coverage and Performance of 4G and 5G deployments". In: *Computer Networks 237, 110060.* 2023.

- Muhammad Iqbal Rochman et al. "A Comprehensive Real-World Evaluation of 5G Improvements over 4G in Low-and Mid-Bands". In: *IEEE Dynamic Spectrum Access Networks (DySPAN).* 2024.

CHAPTER 7

CELLULAR COEXISTENCE IN THE 3 GHZ SPECTRUM

7.1 Overview and Related Works

The increased demands on cellular traffic has led to increasing swathes of mid-band frequencies being allocated for 5G services. In the US, the three most recent allocations in the mid-band are the 3.7 - 3.98 GHz (C-Band) [65], the immediately adjacent 3.55 - 3.7 GHz (Citizens Broadband Radio Services, or CBRS) [62] and the latest allocation of 3.45 - 3.55 GHz (AMBIT) for cellular services [40] as shown in Fig. 7.1.

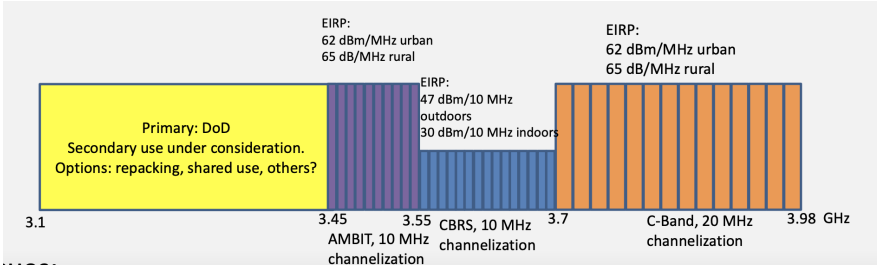


Figure 7.1: Spectrum Chart from 3.1 to 3.9 GHz

Allocated between C-Band and AMBIT, the CBRS band prioritizes incumbent Navy radars (Tier 1) with full spectrum access. Tier 2 consists of licensed users (PAL) with access to specific 10 MHz channels (3.55-3.65 GHz). Finally, Tier 3 (GAA) allows unlicensed users opportunistic access to any unused channels. To ensure coexistence, all users communicate with the SAS for access permission. Additionally, Tier 2 and 3 users have limited transmit power (30 dBm/10 MHz indoors, 47 dBm/10 MHz outdoors) to minimize interference with incumbents. This is significantly lower than power levels allowed in adjacent C-Band and AMBIT. This, combined with the absence of guard bands, creates the potential for adjacent channel interference (ACI), especially with the deployment of TDD systems. Furthermore, the CBRS spectrum is increasingly utilized for private 4G/5G networks in various public settings, from manufacturing to smart homes and stadiums [84]. Additionally, major carriers

like Verizon leverage CBRS to supplement their licensed spectrum via techniques like Carrier Aggregation (CA) and Dual Connectivity (DC). This growth in CBRS adoption creates scenarios where users within the same area, regardless of their provider or network type (private or public), may experience co-channel interference (CCI).

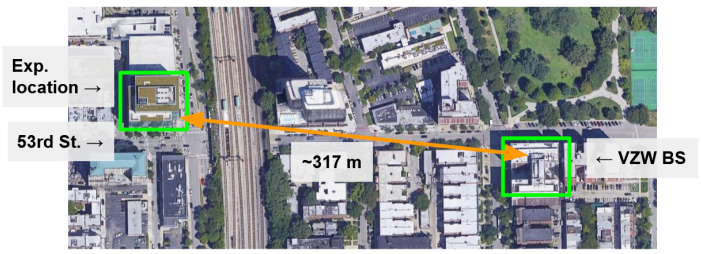
The above interference scenarios in the 3 GHz spectrum of cellular deployments is not one that has been studied comprehensively in the literature. A few papers discuss similar problems and propose reducing adjacent channel interference by better filtering [113, 12]. We believe that the following results are the first to show the effect of ACI and CCI in a real world environment.

7.2 Adjacent Channel Interference between CBRS and C-Band

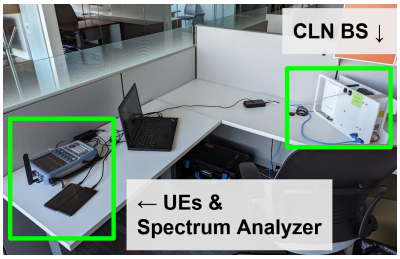
7.2.1 Deployment Overview, Measurement Tools, and Methodology

We leverage an outdoor C-band BS deployed on top of a 10-storey building at the intersection of 53rd and E Hyde Park Ave in Chicago. In order to study adjacent channel interference between CBRS and this C-band deployment, we deployed a Celona CBSD (CBRS device, or CBRS base station) indoors on the 9th floor of a UChicago building at 5235 S Harper Court, where the C-band transmission can be received indoors with sufficient signal strength. The set-up is shown in Figs. 7.2a and 7.2b. The CBSD is deployed in a cubicle facing the window with LOS to C-Band. We did our experiments over August-September 2022 and December 2022, with the additional 20 MHz guard band experiments over March 2023. Table 7.1 summarizes the parameters of both systems. The two operators are labeled as: VZW (**Verizon**), with the C-band deployment, and CLN, the private CBRS network with its CBSD/BS connected to the University of Chicago backhaul.

Overview of Deployments: The VZW deployment is a 5G NR non-standalone (NSA) configuration with a primary LTE Frequency Division Duplex (FDD) channel in band 66 (DL: 2.11 -



(a) Map of C-band deployment and experiment location.



(b) Experiment setup.

Figure 7.2: Experiment map and setup.

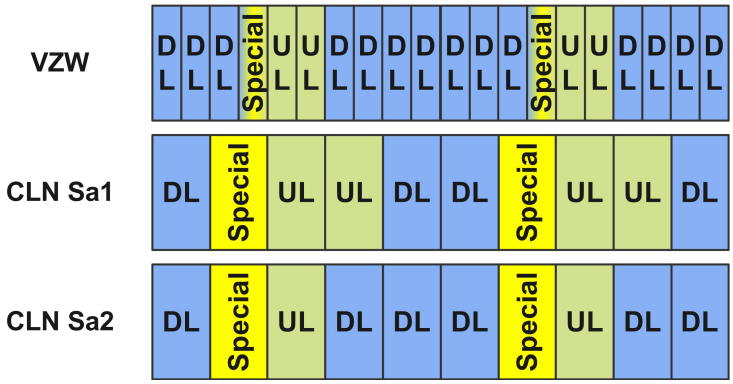


Figure 7.3: Comparison of TDD configuration.

2.13 GHz, UL: 1.71 - 1.73 GHz), and a secondary NR TDD channel in band n77/C-band (3.7 - 3.76 GHz) with 30 kHz sub-carrier spacing. In our throughput analysis, we only consider data transmitted over the 60 MHz C-band and omit the LTE data. The TDD configuration used by VZW in C-band is shown in Fig. 7.3: 7 slots for DL and 2 slots for UL, with a slot length of 0.5 ms. Additionally, the "Special" slot is defined to allow greater freedom for resource allocation: 6 symbols are reserved for DL, 4 symbols for UL, and 4 symbols for messaging. In total, there are 7.4 slots reserved for DL and 2.2 slots reserved for UL.

To evaluate potential adjacent channel interference, the CLN CBRS was deployed on the immediately lower adjacent channel, 3.68 - 3.7 GHz using the General Availability Access (GAA) tier of CBRS. As a comparison, we also deployed it on 3.66 - 3.68 GHz, essentially adding a 20 MHz guard band between the CBRS and C-band channels. Since the CBSD was under our control, we varied the TDD configuration of the CBSD between **Sa1** and **Sa2**

Table 7.1: Experiment parameters

Parameter	**Value**	
Operators	VZW	CLN
Operating band	C-band	CBRS GAA
Radio tech.	5G	4G
Center freq.	3.73 GHz	3.69 and 3.67 GHz
Bandwidth	60 MHz	20 MHz
TDD config. scenarios	7.4 DL + 2.2 UL	Sa1: 4 DL + 4 UL, Sa2: 6 DL + 2 UL
TDD periodicity	5 ms	10 ms
BS deployment	Outdoor	Indoor
Max. BS Power	79 dBm[a]	23 dBm
UE	Samsung S22+	Samsung S22+
Traffics scenarios	DL, UL	ping, ping + DL, ping + UL
ping target	N/A	CLN edge server
DL/UL server	iperf01.uchicago.edu	CLN edge server
DL/UL parameters	target bandwidth 2 Gbps, TCP buffer size 8196 bytes, 10 parallel conns., 500 packets burst	
UE location scenarios	VZW @ A, CLN @ A; VZW @ B, CLN @ B; VZW @ B, CLN @ A, see Fig. 7.4	
Exp. run time	10 minutes per combination of scenarios	
Total exp. time	660 minutes	
Time of exp.	Between 1 am - 6 am	

[a]We assume the maximum TX power based on the 62 dBm/MHz limit.

where **Sa1** uses 4 DL and 4 UL subframes, and **Sa2** uses 6 DL and 2 UL subframes per radio frame with a subframe length of 1 ms, as shown in Fig. 7.3. For both configurations, the "Special" subframe contains 10 symbols reserved for DL, 2 for UL, and 2 for messaging. The difference of DL/UL allocation between CLN (4G: per subframe) and VZW (5G: per slot) may resulted in synchronization issues. Since the CBSD was 4G, the TDD configurations could not be exactly matched to 5G in C-band.

Measurement Tools and Methodology: Two Samsung S22+ phones (running Android 12) are used as user equipment (UEs), one with a CLN SIM and the other with a VZW SIM. Both SIMs have unlimited data plans with no throttling of data rates. We also use a spectrum analyzer (R&S Spectrum Rider FPH) to measure power over the CBRS and

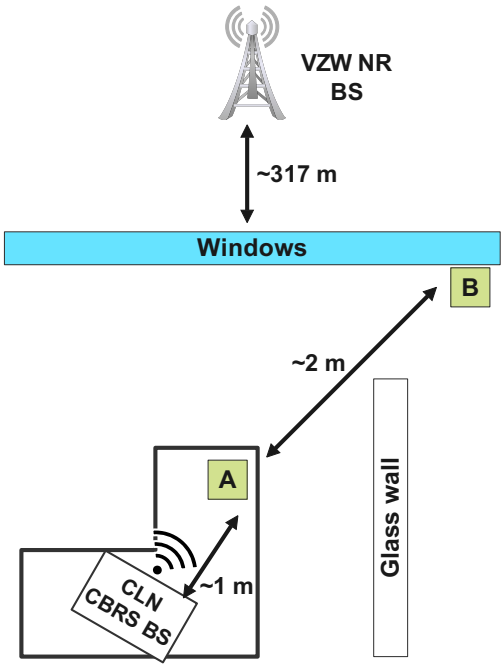


Figure 7.4: Experiment set-up.

C-band channels. Fig. 7.4 is a schematic of the deployment scenario. The CBSD is placed on top of a desk in the cubicle and UEs are deployed in two locations, A and B. Location A is ∼1 m from the CBSD, while location B is on top of a desk in an office ∼3 m from the CBSD. The spectrum analyzer is always at location A. Both locations are LOS to the VZW BS. We define three measurement scenarios: (1) both UEs at A representing the best condition for CLN UE (*i.e.*, the closest to CBSD), (2) both UEs at B representing the best condition for VZW UE (*i.e.*, indoor location closest to VZW BS), and (3) CLN UE at A and VZW UE at B representing the best condition for both UEs to their respective BSs.

Signal measurements are obtained from the Android phones using a commercial measurement app called Qualipoc [100] which utilizes the UE's root privilege to establish a low-level interface with the *Qualcomm Diag* utility thus enabling extraction of detailed signal parameters such as primary and secondary channel's RSRP, RSRQ, SINR, MCS, Resource Block (RB) allocation, block error rate (BLER), TDD Config, and physical layer throughput. The DL and UL throughput values mentioned in this paper are physical layer throughput values

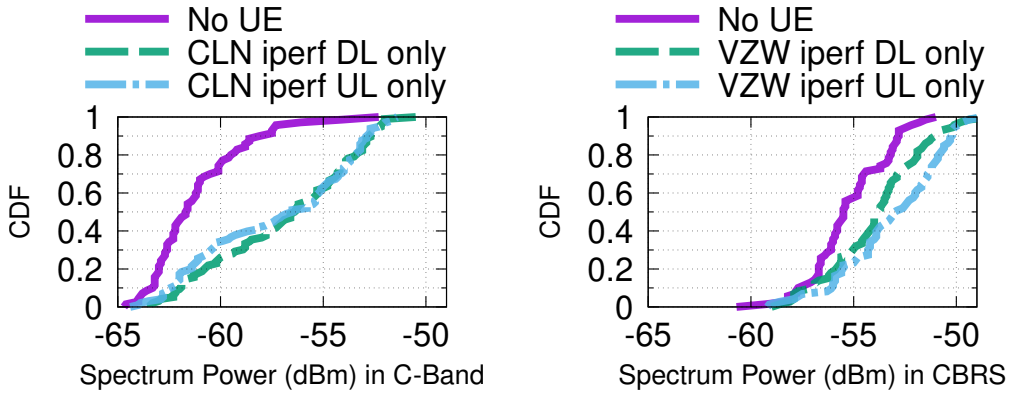
extracted from Qualipoc. Qualipoc is also capable of actively creating traffic using iperf [61] and ping tools.

Experiments were run for 10 minutes per scenario, with a total experiment time of 660 minutes. The experiments were conducted between 1 am and 6 am to reduce the impact on performance due to the presence of other VZW users. Two data transmission scenarios were defined using iperf: DL and UL which generate full-buffer downlink (iperf server to UE) and uplink (UE to iperf server) transmission, respectively, with parameters defined in Table 7.1. Table 7.1 also defines different iperf target servers for each operator, since there is a need to separate the backhaul used for each operator: the VZW UE uses the UChicago iperf server (*iperf01.uchicago.edu*), while the CLN UE uses an edge server as its target server. The edge server is connected directly to the CLN BS, so the CLN throughput closely reflects the wireless link performance, while VZW throughput includes the wireless + backhaul performance. Due to this difference, we do not compare the performance between the operators, rather we compare the relative performance for each operator between the two cases: (i) "single" case where one operator is active while the other is idle, and (ii) "coexistence" case where both operators are active concurrently.

Additionally, we also measure the performance of CLN for latency-sensitive applications using ping traffic (64 kbyte ping packets every 10 ms over 10 minutes per scenario) to a separate edge server. The latency metric collected by the ping tool is defined as the round trip time between UE and the ping target. To further emulate an intensive low-latency application, we implemented MicroSlicing [20], a network slicing technology that allows precise control over end-to-end resource and service allocation based on specific Quality of Service (QoS) metrics for different applications and devices. Network administrators can use the Celona Orchestrator or the developer APIs to customize network settings on a device or application specific basis. The orchestrator offers control and adjustments for numerous service types, including data throughput, quality, latency, reliability, and network access

policies among others. This enables users to set aside guaranteed portions of the network dedicated to the smooth functioning of the respective device and application. The platform also records application-specific service level agreements (SLA) and key performance indicators (KPI) across all devices, granting complete user visibility of device performance across the spectrum. In this experiment, MicroSlicing based resource allocation policy is specified to prioritize ping over DL and UL traffic.

7.2.2 Experimental Results



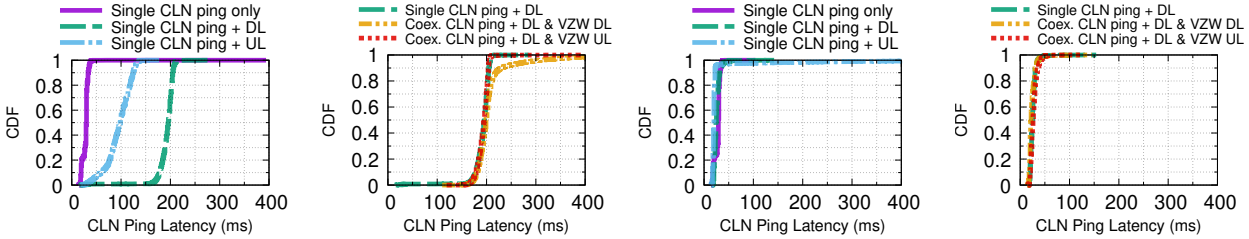
(a) C-band power due to leakage from CLN.

(b) CBRS power due to leakage from VZW.

Figure 7.5: Spectrum Analyzer measurements of mutual OOB leakage between CBRS and C-band.

Out-of-band (OOB) interference quantified by spectrum analyzer measurements: Fig. 7.5 shows the spectrum analyzer measurements of OOB interference due to transmissions to and from the UEs. These spectrum measurements are done with all UEs and the spectrum analyzer in close proximity to each other in location A. The spectrum analyzer measures the power on the 3.68-3.7 GHz CBRS channel and the 3.7-3.76 GHz C-band channel in the following scenarios: (i) both UEs are turned off, (ii) only the CLN UE transmits DL/ UL, and (iii) only the VZW UE transmits DL/ UL. We also vary CLN TDD configurations between Sa1 and Sa2. Fig. 7.5a shows the OOB effect on C-band channel due to CLN

transmission on the CBRS channel using both TDD configurations, *i.e.*, there is clearly an increase of power observed in the adjacent C-band channel compared to when both UEs are turned off. Similarly, Fig. 7.5b shows the effect of VZW transmission in C-band on the CBRS channel, again demonstrating a power increase. This initial power analysis clearly demonstrates the potential of OOB interference on both operators. In the following subsections, we demonstrate the impact of increased OOB interference to ping latency and DL throughput performance at the UEs.



(a) Single cases with varying traffics, no MicroSlicing

(b) Single *vs.* Coex. cases on ping + DL, no MicroSlicing

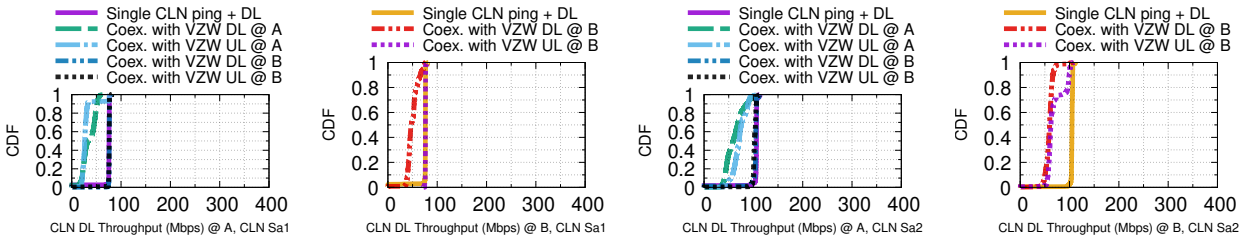
(c) Single cases with varying traffics and MicroSlicing

(d) Single *vs.* Coex. cases on ping + DL, with MicroSlicing

Figure 7.6: Ping latency performance of CLN.

Latency performance of CLN: Latency performance of CBRS with and without adjacent channel transmissions was evaluated only in location A, with CLN TDD configuration set to Sa1. Fig. 7.6a shows the "single" case, *i.e.*, no interference from the VZW UE, without MicroSlicing and Fig. 7.6c shows the performance in the same scenario but with MicroSlicing. Similarly, Fig. 7.6b shows the "coex" case, *i.e.*, interference from the VZW UE, without MicroSlicing and Fig. 7.6d shows the performance in the same scenario but with MicroSlicing. In both cases, overall, we observe less difference in latency when ping traffic is transmitted along with DL and UL when MicroSlicing is used compared to no MicroSlicing. In particular, we observe increased latency on 20% of the data, when VZW is using DL traffic without MicroSlicing while there is no impact of OOB interference to CLN's latency performance when it is using MicroSlicing (Fig. 7.6d). The reduction of the effect of the OOB interference can be explained by the MicroSlicing policy, which assigns a higher priority to ping packets

thus ensuring timely packet arrival, even under OOB interference.

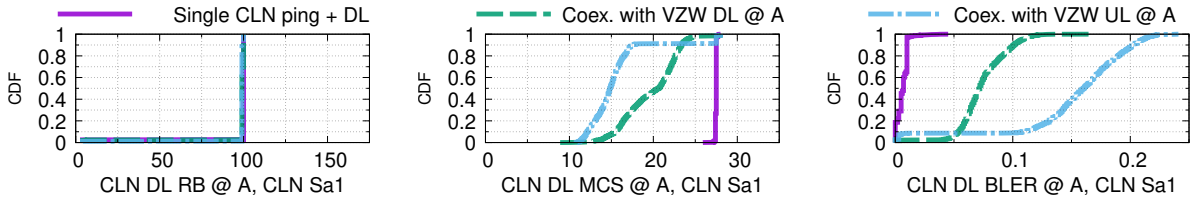


(a) CLN DL tput. @ A, CLN Sa1 (b) CLN DL tput. @ B, CLN Sa1 (c) CLN DL tput. @ A, CLN Sa2 (d) CLN DL tput. @ B, CLN Sa2

Figure 7.7: Coexistence performance in terms of CLN DL throughput under varying CLN TDD configurations.

Impact of VZW's OOB interference on CLN's throughput: Fig. 7.7 shows the coexistence performance of CLN in terms of physical layer DL throughput with varying CLN TDD configurations. Due to page limitations, we omit the UL throughput results which did not demonstrate any effect of adjacent channel interference. Only ping + DL traffic is analyzed as there is **no difference** between the DL only and ping + DL, which is expected since the flow of ping packets are also counted in the throughput metric. Figs. 7.7a and 7.7b show the effect of OOB interference on CLN DL throughput, using Sa1 configuration, at location A and B, respectively. Firstly, we observe no impact of coexistence when CLN UE is at A and VZW UE is at B, *i.e.*, the effect of OOB interference is only observed when the UEs are close to each other. When CLN is using Sa1, we observe the highest throughput degradation when CLN ping + DL @ A and VZW UL @ A coexist: 60 % reduction of CLN DL throughput compared to the "single" case. When the VZW UE is transmitting UL @ A, the proximity to the CLN CBSD causes a large throughput reduction which can be explained by the TDD configuration as shown on Fig. 7.3: in the worst case, CLN's DL capability is reduced to half due to the overlap with two of VZW's UL slots. This effect is not observed at B due to the greater distance to the CBSD. Only DL traffic from VZW at B affects CLN which is also at B. Similarly when CLN is using Sa2, the DL throughput degradation is observed on Figs. 7.7c and 7.7d. The greatest throughput degradation in this case is between CLN ping

+ DL @ B and VZW DL @ B, which is 43% reduction from the single case. Additionally, VZW UL @ B affects CLN DL throughput on Sa2 (an effect not observed on Sa1), which is possibly due to the higher number of DL subframes in the Sa2 configuration which leads to a higher probability of overlap with VZW UL slots.

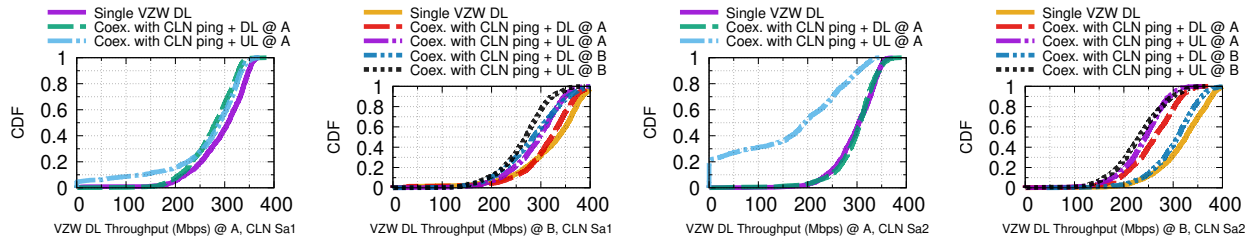


(a) CLN DL RB (b) CLN DL MCS (c) CLN DL BLER

Figure 7.8: Representative comparison of DL RB, MCS, and BLER for CLN @ A, on CLN Sa1.

To further demonstrate the effect of OOB interference, we correlate RB, MCS, and BLER values when CLN is using ping + DL traffic as shown in Fig. 7.8. We could not correlate OOB interference to the captured RSRP and RSRQ values: while the RSRP and RSRQ are well-defined by 3GPP, we cannot confirm the correctness of its implementation inside the modem. A representative coexistence case of CLN ping + DL @ A and VZW DL @ A on CLN Sa1 is chosen for analysis, but the same conclusion is observed in other cases. First, Fig. 7.8a shows the full RB allocation to the CLN UE in all cases, since the CLN UE is the only one connected to the CBSD. On the other hand, Figs. 7.8b and 7.8c respectively show a degradation of MCS allocation and increase in BLER under coexistence, leading to a reduction in throughput. Combined with the spectrum analyzer power analysis and the higher VZW BS transmit power, we are certain that CLN's DL throughput reduction is caused by OOB interference.

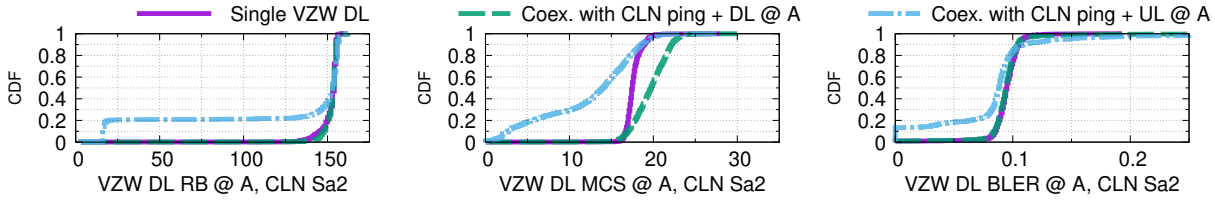
Impact of CLN's OOB interference on VZW throughput: Similar to the previous analysis, we only focus on analyzing the coexistence between VZW DL and CLN ping + DL/UL (hereinafter shortened to CLN DL/UL). We omit the analysis on VZW UL due to



(a) VZW DL tput. @ A, CLN Sa1 (b) VZW DL tput. @ B, CLN Sa1 (c) VZW DL tput. @ A, CLN Sa2 (d) VZW DL tput. @ B, CLN Sa2

Figure 7.9: Coexistence performance in terms of VZW DL throughput under varying CLN TDD configurations.

no impact of OOB interference. Additionally, data containing CLN ping only traffic is also omitted from our analysis due to no interference from ping traffic's low network utilization. Fig. 7.9 shows VZW DL throughput on varying locations and CLN TDD configuration. When CLN is using Sa1 configuration, Fig. 7.9a shows a similar reduction of DL throughput when coexisting with CLN DL and UL at location A, while Fig. 7.9b shows the largest throughput reduction (in Sa1) of 17% when coexisting between VZW DL @ B and CLN UL @ B. We also observe a DL throughput reduction for VZW in the location scenario CLN @ A and VZW @ B, although this is lower compared to when both UEs are side-by-side. For Sa2, the highest DL throughput reduction is observed in scenario VZW DL at A and CLN UL at A as shown on Fig. 7.9c, *i.e.*, 43% reduction compared to the single case. Fig. 7.9d shows the counterpart at location B, with the highest reduction of 27% when coexisting with CLN UL at B.

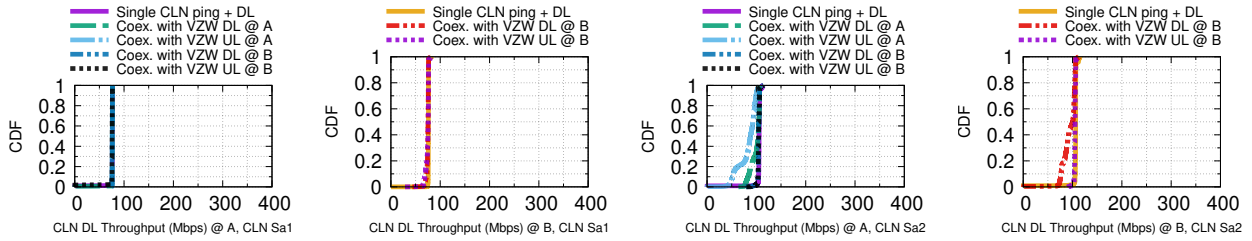


(a) VZW DL RB (b) VZW DL MCS (c) VZW DL BLER

Figure 7.10: Representative comparison of DL RB, MCS, and BLER for VZW @ A, on CLN Sa2.

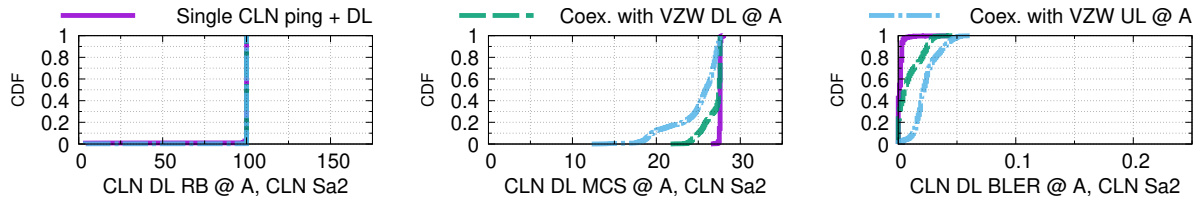
Most of the scenarios described above do not seem to exhibit a drastic change in terms of RB allocation, MCS, and BLER between the coexistence and single cases, except for the scenario of VZW @ A & CLN @ A, CLN uses Sa2 configuration. Thus, we focus on analyzing the said scenario as shown in Fig. 7.10. Fig. 7.10a, 7.10b, and 7.10c shows the CDF comparison of RB allocation, MCS, and BLER, respectively. There is a slight decrease of RB allocation, MCS, and BLER on coexistence cases compared to the single case. As we see from Fig. 7.3, CLN UL using Sa2 should affects VZW DL less than Sa1 due to the fewer number of uplink subframes that overlap with VZW's downlink slots. However, our experiment is not capable of capturing the exact frame timing to determine interference. Thus, the effect of OOB interference is not directly apparent here: the VZW BS may have possibly reacted to the interference by lowering RB allocation and MCS thus resulting in better BLER performance but lower throughput.

Impact of OOB interference with a 20 MHz guard band: In this analysis, we measured the throughput performance of both operators when the CLN operating channel was moved to 3.66 - 3.68 GHz, thus adding a 20 MHz guard band between the CBRS and C-band channels. We refer to these scenarios as **GAP**, while the prior scenarios as **non-GAP**. We omit showing the spectrum analysis in this scenario, since we observed no power leakage in the C-band channel and the new CBRS channel (3.66 - 3.68 GHz) as expected.



(a) CLN DL tput. @ A, CLN Sa1 (b) CLN DL tput. @ B, CLN Sa1 (c) CLN DL tput. @ A, CLN Sa2 (d) CLN DL tput. @ B, CLN Sa2

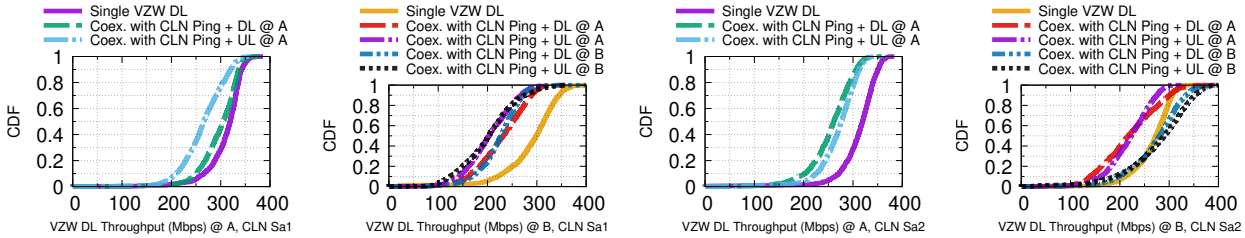
Figure 7.11: Coexistence performance in terms of CLN DL throughput with 20 MHz guard band.



(a) CLN DL RB (b) CLN DL MCS (c) CLN DL BLER

Figure 7.12: Representative comparison of DL RB, MCS, and BLER for CLN @ A, on CLN Sa2, with 20 MHz guard band.

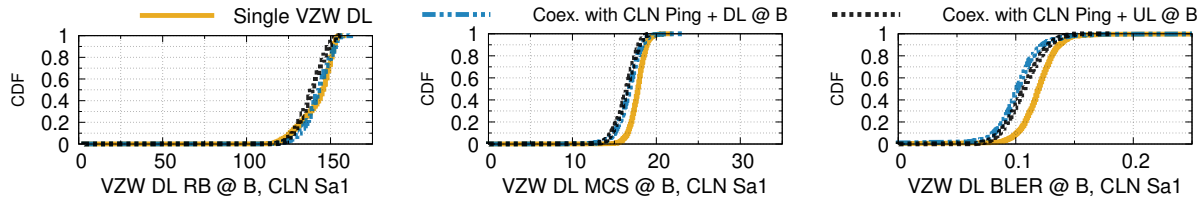
Fig. 7.11 shows the DL throughput performance of CLN under **GAP** scenarios. When CLN uses Sa1 configuration (Fig. 7.11a, 7.11b), we observe no throughput degradation due to the low number of DL subframes utilized. When CLN is using Sa2, we observe the highest degradation of 21% when coexisting with VZW UL @ A. This is an improvement from the highest degradation 60% in the same scenario without the guard band. Further, Fig. 7.12 shows the DL RB, MCS, and BLER of the representative **GAP** results of CLN and VZW @ A, when CLN is using Sa2. While the RB allocations stays at the maximum, we observe higher MCS allocation and lower BLER compared to representative **non-GAP** results on Fig. 7.8.



(a) VZW DL tput. @ A, CLN Sa1 (b) VZW DL tput. @ B, CLN Sa1 (c) VZW DL tput. @ A, CLN Sa2 (d) VZW DL tput. @ B, CLN Sa2

Figure 7.13: Coexistence performance in terms of VZW DL throughput with 20 MHz guard band.

Next, Fig. 7.13 shows the DL throughput performance of VZW under **GAP** scenarios. We observe throughput degradation on various parameters, with the highest reduction of 30% when VZW is coexisting with CLN UL @ B using Sa1. However, these reductions can be



(a) VZW DL RB (b) VZW DL MCS (c) VZW DL BLER

Figure 7.14: Representative comparison of DL RB, MCS, and BLER for VZW @ A, on CLN Sa1, with 20 MHz guard band.

explained by the higher MCS used on the single cases. As a representative result, Fig. 7.14 shows the DL RB, MCS, and BLER of **GAP** results of CLN and VZW @ B, when CLN is using Sa1. We observe a higher MCS and correspondingly, a slightly higher BLER on the single case. Additionally, we observed a median DL BLER of 0.1-0.12 on all cases. Therefore, these throughput degradations are not caused by interference, but network variations.

7.3 Co-channel Interference between CBRS Channels

7.3.1 Deployments, Tools, and Methodology

Deployment overview: An extensive measurement campaign was conducted over a wide area of approximately 12 km^2 where the South Bend school district has deployed CBRS, as shown in Fig. 7.15. Four BSs, *i.e.*, James Whitcomb Riley High School (BS-1), Hayes Tower (BS-2), West Tower (BS-3), and Navarre Middle School (BS-4) have been deployed on school buildings and towers, allowing South Bend schools to launch its own private LTE network to serve students and families. To sustain a high throughput and enhance system capacity, each BS has multiple CBSDs, each operating on a separate sector at the maximum permitted power of 47 dBm/10 MHz. Each CBSD is identified by its Physical Channel Identity (PCI) and operates over a single 20 MHz wide channel. Table 7.2 provides the details about these BSs including their height, PCI, and the center frequencies of the channel allocations. Since there are only 7 non-overlapping 20 MHz channels in the CBRS band and the deployment

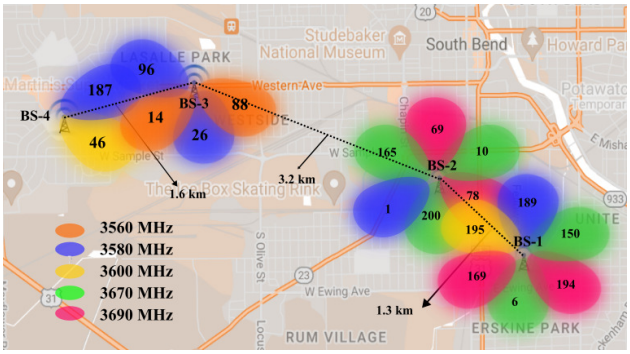


Figure 7.15: CBRS deployment by the South Bend school district.

Table 7.2: Height, PCI, and the center frequencies of the channel allocations for BSs.

Region	**Height (m)**	**Channel Allocations (Center freq.)**				
		3560 MHz	3580 MHz	3600 MHz	3670 MHz	3690 MHz
BS-1 (6 PCIs)	45	N/A	189	195	6, 150	169, 194
BS-2 (6 PCIs)	55	N/A	1	N/A	10, 200, 165	78, 69
BS-3 (4 PCIs)	33	14, 88	96, 26	N/A	N/A	N/A
BS-4 (2 PCIs)	13	N/A	187	46	N/A	N/A

has 18 PCIs, it is clear that CBSDs will reuse channels. Thus, channel reuse is introduced at each BS via sectorization at the expense of potential CCI. It should be noted that the Google SAS shows that all 15 channels (10 MHz each) are available for GAA use by this deployment.

BS-1 is deployed on the roof of James Whitcomb Riley High School at a height of 40 m. It uses four 20 MHz channels and six sectors with the PCIs as shown in Table 7.2.

BS-2 is mounted on a tower with a height of 55 m, and uses three channels across six PCIs, three of which operate on the same frequency (3670 MHz). The distance between BS-1 and BS-2 is about 1.3 km.

BS-3 is located on a tower at a lower height (33 m), compared to BS-1 and BS-2, and two channels, i.e., 3560 MHz and 3580 MHz, are used to serve four sectors with PCIs as shown in Table 7.2.

BS-4 is placed on the roof of Navarre Middle School at the lowest height (13 m), and uses 3580 MHz and 3600 MHz to serve PCIs 187 and 46, respectively. The sector with PCI 187

is directed towards BS-3 with PCIs 96 and 26 operating on the same channel, representing potential CCI.

Table 7.3: Measurement tools and devices.

App./Tool	**Features**	**Devices**
SigCap	Operator,PCI, EARFCN, Band, Frequency, Altitude, Longitude, Latitude, RSRP, RSRQ, RSSI	1 × Google P5, 1 × Google P6, 1 × Samsung S21
QualiPoc	Operator, PCI, Band, Altitude, Longitude, Latitude, RSRP, RSRQ, CQI, RSSI, DL/UL Throughput, RB per subframe	2 × Samsung S22+
PRiSM	PCI, EARFCN, Frequency, Altitude, Longitude, Latitude, RSRP, RSRQ, RSSI	1 × Google P5

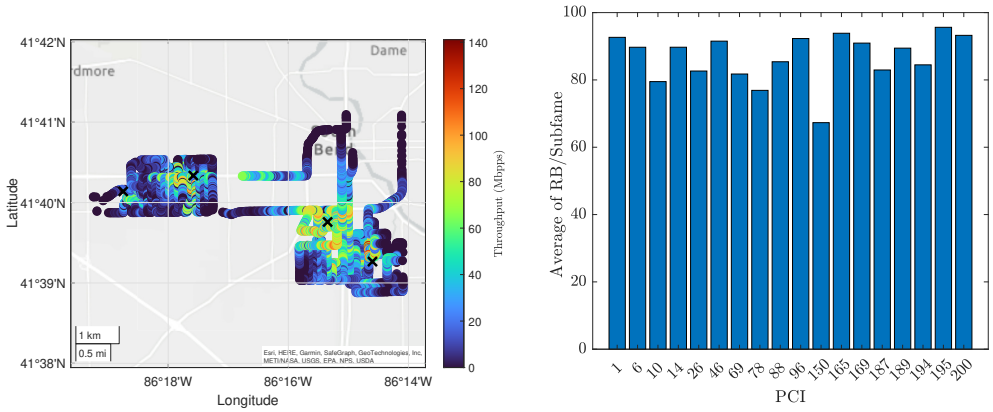
Measurement tools: Smartphones were used as user equipment (UEs) to capture detailed signal information, using tools such as SigCap, QualiPoc, and PRiSM as shown in Table 7.3.

SigCap is an Android application which collects wireless signal parameters (cellular and Wi-Fi) by using APIs without requiring root access. It allows extraction of detailed signal parameters such as Received Signal Strength Indicator (RSSI), RSRP, RSRQ, channel band and frequency for 4G, 5G, and Wi-Fi technologies every 5 seconds, along with location and time-stamps from the GPS receiver on the device.

QualiPoc is a commercial measurement application developed by Rohde & Schwarz and installed on Android phones [100]. In addition to signal parameters extracted by SigCap, QualiPoc collects MCS, block error rate (BLER), time division duplexing (TDD) configuration, channel quality indicator (CQI), and physical layer throughput. All DL throughput results discussed in this work are extracted from QualiPoc, running an iperf utility.

PRiSM is a software-defined radio (SDR) based handheld network scanner for surveying 4G/5G networks and also operates as a spectrum analyzer from 70 MHz to 6 GHz [33]. It easily connects to PCs, tablets, and smartphones to monitor the frequency of interest. Unlike the above two tools, PRiSM does not require a SIM card to extract network information and

uses the smartphone merely as a display and recording device to track channel occupancy.



(a) Throughput performance. (b) Average RBs/subframe per PCI.

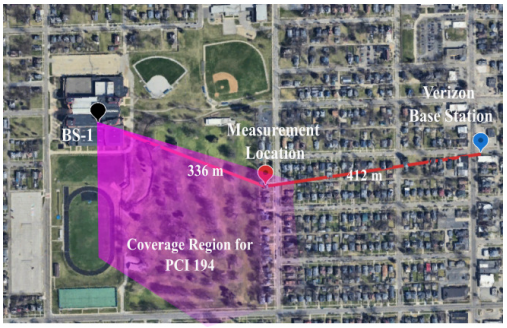
Figure 7.16: Throughput performance and average RBs/subframe for each BS.

Measurement campaigns: Driving and stationary measurements campaigns (MCs) were conducted during the summer months of 2023, with dense foliage-covered trees. The UEs connected to the CBRS network using SIM cards provided by the school district. Measurements of the Verizon network used a 5G SIM with an unlimited data plan and no throttling. We grouped our experiments into three separate campaigns.

MC-1: Driving measurements were conducted around all the CBSDs as shown in Fig. 7.16a, at an average speed of 32 km/hour, over a time period of nearly 3 hours per CBSD. QualiPoc, SigCap and PRiSM were used to collect data, running on the smartphones shown in Table 7.3. DL throughput measurements were recorded on two Samsung S22+ phones with QualiPoc, while the PRiSM was connected to a Google P5 and scanned all CBRS and C-Band channels in order to identify other users using these bands.

MC-2: This campaign focused on BS-3 and BS-4, which are 1.6 km apart, to evaluate potential CCI in the deployment due to reuse of 3580 MHz by CBSDs in these two BSs. After identifying CCI, we worked with the network provider to change frequency assignments and evaluated the improvement when CCI was removed.

MC-3 To evaluate ACI due to C-band, we conducted focused, stationary, measurements between PCI 194 deployed on 3690 MHz in BS-1 and a nearby Verizon BS operating in 3700 - 3760 MHz. Fig. 7.17a shows the measurement location for MC-3, and its distance from BS-1 and the Verizon BS. The experiments were conducted in two phases to assess the performance of PCI 194 on 3690 MHz under ACI caused by the usage of C-Band. CBRS and C-Band users first conducted DL transmissions at different time instants, avoiding ACI. Then, they performed simultaneous DL transmissions, leading to ACI on CBRS band. Fig. 7.17b shows the devices used during MC-3. PRiSM was used to continuously monitor CBRS (Band 48) and C-band (n77/n78) usage.



(a) Distance from BS-1 and Verizon BS.

(b) Measurement setup.

Figure 7.17: Measurement environment and setup for MC-3.

7.3.2 Performance Results and Discussions

In this section, we present statistical analyses of the measurements under different conditions. The discussion is divided into four main categories: i) the performance of a real-world CBRS deployment, ii) CCI amongst GAA users, iii) ACI from C-band to CBRS, and iv) utilization of CBRS band by mobile operators and comparison with C-band.

Performance Evaluation: Fig. 7.16a illustrates the map of outdoor throughput obtained via driving measurements and Fig. 7.16b shows the distribution of RBs per subframe across all the PCIs in the deployment. The outdoor throughput observed is in the range of 20-

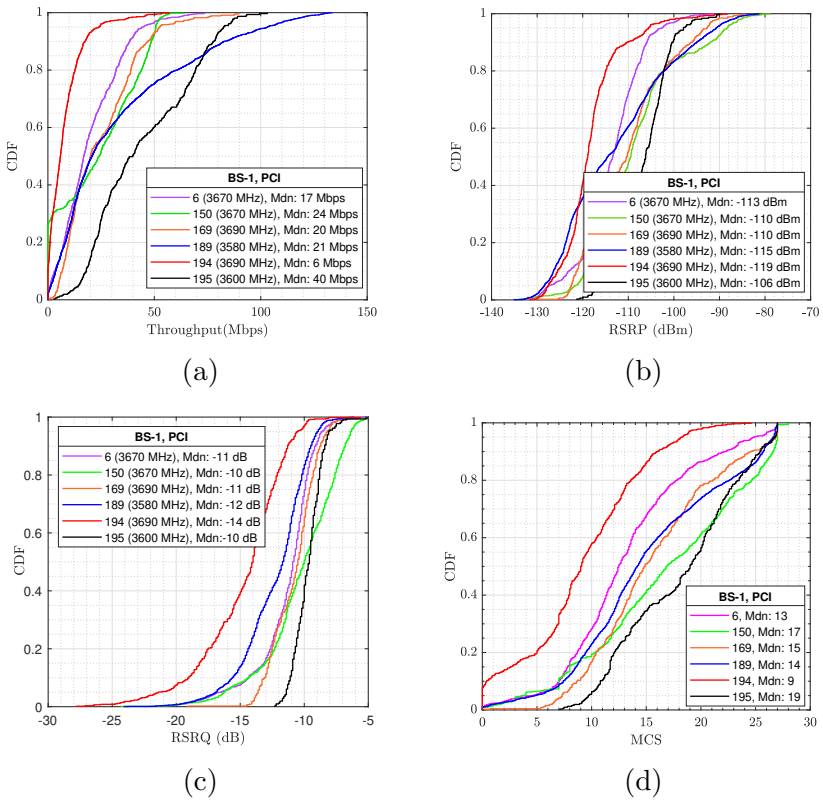


Figure 7.18: CDF plots of throughput, RSRP, RSRQ, and MCS for PCIs at BS-1.

40 Mbps on average. The highest and lowest throughput were observed around BS-2 and BS-4 due to the height of these BSs at 55 m and 13 m, respectively. Throughput observed around BS-2 is notably higher compared to other BSs, while the lowest tower height of BS-4 leads to only a small area with high throughput. BS-1 is at a comparable height to BS-2; however, its coverage area is notably smaller than that of BS-2 due to dense tree coverage, especially to the southeast. Since throughput is primarily a function of number of RBs allocated and MCS, we verify that the differences in measured throughput are not primarily due to RB allocation: Fig. 7.16b shows that the RB usage is approximately similar, with some differences that will be addressed later. We further analyze the measured throughput, RSRP, and RSRQ for each BS using cumulative distribution functions (CDFs).

Performance of BS-1: Fig. 7.18 presents the results for each PCI of BS-1. PCI 195 has the best throughput in Fig. 7.18a, almost double that of the other PCIs, as it is the

only PCI from BS-1 or BS-2 operating on 3600 MHz, as seen from Table 7.2, and thus faces no CCI from other PCIs on the same channel. Similarly, the RSRP and RSRQ for PCI 195 outperforms the other PCIs in BS-1 as given in Figs. 7.18b and 7.18c, respectively. PCIs 6 and 150 operate on 3670 MHz, while PCIs 169 and 194 operate on 3690 MHz. Although PCIs 6 and 150 showed similar median throughput performances at 17 Mbps and 24 Mbps, respectively, there is a substantial performance gap between PCI 169 and PCI 194, achieving 20 Mbps and 6 Mbps respectively. PCI 194 also exhibited the worst RSRP, RSRQ and MCS performance as compared to the best performing PCI 195 in BS-1 as seen from 7.18d, which explains the lower throughput. Based on our detailed analysis of signal strength measurements in the vicinity of BS-1, the reason for this is that PCI-194 experiences ACI due to the use of the immediately adjacent C-band, by a nearby Verizon BS, as shown in Figs. 7.17a and 7.19. The performance of PCI 194 both with and without C-band usage, will be discussed below.

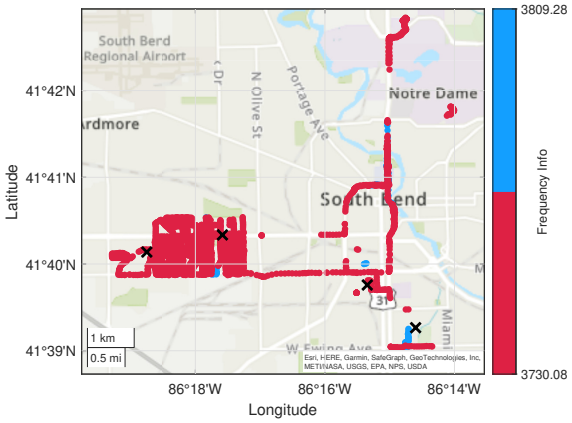
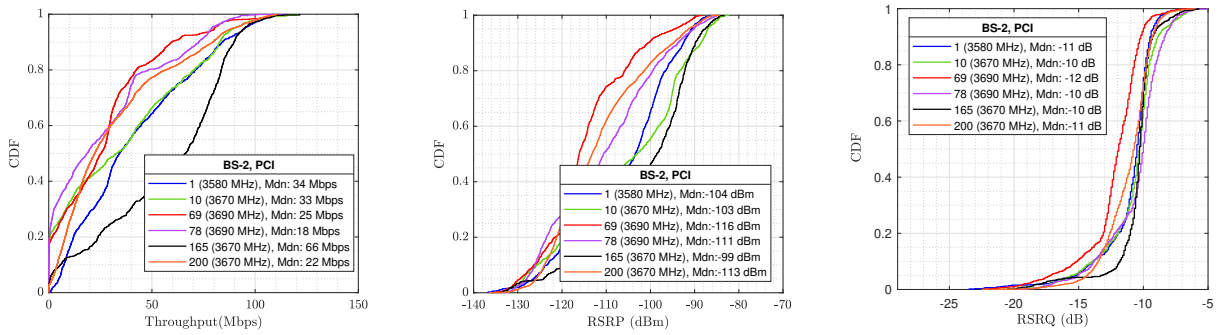


Figure 7.19: The usage of C-Band by Verizon in the region.

Performance of BS-2: Fig. 7.20 shows the performance of BS-2, operating at a height similar to BS-1, but within an area where free-space propagation is more prevalent. Hence, PCI 165 on 3670 MHz achieves the highest median throughput of the CBRS deployment, reaching 66 Mbps as indicated in Fig. 7.20a. The median throughput of PCI 165 is nearly double that observed on the other PCIs on 3670 MHz in BS-2 and BS-1, as PCI 165 is the

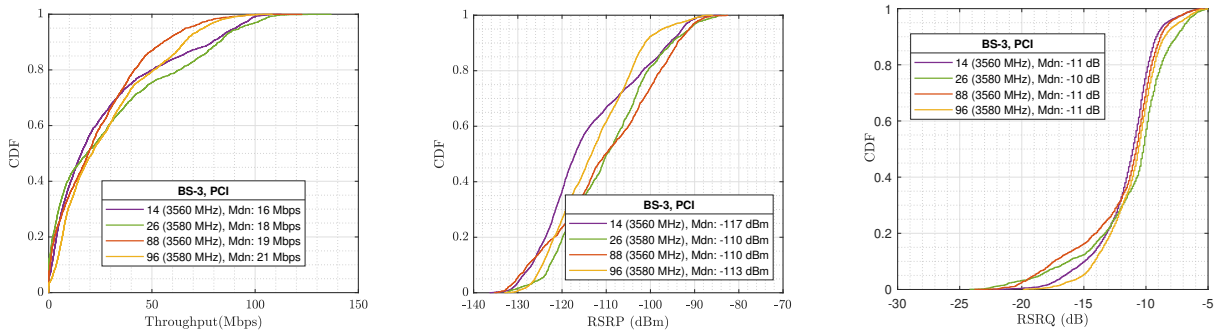


(a) (b) (c)

Figure 7.20: CDF plots of throughput, RSRP, RSRQ, and MCS for PCIs at BS-2.

only one directed northwest, while the rest are oriented southeast, potentially leading to CCI among them. PCI 200 has the lowest median throughput, 22 Mbps, amongst the PCIs on 3670 MHz in BS-2 due to its orientation toward a residential area with dense trees. As discussed for PCI 194 in BS-1, we observe that PCIs 69 and 78 on 3690 MHz have the worst performance in BS-2: this can be explained by ACI resulting from the usage of 3730 MHz in the vicinity of BS-2, as shown in Fig. 7.19. PCI 78 has the lowest median throughput of 18 Mbps on BS-2, and 7 Mbps lower than PCI 69, since its coverage overlaps with PCI 169 on 3690 MHz coming from BS-1, as seen in Fig. 7.15. RSRP results in Fig. 7.20b clearly exhibit the reduced impact of foliage on BS-2, where three PCIs (165, 1 and 10) have a median greater than -105 dBm. Similarly, in Fig. 7.20c, the median RSRQ levels in BS-2 ranged from -12 dB to -10 dB, and provided better performance than BS-1. As in the throughput results, PCI 69 on 3690 MHz offered the lowest RSRQ performance due to the ACI.

Performance of BS-3: Fig. 7.21 presents the results of BS-3, which is less likely to suffer from interference since the distance of 3.2 km between BS-3 and BS-2 mitigates the presence of CCI, while the utilization of the lower edge of the CBRS spectrum (3560 MHz and 3580 MHz) offers a sufficient guard band to avoid the effect of C-band ACI. Hence, all PCIs on BS-3 exhibit similar throughput, RSRP and RSRQ behavior. The obtained throughput levels



(a) (b) (c)

Figure 7.21: CDF plots of throughput, RSRP, RSRQ, and MCS for PCIs at BS-3.

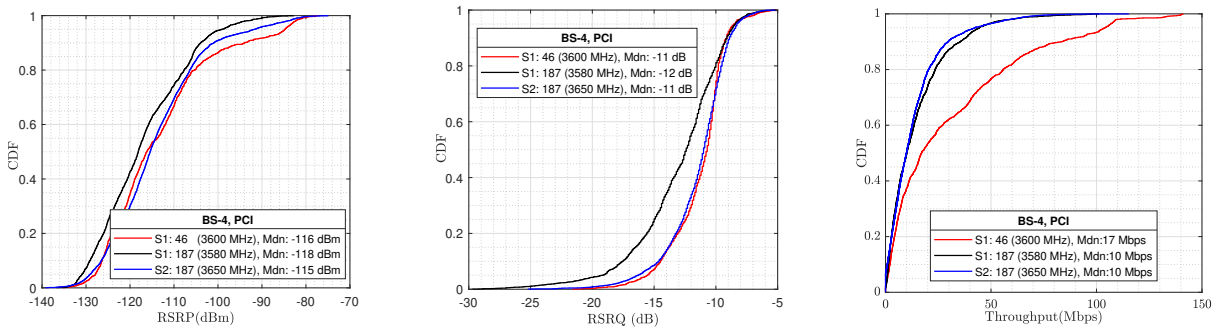
at BS-3, including the peak throughput on PCI 88 (3560 MHz), is much lower compared to BS-1 and BS-2 due to the lower tower height.

As shown in Fig. 7.15, BS-3's PCI 96 faces west. Due to the short distance between BS-3 and BS-4, 1.6 km, and lower tower height of BS-3, this poses a potential CCI threat to PCI 187 in BS-4 operating on the same frequency.

Avoiding CCI by selecting an appropriate frequency: MC-2 on PCI 187 evaluated the impact of CCI within the CBRS deployment itself and aims to improve system performance via a suitable frequency allocation.

Performance of BS-4: PCI 187 from BS-4, operating on 3580 MHz (S1) shows the worst throughput, RSRP and RSRQ due to CCI coming from PCI 96 of BS-3, as shown in Fig. 7.22, while PCI 46 from the same BS does not experience CCI and exhibits nearly the same performance as the PCIs on BS-3 as it is the only PCI operating on 3600 MHz in the region of BS-3 and BS-4.

To alleviate the effect of CCI on PCI 187, we proposed changing the frequency from 3580 MHz (S1) to 3650 MHz (S2) based on our study of frequency allocations and measurements of signal strengths in the vicinity of the CBRS deployment. The frequency 3650 MHz was not used by any of the BSs deployed by the school district, as seen from Table 7.2. As illustrated in Fig. 7.23, Verizon has utilized the frequency 3650 MHz in the region of BSs,



(a) (b) (c)

Figure 7.22: CDF plots of RSRP, RSRQ, and throughput for BS-4 i) Scenario 1 (S1): PCI 187 on 3580 MHz and PCI 46 on 3600 MHz, and ii) Scenario 2 (S2): PCI 187 on 3650 MHz.

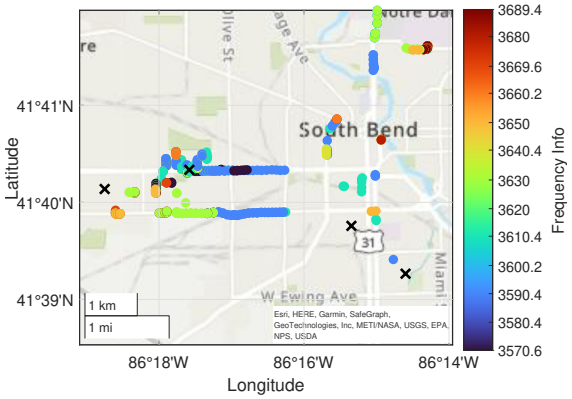
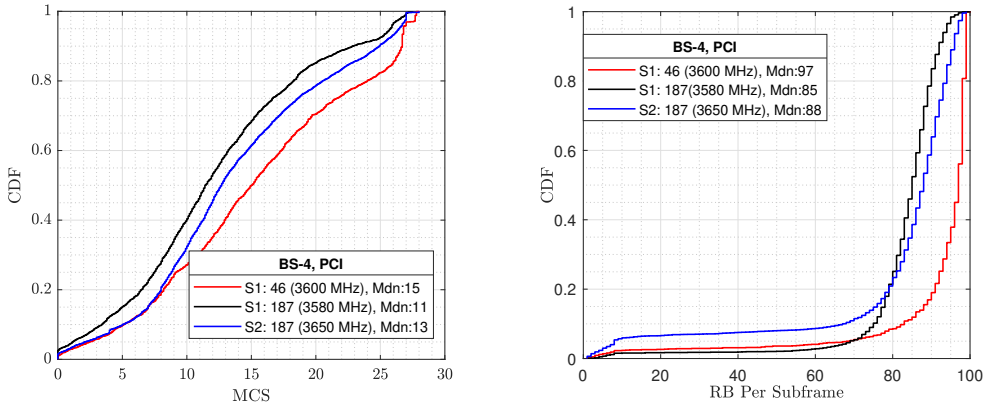


Figure 7.23: CBRS band usage by Verizon in the region.

but not in the direction of PCI 187.

Fig. 7.22a and Fig. 7.22b show that changing the frequency of PCI 187 to 3650 MHz resulted in higher RSRP and RSRQ levels compared to the original frequency of 3580 MHz, and a similar performance to PCI 46, which is free of CCI. It is important to highlight that PCI 46 maintained the same performance after the frequency change on PCI 187, as they do not operate on the same frequency.

As compared with S1, the peak throughput of S2 increased by around 20 Mbps, from 100 Mbps to 120 Mbps, while the median throughput remained the same as shown in Fig. 7.22c. This can be explained as follows: throughput is determined by the MCS and number of resource blocks (RBs) allocated per subframe, as shown in Fig. 7.24. In Fig. 7.24a, the



(a) (b)

Figure 7.24: MCS and RBs per subframe for PCIs at BS-4.

median value of MCS for S2 increased by 2 indicating that the frequency 3650 MHz is exposed to less CCI compared to the frequency 3580 MHz, and the number of RBs also improved slightly, but not enough to deliver a significant throughput increase. We see that PCI 46 for example has a higher number of RBs/subframe leading to consistently higher throughput. We speculate that the number of RBs/subframe allocated to PCI 187 were lower than PCI 46 due to proprietary network optimization algorithms, and hence, even though the signal metrics, RSRP, RSRQ and MCS all improved with the change in frequency, the resulting median throughput remained unchanged, though the maximum throughput did improve.

Impact of ACI from C-band on CBRS: MC-3 on PCI 194 evaluates the effect of ACI caused by C-band on CBRS. We performed stationary measurements in the location shown in Fig. 7.17a where the strongest RSRP was measured for PCI 194 on 3690 MHz.

Fig. 7.25 shows the DL throughput performance when connected to PCI 194 in BS-1, in the absence and presence of a Verizon C-band UE. First, we measured DL throughput on the UE connected to CBRS only, followed by simultaneous DL transmissions to two UEs, one connected to CBRS and the other connected to C-band. We observed around 16% throughput degradation on the CBRS UE due to ACI from C-band, when both devices were

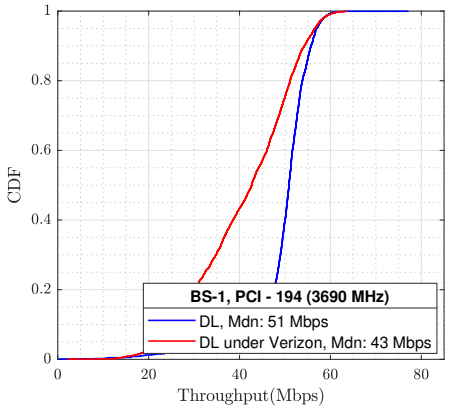
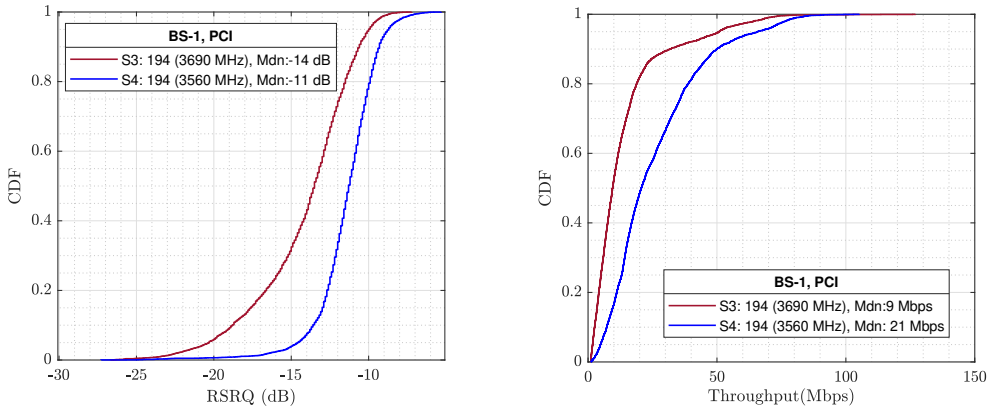


Figure 7.25: The impact of C-Band on PCI 194 (3690 MHz) at BS-1.

simultaneously connected. The CBRS UE achieved a peak throughput of approximately 80 Mbps when there was no transmission from the C-band user. However, its maximum throughput was limited to around 60 Mbps in the presence of the C-band UE. The absence of guard bands between CBRS and C-band, the transmit power difference and lower tower height of BS-1 compared to the Verizon C-band, all contribute to the reduced throughput performance on CBRS UE due to adjacent channel C-band usage.



(a) (b)

Figure 7.26: RSRQ and throughput for PCI 194 i) Scenario 3 (S3): 3690 MHz, and ii) Scenario 4 (S4): 3560 MHz.

Fig. 7.26 assesses the performance improvement of PCI 194 after a frequency change from 3690 MHz (S3) to 3560 MHz (S4): this change was made in response to our measurements

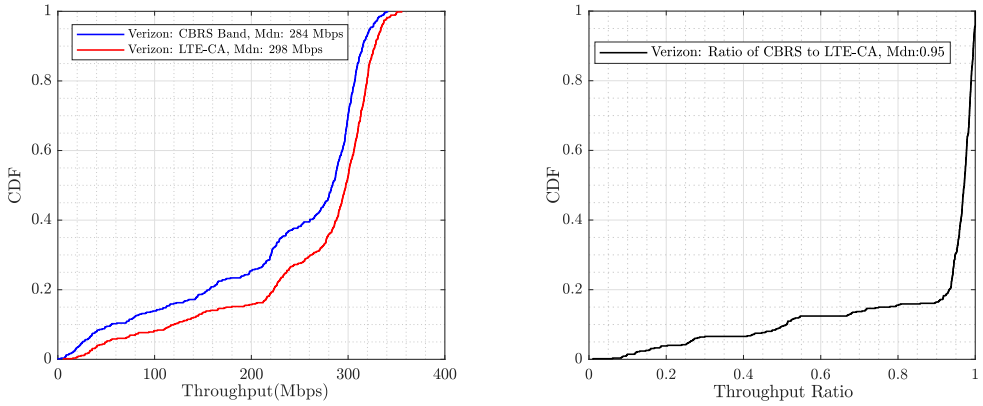
Table 7.4: Frequencies used by Verizon in the vicinity of the South Bend CBRS deployment.

Band	**Freq. (MHz)**	**Band**	**Freq. (MHz)**
CBRS, Band 48	3560, 3570, 3580, 3590, 3600, 3610, 3610, 3620, 3630, 3640, 3650, 3660, 3670, 3680	C-band, Bands n77/n78	3730, 3809

that indicated significant adjacent channel interference from C-band deployments in the vicinity. We performed a driving measurement campaign in the coverage area of PCI 194 after the frequency change to evaluate the influence of appropriate frequency allocations on mitigating ACI from C-band in CBRS band. Fig. 7.26a shows that changing to S4 resulted in higher median RSRQ levels compared to the original frequency of 3690 MHz: an increase from -14 dB to -11 dB. Moreover, S4 now exhibits comparable RSRQ performance to the neighboring PCI 150 of BS1, which is free of ACI. As compared with S3, the median throughput of S4 increased by around 12 Mbps, from 9 Mbps to 21 Mbps, while the peak throughput remained the same as shown in Fig. 7.26b.

A similar scenario will arise between 3.45 GHz and CBRS once 5G deployments in the 3.45 - 3.55 GHz band increase, indicating further performance degradation on CBSDs operating at the lower edge of the CBRS band. Hence CBRS deployments need to know whether 5G is being deployed in upper and/or lower adjacent bands and not use the band-edge CBRS channels which will be impacted the most by ACI. Since the SAS does not provide this information, this intelligence needs to be available at the deployment site using measurements tools such as the ones used in this study.

CBRS band use by Verizon using LTE-CA: During our experiments for MC-3, we observed that the Verizon BS also transmits on the CBRS band using LTE with carrier aggregation (LTE-CA), aggregating up to five 20 MHz CBRS channels with four channels being aggregated most often (80%). Along with a 20 MHz primary LTE channel, this allows up to 120 MHz of bandwidth for use when high capacity is required: this is significantly higher than the C-band channel bandwidth of 60 MHz that Verizon has exclusive license to, but at



(a) (b)

Figure 7.27: Verizon throughput with LTE-CA using CBRS.

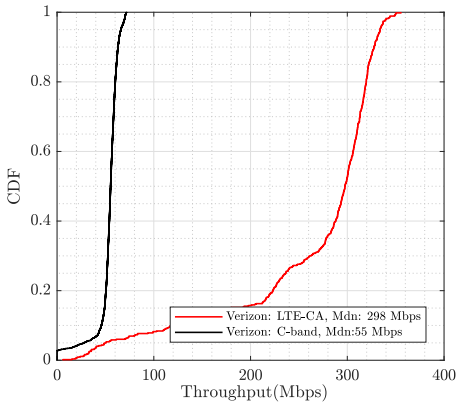


Figure 7.28: Verizon LTE-CA and C-band throughput.

zero cost compared to the billions of dollars spent for exclusive licenses. Table 7.4 details how the CBRS band (also called Band 48), is utilized by Verizon in the vicinity of the South Bend CBRS deployment. We see that Verizon CBSDs are deployed on all available CBRS frequencies, creating potential CCI for other CBRS deployments. Additionally, we observed that when LTE-CA uses CBRS channels, the total throughput as well as the proportion of throughput carried over CBRS are both very high, as shown in Fig. 7.27 and overall throughput of 4G using LTE-CA was significantly higher than 5G using C-band at the same location as shown in Fig. 7.28. Thus, even as operators roll out 5G using their new, licensed, spectrum, CBRS remains extremely competitive when additional capacity is needed.

7.4 Summary and List of Accomplishments

This chapter presents our first comprehensive, device-based measurement analysis of ACI between adjacent CBRS and C-Band channels, along with CCI within CBRS channels. We demonstrate that the lack of guard bands, significant power differences, and asynchronous TDD operation severely limit the potential throughput for both CBRS and C-Band. Introducing a 20 MHz gap between the CBRS and C-Band channels significantly mitigates throughput degradation (CBRS: 60% to 21%, C-band 43% to 30%), underscoring the impact of OOB interference. Due to the 3.55-3.65 GHz PAL license restriction, PAL channels face the lowest risk of ACI compared to GAA and Tier 1.

Our next extensive study on CBRS deployments in South Bend, highlights that secondary coexistence between GAA CBSDs, even within the same network, can hinder optimal performance. In the deployments, despite SAS clearance for all CBRS channels, concentrated use of specific frequencies (3580 MHz, 3670 MHz, 3690 MHz), coupled with the unexpected emergence of adjacent CBRS and C-band deployments, significantly impacted performance. Collaborating with the CBRS provider, we successfully demonstrated improved signal quality by changing the frequency of a CBSD. However, SAS limitations delayed this change, emphasizing the need for dynamic channel allocation based on real-world measurements–a capability currently unavailable. Additionally, even with 4G, aggregating multiple CBRS channels outperformed C-band 5G, demonstrating the value of CBRS for both large mobile operators and smaller private network providers.

The following papers has been published in the topic of machine learning in wireless networks:

- Muhammad Iqbal Rochman et al. "A Measurement Study of the Impact of Adjacent Channel Interference between C-band and CBRS". In: *IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. 2023.

- Armed Tusha et al. "A Comprehensive Analysis of Secondary Coexistence in a Real-World CBRS Deployment". In: *IEEE Dynamic Spectrum Access Networks (DySPAN)*. 2024.

CHAPTER 8

MACHINE LEARNING IN WIRELESS NETWORKS

8.1 Overview and Related Works

Machine Learning (ML) approaches has been used in wireless networks due to the ability to learn useful information from input data to improve future network performance. ML models enable us to replace heuristics with more robust and general alternatives. In [118, 22, 129], several state-of-the-art applications of ML in wireless communication and unresolved problems have been described, *i.e.*, resource management in the MAC layer, networking and mobility management in the network layer, and localization in the application layer. In this dissertation, we present two works on the ML-based approach to solve problems of spectrum sharing in the coexistence between LTE-U and Wi-Fi [32], and to determine whether a smartphone is located indoor or outdoor based on its signal data [89].

8.2 Machine learning-enabled spectrum sharing in dense LTE-U/Wi-Fi coexistence scenarios

LTE-U was developed by the LTE-U forum [71] as an alternative to the LAA specification for unlicensed spectrum access. While LAA uses a carrier sensing LBT mechanism, LTE-U uses a simple duty-cycling technique where the LTE-U BS will periodically switch between ON and OFF states in an interval set according to the number of Wi-Fi APs present in the channel. In the ON state, the BS transmits data as a normal LTE transmission while in the OFF state, the BS does not transmit any data but passively senses the channel for the presence of Wi-Fi. The number of sensed Wi-Fi APs is then used to properly adjust the duty cycle interval, and this process is known as Carrier Sense Adaptive Transmission (CSAT). In this work, we present a method to accurately determine the number of coexisting Wi-Fi

Table 8.1: Different Types of LTE-U CSAT.

CSAT Types	**Method**	**Pros**	**Cons**
Header Decoding (HD)	Decodes the Wi-Fi MAC header at the LTE-U BS	100% accurate	Additional Complexity [21], high cost
Energy Detection (ED)	Based on the change in the *energy level* of the air medium	Low-cost, low-complexity	Low-accuracy [107]
Auto-correlation (AC)	LTE-U BS performs correlation on the Wi-Fi L-STF symbol in the preamble	Low-cost, low-complexity	Medium accuracy (more accurate than ED) [106]
Machine Learning (ML)	Train the model based on energy values on the channel	Much more accurate than ED and AC methods	Requires gathering data and training models

APs [32], which is important for optimum operation of the CSAT procedure.

Table 8.1 shows the various approaches to determine the number of Wi-Fi AP for CSAT, which includes the advantages and disadvantages of each approaches. In this work, we observe the Wi-Fi AP energy values during LTE-U OFF duration and using the data to train different ML models [130]. We also apply the models in an online experiment to detect the number of Wi-Fi APs. Finally, we demonstrate significant improvement in the performance of the ML approach as compared to the ED and AC detectors.

8.2.1 Experiment setup

Our experimental set-up consists of one LTE-U BS and a maximum of five Wi-Fi APs. To emulate the LTE-U BS, we use the National Instruments USRP 2953-R software defined radio (SDR) which is equipped with the LTE-U radio framework. We assume the LTE-U BS transmits only downlink packets on the unlicensed spectrum, while all uplink transmissions are on the licensed spectrum. Control and data packets are transmitted using PDCCH and PDSCH respectively. There are five Netgear Wi-Fi APs and five Wi-Fi clients deployed in a static configuration. The Wi-Fi clients are combination of laptops and smartphones capable

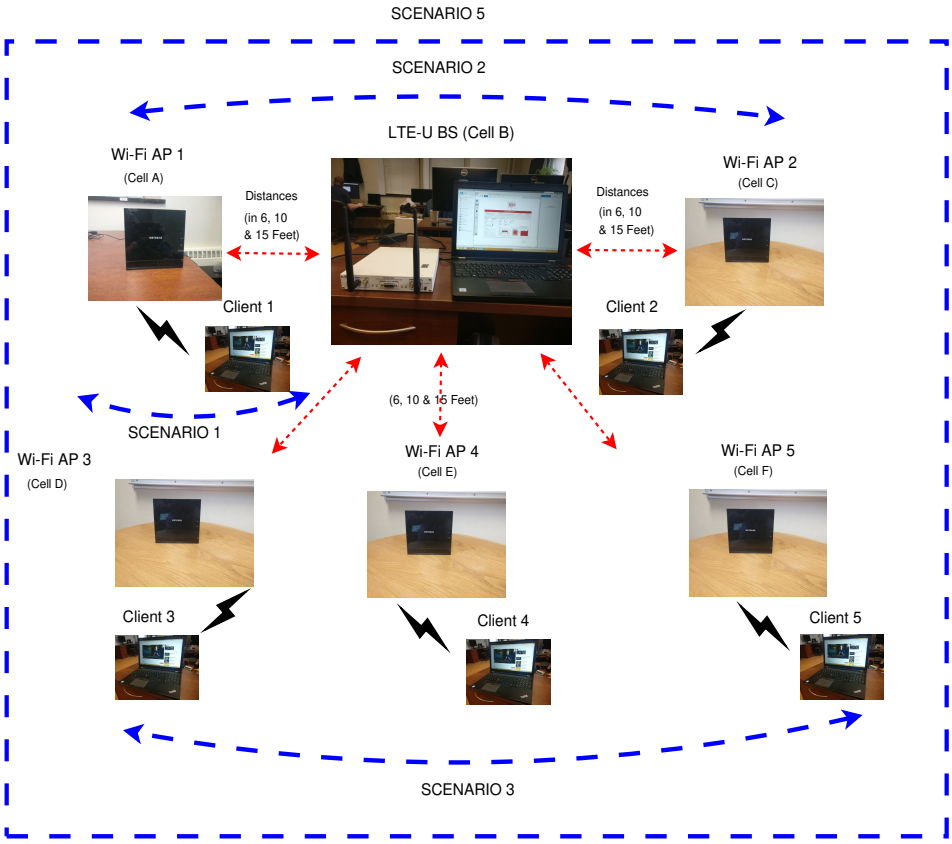


Figure 8.1: LTE Wi-Fi Co-existence Experimental Setup.

of Wi-Fi 802.11 ac connection. As soon as the client connects to the Wi-Fi AP, it starts a live video streaming application to simulate a full-buffer transmission. The experimental setup is shown in Fig. 8.1 and the complete experimental parameters are described in Table 8.2. Both LTE-U BS and Wi-Fi APs operates at maximum transmit power using all possible resource blocks and the highest modulation coding scheme (*i.e.*, 64-QAM). CSMA/CA and duty-cycle adaptation mechanism are used for channel access for Wi-Fi and LTE-U, respectively. Both Wi-Fi and LTE-U follow their respective retransmission schemes. Finally, we assume that the Wi-Fi APs support both active and passive scanning mode, *i.e.*, both beacon and probe response packets are transmitted by the AP during the association process. We separated the APs and BS into six cells, with five cells (Cell A, C, D, E, and F) as Wi-Fi cells and one cell (Cell B) as the LTE-U cell. Each Wi-Fi cell consists of one AP and one client, while the

Table 8.2: Experimental Set-up Parameters

Parameter	**Value**
Available Spectrum and Frequency	20 MHz and 5.825 GHz
Maximum Tx power for both LTE and Wi-Fi	23 dBm
Wi-Fi sensing protocol	CSMA/CA
Traffic	Full Buffer (Saturation Case)
Wi-Fi Antenna Type	MIMO
LTE-U Antenna Type	SISO
LTE-U Modulation	64-QAM
LTE-U data and control channel	PDSCH and PDCCH
Type of Wi-Fi Clients	2 Google Pixel, 1 Samsung, 1 Redmi, and 1 Apple Laptop

LTE-U BS and UE are contained within the same USRP board. We also ensure that there is no extra interference in the channel from other Wi-Fi APs.

Both BS and APs transmit full buffer data at maximum power. The BS operates at a 50% duty cycle during the experiment, and listens to the configured unlicensed channel during the OFF period for *RF power* and AC measurement. The *RF power* measurement is configured in the LTE block control module of the NI LTE application framework, which outputs energy value as defined in §8.2.2. The AC function is also configured in the LTE block control module of the same framework and outputs the AC events as defined in §8.2.2. The energy values observed from Algorithm 2 are given as input to the ML algorithm to classify the number of Wi-Fi APs on the channel.

We measure the energy, AC value and ML (same energy value as input to ML) at the LTE-U BS for the following scenarios:

- **Scenario 0:** No Wi-Fi APs are deployed and only one LTE-U cell (*i.e.*, Cell B) is deployed.
- **Scenario 1:** One Wi-Fi AP (*i.e.,* Cell A) and one LTE-U (*i.e.*, Cell B) is deployed.
- **Scenario 2:** Two Wi-Fi APs (*i.e.*, Cell A & C) and one LTE-U (*i.e.*, Cell B) are

deployed.

- **Scenario 3:** Three Wi-Fi APs (*i.e.*, Cell D, E, & F) and one LTE-U (*i.e.*, Cell B) are deployed.
- **Scenario 4:** Four Wi-Fi APs (*i.e.*, Scenario 1: Cell A, Scenario 3: Cell D, E, & F) and one LTE-U (*i.e.*, Cell B) are deployed.
- **Scenario 5:** Five Wi-Fi APs (*i.e.*, Cell A, C, D, E, & F) and LTE-U (*i.e.*, Cell B) are deployed.

In all scenarios, Cell B measures the energy and AC values during the LTE-U OFF period, while the rest of the Wi-Fi cells are transmitting full buffer downlink transmission. We also vary the distances and the LOS and NLOS environment of each cell. In NLOS setup, the wall act as a obstruction between the LTE-U and Wi-Fi APs. We measure the received Wi-Fi AP signals at the LTE-U BS for different 6 feet (For example in Scenario 5, where all the 5 Wi-Fi APs placed at 6 feet from the LTE-U BS), 10 feet and 15 feet distances. Our previous work focused only on detecting Scenarios 1 and 2 (*i.e.*, 1 and 2 Wi-Fi APs coexisting with LTE-U) [107, 106]. Also, we demonstrated that Scenario 0 can be easily distinguished from other scenarios [105].

8.2.2 LTE-U Duty Cycle Adaptation Algorithms

For quantitative comparison of our ML-based algorithm, we also propose header (HD), energy (ED) and auto-correlation (AC) based detection algorithms. Fig. 8.2 explains how different sensing algorithms work based on the known Wi-Fi packet structure.

Header-Decoding based LTE-U duty cycle adaptation algorithm We assume that there is either a common preamble [88, 15] between the LTE-U and Wi-Fi systems or the LTE-U BS has a full Wi-Fi decoder that will allow it to decode the Wi-Fi MAC header and

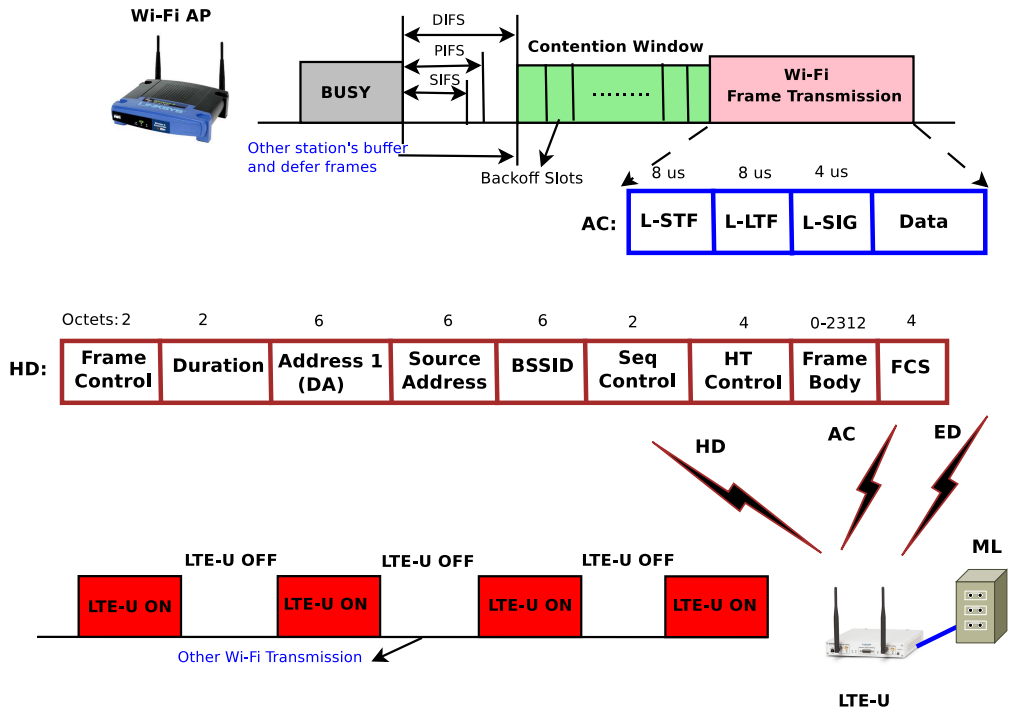


Figure 8.2: LTE-U Duty Cycle Adaptation Algorithm.

hence obtain the BSSID. Doing so, one can accurately detect the number of Wi-Fi APs on the channel better than energy, auto-correlation, and ML algorithms.

We define a simple algorithm shown in Algorithm 1, to classify the number of active Wi-Fi APs at each time slot while carefully avoid misclassification. In brief, the algorithm counts the number of beacon of each uniquely identifiable BSSID, for a defined time slot. Since we can expect that an AP in a real deployment may hop between channels frequently, it is important to collect beacons for a longer period of time rather than deciding based on just one beacon. The length of the time slot determines the inference delay, hence one would like this delay to be as small as possible. We initially set a time slot of 10 beacons (1.024 s) but reduced it to 5 beacons (0.512 s) while setting a threshold to 4 beacons for an AP to be considered active, *i.e.*, a confidence rate is of 80%. This reduces the inference time to half without compromising the detection accuracy.

Algorithm 1 : Header-decoding based LTE-U Scale Back

Initialization: (i) $Beacon_i = 0$

(ii) $Count.detect_i = 0$, $Count.falsealarm_i = 0$

(iii) $LastTime = 0$, $TimeSlot = 0.512$ s, $Threshold = 4$

```
while true do
    /* A Wi-Fi beacon with BSSID i is detected at time CurrentTime */
    Beacon_i ++;
    if CurrentTime − LastTime ≥ TimeSlot then
        NumberOfAp = 0;
        for i in Beacon do
            if Beacon_i ≥ Threshold then
                NumberOfAp ++;
            end
            Beacon_i = 0;
        end
        LastTime = CurrentTime;
        for i = 1 to 5 do
            if i Wi-Fi is ON then
                if i == NumberOfAp then
                    Count.detect_i ++;
                else
                    Count.falsealarm_i ++;
                end
            end
        end
    end
end
```

Algorithm 2 Energy Based LTE-U Scale Back

Input: $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$

Initialization: (i) $\alpha_6 = \infty$

$(ii) Count.detect_i = 0$, $Count.falsealarm_i = 0$

---

while *true* **do**
  /* Received $Avg(EnergyLevel)$ over one second */
  for *i = 1 to 5* **do**
    if *i Wi-Fi is ON* **then**
      if $\alpha_i \leq$ *Avg(Energy Level)* $\leq \alpha_{i+1}$ **then**
        $Count.detect_i$ ++;
      else
        $Count.false.alarm_i$ ++;
      end
    end
  end
end

Energy based LTE-U duty cycle adaptation algorithm As shown in Fig. 8.1, we measure the received energy at the LTE-U BS for different distances between the LTE-U BS and Wi-fi APs and obtain histograms of the measured signal when one or more Wi-Fi APs are transmitting at 6, 10 and 15 feet from the LTE-U BS. We then fit the measured histograms to probability distribution functions as described in [107] to develop a classification algorithm. In Algorithm 2, an energy-based detection listens to the energy level in the channel and according to a set threshold [107], decides whether to scale back the duty cycle or not. Since the measured energy threshold depends on the the number of detected Wi-Fi APs, the choice of threshold is important to the algorithm. Finally, we implement the algorithm in

the LTE-U BS NI hardware and validate it experimentally.

First, we modify the NI LTE application framework to measure *RF power* during the LTE-U OFF period. The collected energy values are then averaged over one second time duration and used for algorithm input. If the averaged energy value is greater than the specified threshold α_1, *i.e.*, if energy value $\geq \alpha_1$ then there is a possibility of Wi-Fi packets (beacon, probe request, probe response, data, or ACK) transmitted in the channel. The BS then can declare whether one, two, three, four, or five AP is present, based on the other thresholds: α_2, α_3, α_4, α_5 (*e.g.*, if $\alpha_3 \leq$ energy value $\leq \alpha_4$ then there are 4 APs in the channel). By keeping count of correct and incorrect decisions made by the algorithm, we calculate the probability of correct detection and false positive on predicting the number of Wi-Fi APs in the unlicensed spectrum. These probability values are used as a metric to determine the performance of the threshold, such that we pick a set of threshold with high probability of correct detection and low probability of false positive.

Algorithm 3 : Auto-correlation Based LTE-U Scale Back

Input: th_ρ, R

Initialization: $Count.detect_i = 0$, $Count.falsealarm_i = 0$

```
while true do
    /* Received T number of AC values over one second */
    for i = 1 to 5 do
        if i Wi-Fi is ON then
            Signal = 0;
            for t = 1 to T do
                if AC_t ≥ th_ρ then
                    Signal ++;
                end
            end
            ratio = Signal / T;
            if ratio ≤ R_i then
                Count.detect_i ++;
            else
                Count.falsealarm_i ++;
            end
        end
    end
end
```

AC based LTE-U duty cycle adaptation algorithm In the same experiment setup as shown in Fig. 8.1, we count the total number of AC events that are above a threshold for every one second over the duration of 90 seconds. We measure the total number of events above the AC threshold at the LTE-U BS for 6, 10 and 15 feet distances. Then, we observe

the PDF distribution of the number of AC events above the threshold [106] for Scenario 0 to 5 described above. We make use of this key observation to develop a classification algorithm (*i.e.,* Algorithm 3) for both LOS and NLOS scenarios. The algorithm uses AC functions and optimal thresholds to determine the number of Wi-Fi APs in the channel, therefore the selection of threshold is also important and will be shown in this section. We implement the algorithm in the LTE-U BS hardware and validate it experimentally. The AC function is performed at LTE-U BS to sense the spectrum for Wi-Fi preamble signals (*i.e.,* L-STF). The output of the function is an AC value which determine the likelihood that the signal is a Wi-Fi preamble. We observed on many experiments, that the threshold th_ρ of 0.25 is sufficient to determine that the captured signal is a Wi-Fi signal (beacon, probe request, probe response, data, or ACK). Using the threshold, we predicted the number of Wi-Fi signals in every one second period. Next, we calculate the ratio [106] and then compared to R_i which is a threshold determined during a preliminary experiment with i Wi-Fi AP and no LTE-U on the channel. The R_i is determined such that the true positive rate is as high as possible and false positive rate is as low as possible during the preliminary experiment. Since it is not possible for the observed ratio to be higher than R_i, we set a correct prediction that i Wi-Fi AP is present in the channel if the ratio is less than or equal to the threshold R_i, and false prediction otherwise.

8.2.3 ML Algorithms for LTE-U Duty Cycle Adaption

We consider machine learning models that take time-series data of width w as input, giving an example space of $\mathcal{X} \in \mathcal{R}^w$, where $\mathcal{R}$ denotes the real numbers. Our discrete label space of k classes is represented as $\mathcal{Y} \in \{0, 1\}^k$. For example, $k = 3$ classes, enables us to distinguish between 0, 1, and 2 Wi-Fi APs. Machine learning models represent parametrized functions (by a weight vector θ) between the example and label spaces $f(x; \theta) : \mathcal{X} \mapsto \mathcal{Y}$. The weight vector θ is iteratively updated during the training process until the convergence

of the training accuracy or training loss (usually determined by very small changes to the values despite further training), and then the final state of θ is used for testing and real-time inference.

Data preparation The training and testing data is collected over an extended period of time with a single scenario taking about 8 hours. For ease of exposition, we consider the case with one and two Wi-Fi APs. We collect data for each Wi-Fi AP independently and store the two datasets in separate files. Each file contains more than 2.5 million values and the total raw data size in CSV format is of about 60 MB. Each file is treated as time-series data with a sequence of values that are first divided into chunks. We overlap the time-series chunks arbitrarily by three-fourths of their widths w. For example, for chunks width $w = 128$, the first chunk starts at index 0, the second chunk is formed starting from index 32, the third chunk starts at index 64, and so on. This is part of our data augmentation and a soft guarantee that much fewer patterns are broken on the boundary of chunks. The width w of the (time-series data) chunk acts as a parameter for our ML model. It denotes the number of samples that have to be provided to the model to perform the classification. The longer the time-series width w, the more data samples have to be collected during inference. The result is higher latency of the system, however, the more samples are gathered, the more accurate the predictions of the model. On the other hand, with smaller number of samples per chunk, the time to collect the samples is shorter, the inference is faster but of lower accuracy.

The collection of chunks are shuffled randomly. We divide the input data into training and test sets, each 50% of the overall data size. The aforementioned shuffling ensures that we evenly distribute different types of patterns through the training and test sets so that the classification accuracy of both sets is comparable. Each of the training and test sets contain roughly the same number of chunks that represent one or two Wi-Fi APs. We enumerate classes from 0. For the case of 2 classes (either one or two Wi-Fis), we denote by *0* the class that represents a single Wi-Fi AP and by *1* the class that represents 2 Wi-Fi APs. Next,

we compute the mean μ and standard deviation σ only on the training set. We check for outliers and replace the values that are larger than 4σ with the μ value (e.g., there are only 4 such values in class *1*).

The data for the two classes have different ranges (from about -45.46 to -26.93 dBm for class *0*, and from about -52.02 to about -22.28 dBm for class *1*). Thus, we normalize the data D in the standard way: $ND = \frac{(D-\mu)}{\sigma}$, where ND is the normalized data output, μ and σ are the mean and standard deviation computed on the training data. We attach the appropriate label to each chunk of the data. The overall size of the data after the preparation to detect one or two Wi-Fi APs is about 382 MB, where the Wi-Fi APs are on opposite sides of the LTE-U BSS and placed at 6 feet distance from the LTE-U BSS). The final size of the collected data is 3.4 GB.

For training, we do not insert values from different numbers of Wi-Fi APs into a single chunk. The received signal in the LTE-U BSS has higher energy on average for more Wi-Fi APs, thus there are differences in the mean values for each dataset. Our data preparation script handles many possible numbers of Wi-Fi APs and generates the data in the format that can be used for model training and inference (we follow the format for datasets from the UCR archive).

Neural network models: FC, VGG and FCN Our data is treated as a univariate time-series for each chunk. There are many different models proposed for the standard time-series benchmark [23].

First, we test *fully connected (FC)* neural networks. For simple architectures with two linear layers followed by the ReLU non-linearity the maximum accuracy achieved is about 90%. More linear layers, or using other non-linearities (e.g. sigmoid) and weight decays do not help to increase the accuracy of the model significantly. Thus, next we extract more patterns from the data using the convolutional layers.

Second, we adapt the *VGG* network [115] to the one dimensional classification task. We

changed the number of weight layers to 6 (we also tested 7, 5, and 4 layers, but found that 6 gives the highest test accuracy of about 99.52%). However, the drawback is that with fewer convolutional layers, the fully connected layers at the end of *VGG* net become bigger to the point that it hurts the performance (for 4 weight layers it drops to about 95.75%). This architecture gives us higher accuracy but is rather difficult to adjust to small data.[1]

Finally, one of the strongest and flexible models called *FCN* is based on convolutional neural networks that find general patterns in time-series sequences [124]. The advantages of the model are: simplicity (no data-specific hyper-parameters), no additional data pre-processing required, no feature crafting required, and significant academic and industrial effort into improving the accuracy of convolutional neural networks [31, 66].

The architecture of the FCN network contains three blocks, where each of them consists of a convolutional layer, followed by batch normalization $f(x) = \frac{x-\mu}{\sqrt{\sigma^2+\epsilon}}$ (where ϵ is a small constant added for numerical stability) and ReLU activation function $y(x) = \max(0, x)$. There are 128, 256, and 128 filter banks in each of the consecutive 3 layer blocks, where the sizes of the filters are: 8, 5, and 3, respectively. We follow the standard convention for Convolutional Neural Networks (CNNs) and refer to the discrete cross-correlation operation as convolution. The input x to the first convolution is the time-series data chunk with a single channel c. After its convolution with f filters, with filters denoted as y, the output feature map o has f channels. For training, we insert $s = 32$ time-series data chunks into a mini-batch. We have $j \in f$ and the discrete convolution [122] that can be expressed as:

$$o = x * y \tag{8.1}$$

1. The dimensionality of the data is reduced slowly because of the small filter of size 3.

and in the Einstein notation:

$$o_{(s,j)} = \sum_{i \in c} x_{(s,i)} \cdot y_{(j,i)} \tag{8.2}$$

ML models from scikit-learn To diversify the machine learning models used in our comparison, we select the most popular models from the scikit-learn (also denoted as *sklearn*) library [2]. The library exposes classical machine learning algorithms implemented in Python. This is a common tool used for science and engineering. We run our experiments using *sklearn* version 0.19.1 with Python 3.6. We analyze how the following models perform on our WiFi data and report their test accuracy. The decision tree is a simple classifier that learns decision rules inferred from the data features. The deeper the tree, the more complex the decision rules and the fitter the model. The decision tree classifier achieves accuracy of 79.46% for the task of distinguishing between one or two Wi-Fi APs. The AdaBoost [58] classifier is one of the best out-of-the-box models in the *sklearn* library that creates an ensemble of classifiers. In our experiments, AdaBoost begins by fitting a decision tree classifier on the original dataset and then fits additional decision tree classifiers on the same dataset but where the weights of incorrectly classified instances are modified such that subsequent classifiers focus more on difficult cases. It is tuned by adjusting the maximum number of the decision tree classifiers used. AdaBoost achieves accuracy of 94.57%. Random Forest is an averaging algorithm based on randomized decision trees. Its test accuracy is 79.87%. We find that the best tested model from the *sklearn* library is AdaBoost. The highest test accuracy achieved for AdaBoost for the standard case with two Wi-Fi APs is worse by about 5% when compared to the overall best FCN model (described in section 8.2.3), which achieves accuracy of 99.38% for the same configuration (with 2 Wi-Fi APs, 512 chunk size, NLOS, and 6 feet distance). For more than 5 classes, Random Forest model achieves higher accuracy

2. https://scikit-learn.org/stable/index.html

than AdaBoost.

Time-series specific models BOSS in Vector Space (BOSS VS) model [112] is a time-series classification algorithm, whose properties make it suitable for our task. This algorithm is characterized by fast inference, tolerance to noise that enable us to achieve high test accuracy, moderate training time, which allows for periodic model updates. Moreover, BOSS VS achieves best test accuracy for repetitive and long time-series data. Within the time-series specific models, we also compared to WEASEL [110], which yielded lower test accuracy despite much longer training time.

We run the BOSS VS time-series specific model for the NLOS 6 feet case. Other time-series models train much longer (in the order of days) on our large (a few GBs) time-series data or do not fit even into 128 GB of RAM memory provided. We observe that from 2 to up to 4 WiFi APs, the performance of the BOSS VS model is on-par with the performance of FCN model. However, for the scenario where we have to distinguish between 0 to 5 WiFi APs, the accuracy of the FCN model is higher by about 7%. One concern with the BOSS VS model is that we have to use a machine with 128 GB of RAM to train the model and for larger data sizes, the out of memory exception is thrown as well (the model is implemented in Java). For the FCN, we are able to scale to arbitrary amount of data. Based on the thorough experimental analysis, we see the FCN model and other neural network based models as the most accurate and scalable models that can be used to predict the number of Wi-Fi APs.

Real-time inference We deploy the model in real-time, which is similar to the energy data collection experiment setup, and is shown in Fig. 8.3. We prepare the model only for the inference task in the following steps. Python scripts load and deploy the trained PyTorch model. We set up the Wi-Fi devices and generate some network load for each device. The LTE-U BS is connected to a computer with the hardware requirements of at least 8 GB RAM (Installed Memory), 64-bit operating system, x64-based processor, Intel(R) Core i7,

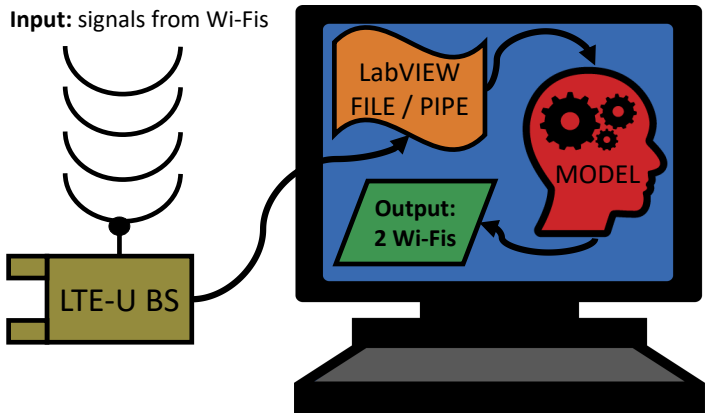


Figure 8.3: The schema of the inference process, where the input received by the LTE-U BS is signals from Wi-Fis and the output is the predicted number of Wi-Fis.

CPU clock 2.60GHz. The energy of the Wi-Fi transmission signal in a given moment in time is capture using NI LabVIEW. From the program, we generate an output file or write the data to a pipe. The ML model reads the new values from the file until it reaches the time-series chunk length. Next, the chunk is normalized and passed through the model that gives a categorical output that indicates the predicted number of Wi-Fis in the real-time environment.

8.2.4 Performance comparison between HD, ED, AC and ML methods

We analyze and study the performance differences between HD, ED, AC and ML methods for different configuration setups and discus the inference delay. In ML method, we validate the performance on ML real-time inference data. For the final evaluation, we train a single Machine Learning model that is based on the FCN network and used for all the following experiments. The model is trained on the whole dataset of size 3.4 GB, where the train and test sets are of the same size of about 1.7 GB.

Comparison between ML methods We present comparison between ML methods in Fig. 8.4. The time-series specific neural network models, such as FCN as well as BOSS

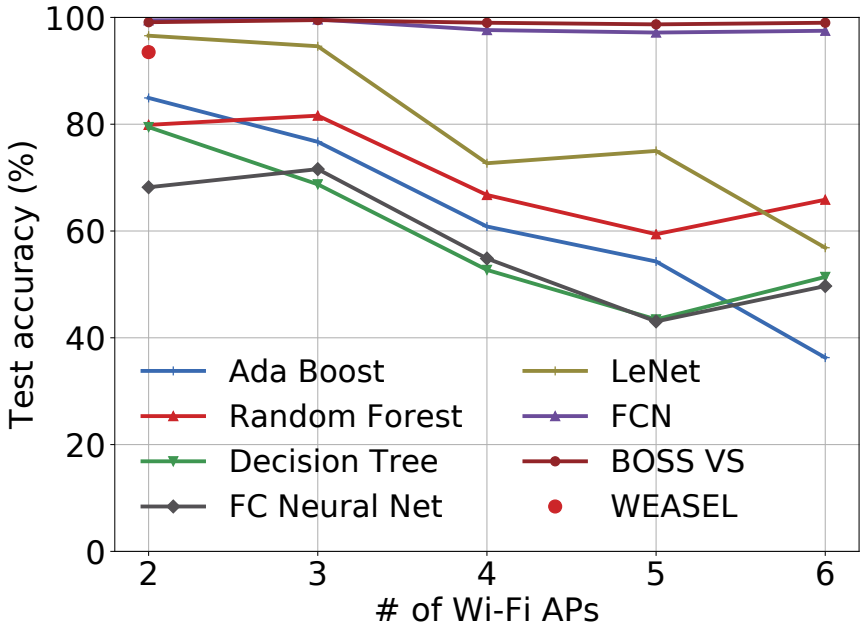


Figure 8.4: Comparison of test accuracy for different ML methods. Number of Wi-Fi APs equals to 2 denotes the Case D configuration (NLOS, 6 feet). Thus, 2 on the x axis corresponds to distinguishing between 1 and 2 Wi-Fi APs, whereas 3 denotes distinguishing between 0, 1, or 2 Wi-Fi APs. Similarly, the values on the x axis (4,5) denote distinguishing from 0 to (x-1) WiFi APs.

VS, perform much better than the general purpose models from scikit-learn library. The middle-ground between the two options is a simple two-layer convolutional network called *LeNet*. The main benefit of using FCN (MEDIUM) or BOSS VS is greater model learning capacity than *LeNet* or scikit-learn models. There is a negligible difference in terms of test accuracy between the FCN and BOSS VS models. However, the FCN models can scale to much bigger data sizes and we observe that the BOSS VS model often goes out of memory for more than a few GBs of input data. Thus, we select FCN as our main Machine Learning (ML) model for all the remaining experiments.

Successful Detection at Fixed Distance We compare the ML performance with HD[3],

3. The successful Wi-Fi detection in HD for LOS and NLOS scenario is 100%. Hence we have not included in the Fig. 8.1.

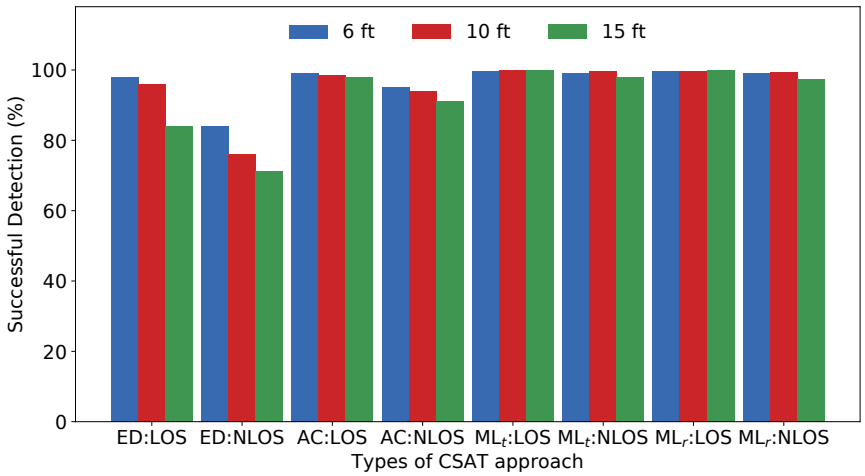


Figure 8.5: Comparison of results for successful detection between ED, AC and ML methods. ML results are presented for the test data (denoted as ML_t:) and for the real time inference (denoted as ML_r:).

ED and AC approaches using the NI USRP platform as shown in Fig. 8.1. Similarly we compare the performance of HD by analyzing the Wi-Fi BSSID through wireshark capture. In the experiment, Wi-Fi APs are transmitting full buffer data, along with beacon and probe response frames following the 802.11 CSMA specification. We performed different experiments with 6ft, 10ft and 15ft for LOS and NLOS scenarios. Fig 8.5 shows the performance of detection for LOS and NLOS scenarios. In ED and AC based approach the proposed detection algorithm achieves the successful detection on average at 93% and 95% for LOS scenario. Similarly, the algorithm achieves 80% and 90% for the NLOS scenario. In this work, we show that ML approach can achieve close to 100% successful detection rate for both LOS and NLOS, and different distance scenarios (6ft, 10ft & 15ft). We observe the ML approach works close to the performance of HD.

Table 8.3 shows the performance of detection for fixed distance configuration setup. From, this table the number of Wi-Fis columns represents the number of Wi-Fi APs deployed in the coexistence setup. The number of Wi-Fi AP 2 corresponds to distinguishing between 1 and 2 Wi-Fi APs, whereas 3 denotes distinguishing between 0, 1, or 2 Wi-Fi APs and so on.

Table 8.3: Performance of detection for fixed distance configuration setup.

Conf.	Classes	HD (%)		ED (%)		AC (%)		ML (%)	
Distance	# of APs	LOS	NLOS	LOS	NLOS	LOS	NLOS	LOS	NLOS
6F	2	100	100	96	91	98	96	98.60	99.10
	3	100	100	88	85	95	90	99.10	99.50
	4	100	100	80	74	87	81	99.40	99.00
	5	100	100	74	62	76	65	99.20	98.70
	6	100	100	62	51	70	59	99.30	99.0
10F	2	100	100	94	89	97	94	99.80	99.98
	3	100	100	86	82	91	88	99.80	99.98
	4	100	100	78	72	85	79	99.80	99.90
	5	100	100	72	60	75	63	99.50	99.85
	6	100	100	64	54	68	57	99.80	99.84
15F	2	100	100	92	87	95	90	99.80	99.80
	3	100	100	84	80	85	81	99.90	99.60
	4	100	100	75	70	79	71	99.90	99.60
	5	100	100	70	58	71	64	99.60	99.50
	6	100	100	63	53	66	55	99.50	99.40

In all cases the performance of ML is close to 100%.

Additional Delay to Detect the Wi-Fi AP To study the additional delay to detect a Wi-Fi AP, we consider a 5 Wi-Fi AP deployment scenario, where, Wi-Fi AP 1 and Wi-Fi AP 2 at 6 feet are ON, Wi-Fi AP 3 and Wi-Fi AP 4 at 10 feet are ON and Wi-Fi AP 5 at 15 feet is ON. We observe a large number of Wi-Fi packets on the air and moreover the LTE-U ON cycle interference impacts the delay in Wi-Fi transmissions. In HD, the total time for the LTE-U BS to decode the BSSID is 1.4 seconds (i.e., Wi-Fi 1st BSSID beacon packet + LTE-U detects K beacon + Additional layer complexity + NI USRP RIO hardware processing time). In ED, the total time for the energy based CSAT algorithm to adopt or change the duty cycle from 50% to 33% is 5.9 seconds (i.e., Wi-Fi 1st beacon transmission time + LTE-U detects K beacon (or) data packets time + NI USRP RIO hardware processing time) as shown in Table 8.4. In AC, the total time for the AC based CSAT algorithm to change the duty cycle from 50% to 33% is 4.8 seconds (i.e., Wi-Fi 1st L-STF packet frame + LTE-U detects L-STF frame time + NI USRP RIO hardware processing time). In ML, the total

Table 8.4: Other additional delay to detect the Wi-Fi AP due to the NI hardware

CSAT Types	NI HW Delay
Header Decoding (HD)	1.4 S
Energy Detection (ED)	5.9 S
Auto-correlation (AC)	4.8 S
Machine Learning (ML)	3.1 S

time for the CSAT algorithm to adopt the duty cycle from 50% to 33% is about 3.1 seconds. This approach is dependent on the chunk size (in this case set to 512).

8.3 ML-based classification of device environment using Wi-Fi and cellular signal measurements

The 6 GHz rules [44] create two different power regimes for unlicensed devices: "indoor" devices that are subject to lower transmit powers (Low Power Indoors or LPI) but are not required to access an Automatic Frequency Control (AFC) database to obtain permission to use a channel, and "outdoor" devices, that can transmit at a higher power but need to consult an AFC prior to using a channel to ensure that the device is not in the exclusion zone for the desired channel, as shown in Fig. 8.6. Very Low Power (VLP) devices shown in Fig. 8.6 have yet to be authorized in the US but are permitted in other regulatory regimes: these devices can be anywhere, do not need to consult an AFC but will transmit at lower power than LPI devices.

Since there are no reliable means for determining if a wireless device is indoors or outdoors, other restrictions were mandated for LPI: indoor access points (APs) could not be battery powered, have detachable antennas or a weatherized exterior, and mobile client devices connected to an indoor AP were subject to a 6 dB lower transmit power constraint (proposed by FCC) compared to the indoor AP since they could be outdoors and pose an interference threat to incumbents if they were to transmit at the same power as an indoor device. These constraints clearly lead to sub-optimal spectrum usage: for example, client

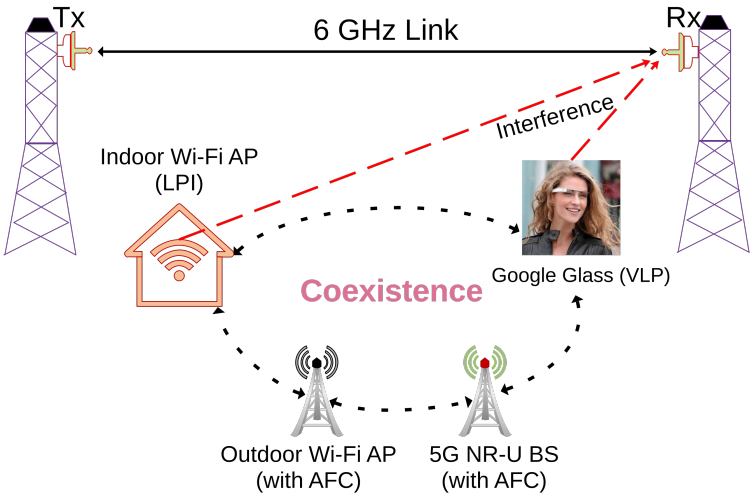


Figure 8.6: Deployment scenario of indoor and outdoor devices in 6 GHz

devices even if they are indoors have to transmit at a lower power, client devices cannot transmit directly to each other without connecting through an AP, and APs being unable to be battery powered can lead to a less resilient network. Hence, the ability of a wireless device to reliably detect its own environment allows device power allocations that do not need to be constrained by external factors and can lead to improved spectrum utilization and increased resilience.

The fundamental premise of our approach in this work [89] is simple: just as the indoor visual environment is quite different from the outdoor visual environment, the same is true for the radio frequency (RF) environment as well. RF transmissions permeate our surroundings: television (TV), radio (AM/FM), cellular and Wi-Fi being the most pervasive. The most obvious difference between indoor and outdoor environments is the signal strength: transmissions from outdoor sources such as Global Positioning System (GPS) satellites, TV transmitters, cellular towers, and radio stations will be received at higher power outdoors while predominantly indoor transmitters such as Wi-Fi will have higher signal strength indoors. There are other differences as well: the number of Wi-Fi APs and cellular base-stations

Table 8.5: Summary of data collected

Location	**Indoor**	**Outdoor**	**Total**
Chicago	9049	6850	15899
Colorado	605	20283	20888
New York	45742	130241	175983
Total	55396	157374	212770

(BSs) received by a device such as a smartphone will also depend on the environment. Today, it is possible to extract detailed information on both signal strength and number of Wi-Fi APs and cellular BSs received by a smartphone, over frequency bands from the unlicensed 2.4 GHz and 5 GHz bands to the low (< 1 GHz), mid (1 GHz - 6 GHz) and high (> 24 GHz) cellular bands, directly, using apps. We posit that such a data-set, collected in labeled indoor and outdoor environments, across a wide variety of frequency bands and signal types, can be used to train Machine Learning (ML) models that can perform robust indoor/outdoor classification, thus leading to improved spectrum usage, incumbent protection and resilience, not only in 6 GHz, but also in future bands such as the 12 GHz satellite band where sharing with indoor devices is being considered [43].

8.3.1 SigCap data collection and pre-processing

SigCap is used to passively collects GPS, Wi-Fi, 4G and 5G information using the Android API, without requiring root access or running bandwidth-hungry speed tests. Table 3.2 shows the full parameters collected every 10 secs. Depending on the phone capabilities and the cellular deployment, the app collects the listed data on all deployed 4G bands including the unlicensed 5 GHz (Band 46) and Citizen Broadband Radio Service (CBRS, Band 48) and on all 5G bands including mmWave.

Data collection methodology. Once the data has been collected and saved on the phone, it can be exported as JavaScript Object Notation (JSON) files, which then converted to Comma Separated Values (CSV) format and used as inputs to the ML models. For data

Table 8.6: Features used in Statistical Analysis

Features	**Count**	**Mean**	**Min**	**Max**	**Std**
Wi-Fi 2.4 GHz RSSI	✓	✓	✓	✓	✓
Wi-Fi 5 GHz RSSI	✓	✓	✓	✓	✓
LTE Low RSRP	✓	✓	✓	✓	✓
LTE Mid RSRP	✓	✓	✓	✓	✓
LTE Low RSRQ	✓	✓	✓	✓	✓
LTE Mid RSRQ	✓	✓	✓	✓	✓
NR FR1 RSRP	✓	✓	×	×	×
NR FR2 RSRP	✓	✓	×	×	×
NR FR1 RSRQ	✓	✓	×	×	×
NR FR2 RSRQ	✓	✓	×	×	×

label, a user-input category field is incorporated in the app prior to exporting the captured data with the options of "indoor" and "outdoor".

We used several Android phones in our data collection effort: Google Pixel 2, Google Pixel 3, Google Pixel 5, Samsung Galaxy S9, Samsung Galaxy S20, Samsung Galaxy S21 and Motorola Edge+, each equipped with a Subscriber Identification Module (SIM) of a different operator. The variety of devices and operators adds diversity to the collected signal parameters (*e.g.*, RSSI, RSRP, RSRQ), since each phone model has different modem chip as well as receiving antennas and front-ends. Outdoor measurements were collected while walking, biking, driving a car, and riding on trains in urban, suburban and rural environments. Indoor measurements were made in single-family houses, apartment buildings, offices, indoor malls and stores. Both indoor and outdoor measurements were collected in the various places described in three different geographical locations: the number of data records from each location is summarized in Table. 8.5. It should be noted here that the number and diversity of outdoor environments captured was greater than indoor, since access to most indoor places was restricted due to shut downs in the past year.

Data pre-processing. The data-set thus collected is quite large: 18 GB. Depending on the measurement environment, a single data record can contain information on 100s of Wi-Fi

APs and many 10s of LTE cells: this is common in dense urban areas. Thus, the raw data cannot be used directly in a ML classifier since the number of inputs per data record would vary with each record. We pre-process the data as follows:

Step 1: The data is cleaned by removing any record with an invalid entry in any field. Null entries, NaN (Not a Number) entries and RSRP, RSRQ and RSSI values that do not fall in the specified range[4] for these parameters are examples of invalid entries. Invalid entries are represented by a very large number, *i.e.,* -200 so the ML algorithm will not be affected by these data points.

Step 2: Since a single record has a varying number of Wi-Fi and LTE cells, we calculate aggregate values as feature inputs to the ML model in order to have the same number of features for each record. As shown in Table 8.6 we first classify the signals into bands: Wi-Fi RSSI in 2.4 GHz and 5 GHz, LTE RSRP and RSRQ in low- and mid-band and NR RSRP and RSRQ in FR1 and FR2. Then, all signal values detected in a band are aggregated using 5 functions: mean, min, max, standard deviation, and count, thus removing the variability between records. For NR FR1 and FR2 data, SigCap only report one RSRP and RSRQ per entry, however this may change in future Android updates. Hence, we have 38 features in Table 8.6 combined with "GPS Accuracy" field in a set of 39 features for use with classification algorithms.

8.3.2 ML algorithm evaluation

Before proceeding to ML classification, we performed univariate analysis on the various features (as shown in Table 8.6) to evaluate the statistical differences between indoor and outdoor data.

4. For 2.4 and 5 GHz Wi-Fi, RSSI varies in the range of -100 dbm to -20 dBm. In LTE, low-band RSRP varies in the range of -150 dBm to -35 dBm and mid-band RSRP varies in the range of -130 dBm to -50 dBm. Similarly, in NR FR1 RSRP varies in the range of -120 dBm to -60 dBm and in NR FR2 RSRP varies in the range of -120 dBm to -70 dBm. The RSRQ is in the range of -20 to -5

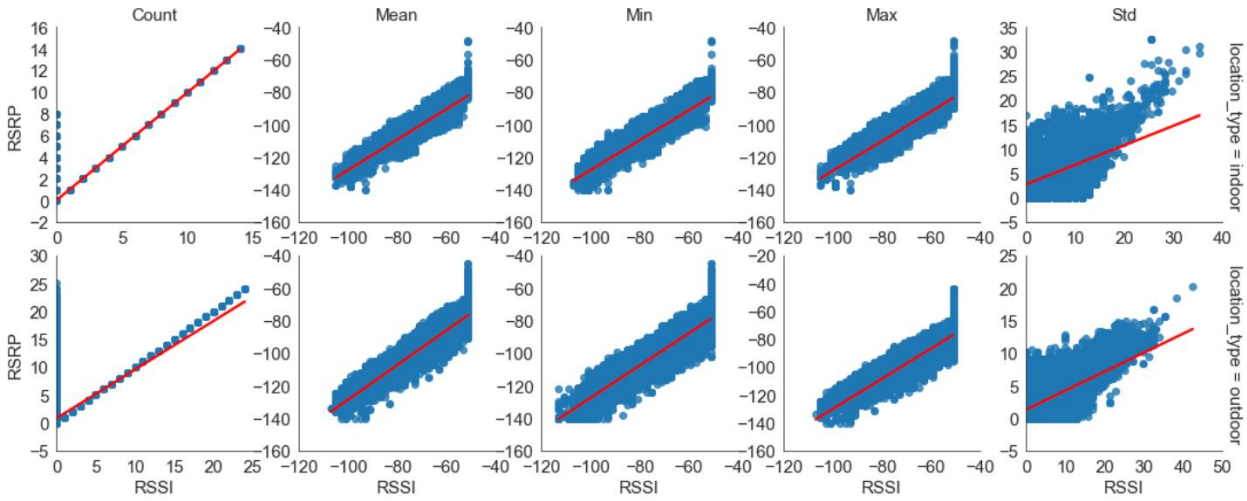


Figure 8.7: Correlation Analysis: LTE (Low + Mid) RSSI and RSRP Features.

We observed high correlation between RSSI and RSRP, and between RSSI and RSRQ in LTE low- and mid-bands, as shown in Fig. 8.7. This is expected since RSSI is a function of RSRP and RSRQ, thus LTE RSSI can be omitted for further ML analysis. On the other hand, Fig. 8.8 shows that LTE RSRP and RSRQ are not highly correlated. This is also expected since: RSRP is a measure of the cell's received power while RSRQ is a measure of interference due to neighboring cells.

Figs. 8.9a, 8.9b, 8.10a, and 8.10b show the distribution of Wi-Fi 2.4 GHz & 5 GHz AP count and mean RSSI[5] indoors and outdoors. We observe clear differences between indoors and outdoors in the Wi-Fi 2.4 GHz AP count and Wi-Fi 5 GHz RSSI mean. Similarly, Figs. 8.9c, 8.9d, 8.10c, and 8.10d show the LTE Low and Mid band count and mean RSRP distributions. Once again, we observe clear differences between the distributions of indoor and outdoor data. Figs. 8.9e, 8.9f, 8.10e, and 8.10f, show the count and mean RSRP for 5G NR deployment in FR1 and FR2. We have not observed any deployment of 5G NR in the FR2 band indoors due to the penetration loss of mmWave signals from outdoors to indoors. Similarly, we analyzed the GPS accuracy and we observe difference between the indoor and

5. We also analyzed the univariate performance in terms of min, max, and standard deviation of the RSSI values. However, due to space limitation, we show only the count and mean.

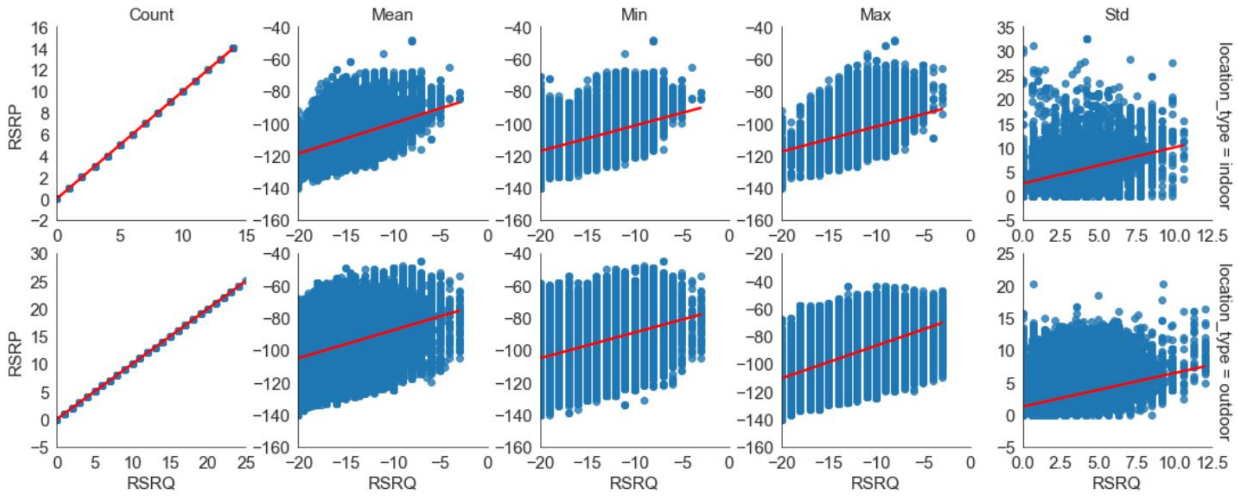


Figure 8.8: Correlation Analysis: LTE (Low + Mid) RSRQ and RSRP Features.

outdoors as shown in Fig. 8.11.

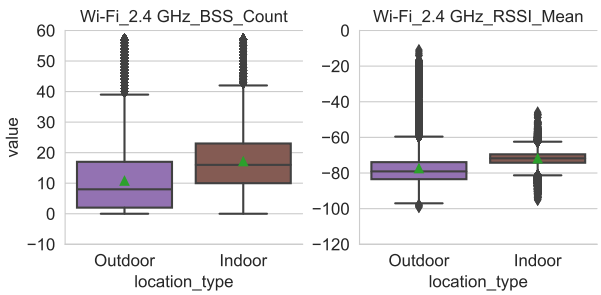
This preliminary statistical analysis indicates that these 39 features can be used in classical ML models to distinguish between indoor and outdoor environments reliably. We tested various ML models in the standard way: the data collected is divided into a training set containing 75% and test set containing 25% of the data. We use the ML models implemented in Scikit Learn [85, 50] with default parameters value.

ML Algorithms. The indoor/outdoor classification problem can be addressed by a number of well-know ML classifiers. We evaluated the following:

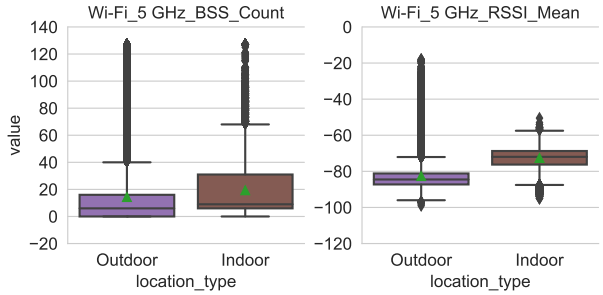
- *Naive Bayes (NB/NBayes):* A classification technique based on Bayes' theorem [68] with an assumption of independence between features.

- *Linear Discriminant Analysis (LDA):* LDA is a dimensionality reduction technique and is mainly used as a pre-processing step in ML. LDA is also used for binary classification problems

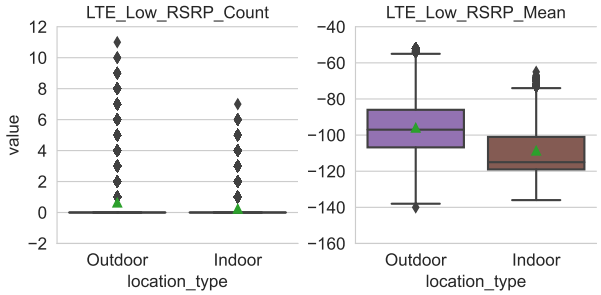
- *AdaBoost:* AdaBoost is one of the first boosting algorithms to be adapted. It helps to combine multiple "weak classifiers" into a single "strong classifier". It works by putting



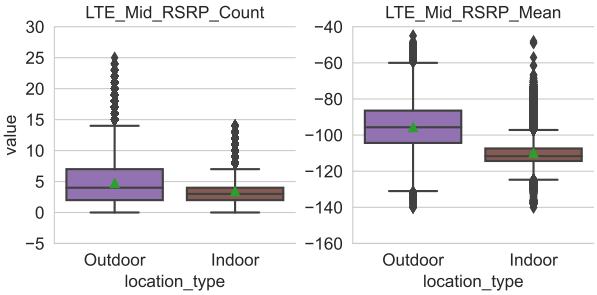
(a) Wi-Fi 2.4 GHz Count & Mean RSSI



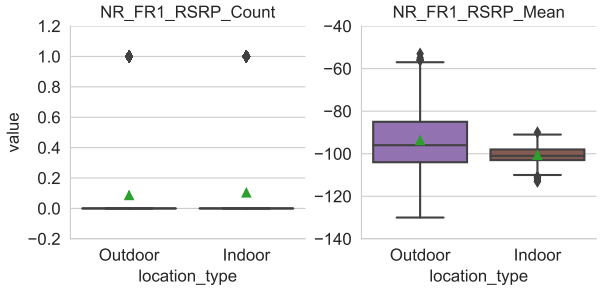
(b) Wi-Fi 5 GHz Count & Mean RSSI



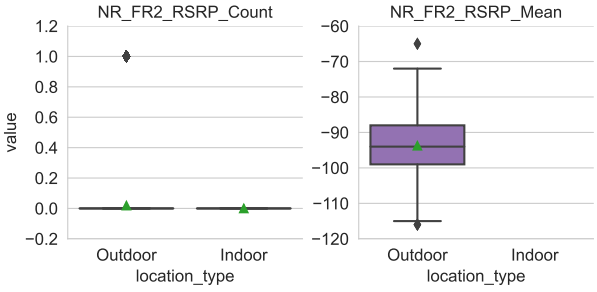
(c) LTE-Low Count & Mean RSRP



(d) LTE-Mid Count & Mean RSRP

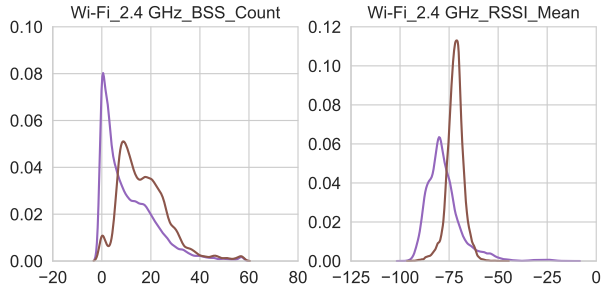


(e) NR FR1 Count & Mean RSRP

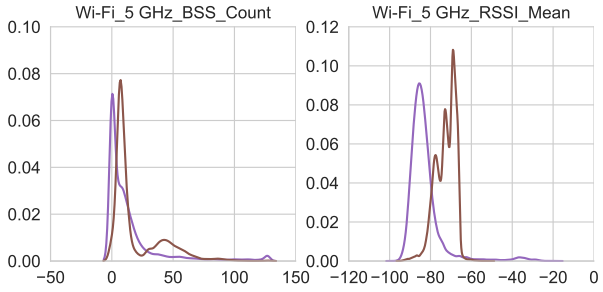


(f) NR FR2 Count & Mean RSRP

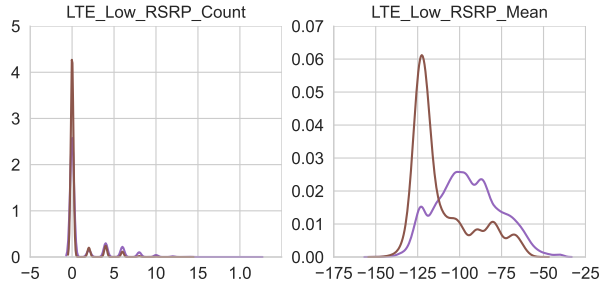
Figure 8.9: Univariate Analysis on Wi-Fi, LTE and NR Features



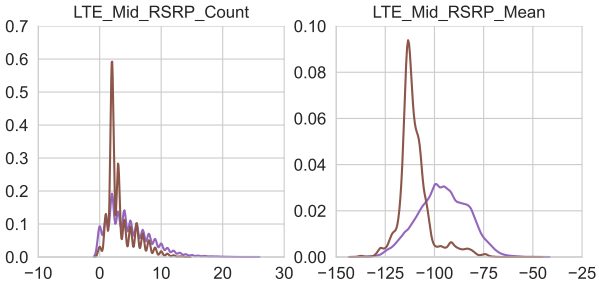
(a) Wi-Fi 2.4 GHz Count & Mean



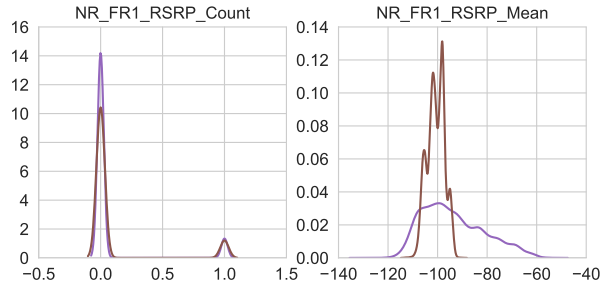
(b) Wi-Fi 5 GHz Count & Mean



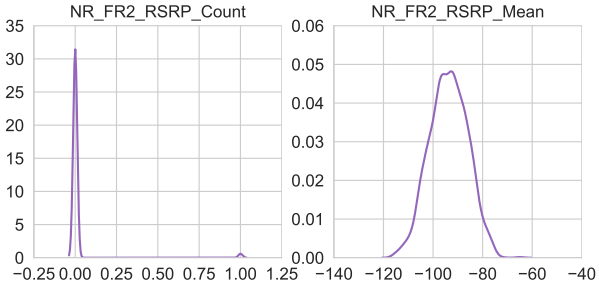
(c) LTE-Low Count & Mean



(d) LTE-Mid Count & Mean

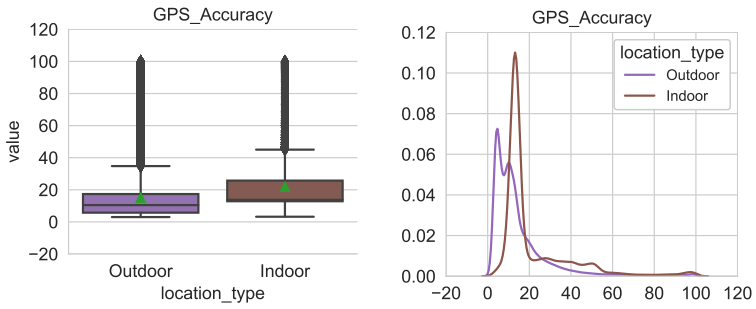


(e) NR FR1 Count & Mean



(f) NR FR2 Count & Mean

Figure 8.10: Univariate Distribution Analysis on Wi-Fi, LTE and NR Features



(a) (b)

Figure 8.11: Univariate Analysis on GPS Accuracy

more weight on difficult to classify instances and less on those already classified.

- *Decision Tree (DecTree):* The data is split into two or more homogeneous sets, based on the most significant features to make as distinct groups as possible.

- *Extra Trees (ExTree):* ExTree is an ensemble ML algorithm that uses the predictions (majority voting) from many decision trees trained on the training dataset for classification.

- *XGBoost:* This algorithm is an extension of gradient boosted decision trees [127] and is designed to improve speed and performance.

- *Random Forest (RF/RForest):* RF is an ensemble of decision trees. In order to classify a new observation based on features, RF applies majority voting on the classification given by each decision tree. The difference between RF and ExTree is in the way they select the cut points to split the nodes in the decision trees. RF chooses the optimal split, whereas ExTree chooses it randomly.

Performance Metrics [19] The following standard metrics were used to evaluate the performance of the above algorithms:

- *Accuracy:* Percentage of correctly predicted records (Indoor and Outdoor Combined).

Table 8.7: F1-score of different ML algorithms on test data for indoor/outdoor classification

Feature Set	**Naive Bayes**	**LDA**	**Ada-Boost**	**Decision Tree**	**XG-Boost**	**ExTree**	**Random Forest**
5G NR	9.3%	85.3%	85.2%	85.6%	85.6%	85.6%	85.6%
5G NR + GPS Accuracy	11.5%	85.1%	87.3%	87.0%	89.6%	87.3%	87.9%
LTE	80.3%	90.2%	91.7%	94.9%	95.0%	96.3%	96.3%
LTE + GPS Accuracy	80.6%	90.3%	92.9%	95.1%	96.3%	96.7%	97.1%
Wi-Fi	94.7%	93.0%	96.1%	98.3%	98.6%	98.8%	98.8%
Wi-Fi + GPS Accuracy	94.7%	93.1%	96.1%	98.2%	98.8%	98.7%	98.8%
NR + LTE + Wi-Fi + GPS Accuracy	37.9%	94.5%	96.6%	98.7%	99.3%	99.4%	99.4%

- *True Positive Rate (TPR)/Recall:* Percentage of correctly predicted outdoor records.
- *True Negative Rate (TNR):* Percentage of correctly predicted indoor records.
- *Precision:* Percentage of correctly identified records among the ones which are classified as outdoor.
- *F1-Score:* Harmonic mean of precision and recall.
- *Area under the curve (AUC):* The AUC is the measure of the ability of a classifier to distinguish between classes.

Performance of ML models. We evaluated the classification performance of various ML algorithms, using different combinations of features on the collected data. Our results, using several standard ML algorithms implemented using Scikit-learn, are shown in Table 8.7, where the F1-score of different algorithms tested with different combinations of feature sets is shown. It is clear that as more frequency bands are added to the feature set, the F1-score

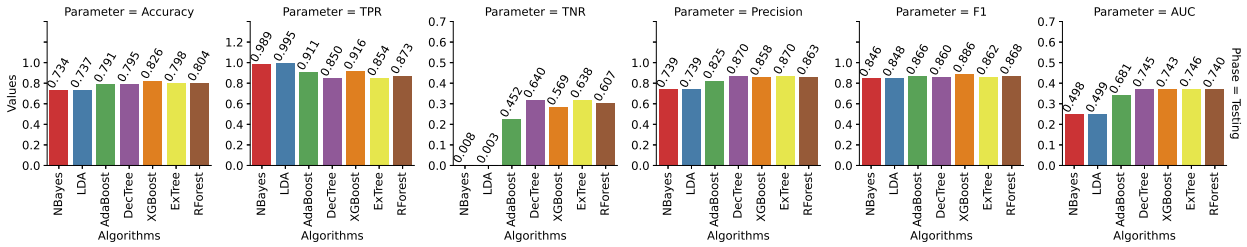


Figure 8.12: Performance of ML models using only the GPS Accuracy feature in terms of Accuracy, TPR, TNR, Precision, F1-Score and AUC.

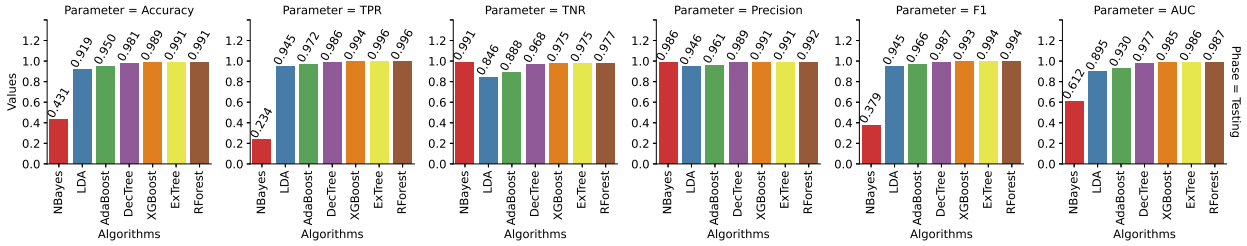


Figure 8.13: Performance of ML models using all the 39 features in terms of Accuracy, TPR, TNR, Precision, F1-Score and AUC.

increases, especially for the tree-based models such as AdaBoost, Decision Tree, XGBoost, ExTree, and Random Forest. We also observed that only Wi-Fi and LTE features are sufficient to get good classification accuracy for indoor as well as outdoor, but adding the NR and GPS accuracy features lead to slight improvement in AdaBoost, XGBoost, and ExTree.

Fig. 8.12 shows the GPS accuracy performance of different ML models on the test data. The XGBoost and Random Forest algorithms guarantee 82.6% and 80.4% accuracy. From the observation, it is clear that we cannot reliably detect indoor and outdoor environments with only GPS accuracy feature. Fig. 8.13 shows the performance of different ML models on the test data when all 39 features are used. The NB algorithm performs poorly *i.e.*, 43%, when all features are used. Since NB assumes that all the features are uncorrelated, the prediction probability reduces significantly even if one of the features has a wrong likelihood probability. XGBoost, ExTree, and Random Forest models consistently outperformed other models for all the feature combinations (see Table 8.7). Especially when all features are

Table 8.8: Random Forest 10-Fold Cross Validation

Metrics		Mean	Std. Dev.
Accuracy	Test	0.9925	0.0004
	Train	0.9999	0
TPR	Test	0.9971	0.0002
	Train	1	0
TNR	Test	0.9928	0.0007
	Train	0.9999	0
F1-score	Test	0.9949	0.0003
	Train	0.9999	0

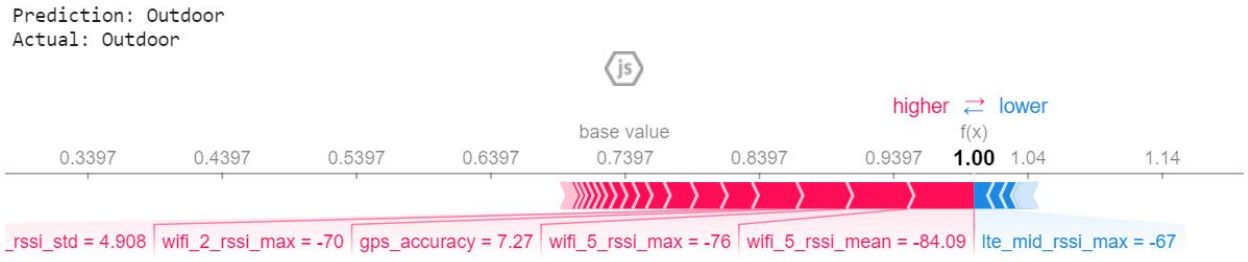


Figure 8.14: Random Forest Explainability: Correct Outdoor Prediction.

used, XGBoost, ExTree, and Random Forest models have above 99% F1-score. This high F1-score also indicates that the ensemble ML models are making accurate predictions for indoor as well as outdoor records (despite the data imbalance between the two classes). We also performed 10-fold cross-validation for the Random Forest model, and the corresponding results are shown in Table 8.8. It shows that the Random Forest model consistently performs above 99% accuracy and F1-score on all the folds. Since the accuracy and the F1-score from the models are already high, hyper parameter tuning of these models is not needed. Hence, a separate validation set is not used.

ML Explainability Study: In this section, we study the explainability of the best performing ML model, *i.e.*, Random Forest, using the SHAP (SHapley Additive exPlanations [73, 72]) package in Python. The SHAP package helps visualize the importance of the input features in classifying a given record as indoor or outdoor. Fig. 8.14 shows the SHAP values for the features of a record which was correctly classified as outdoor by the RF model. The

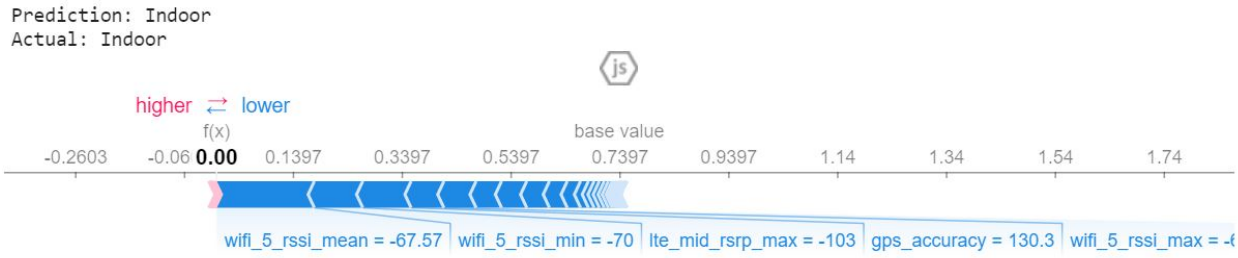


Figure 8.15: Random Forest Explainability: Correct Indoor Prediction.

red and blue arrows indicate the features that push the model towards predicting the record as outdoor and indoor, respectively. The length of an arrow indicates the importance of the feature in deciding the prediction. For example, in Fig. 8.14, the feature Wi-Fi 5GHz RSSI mean (-84 dBm) is the most important feature to make the model classify the record as outdoor. This behavior is consistent with what we observed from univariate analysis (see Fig. 8.9b and Fig. 8.10b): a lower value for Wi-Fi 5GHz RSSI mean indicates that the record is most likely from outdoor. Similarly, Fig. 8.15 shows the SHAP values for the features of a record which was correctly classified as indoor by the RF model.

Fig. 8.16 shows the summary of the SHAP values for 100 test records. The points which are to the left and right of the zero line indicates the importance of the features in making indoor and outdoor prediction, respectively. The color of a point indicates the feature value (red indicates high feature value and blue indicates low feature value). It is clear from Fig. 8.16 that high value for Wi-Fi RSSI feature pushes the model towards making indoor prediction and low value pushes the model towards making outdoor prediction. In contrast, low value for LTE feature pushes the model towards making indoor prediction and high value pushes towards outdoor prediction. Similarly, Fig. 8.17 shows the important feature for prediction in LDA.

Deep Neural Network (DNN) Model We implemented a DNN model using the Scikit Learn package to analyze the classification performance of Neural Networks. The DNN consists of two hidden layers containing 64 neurons in each layer. We trained the DNN

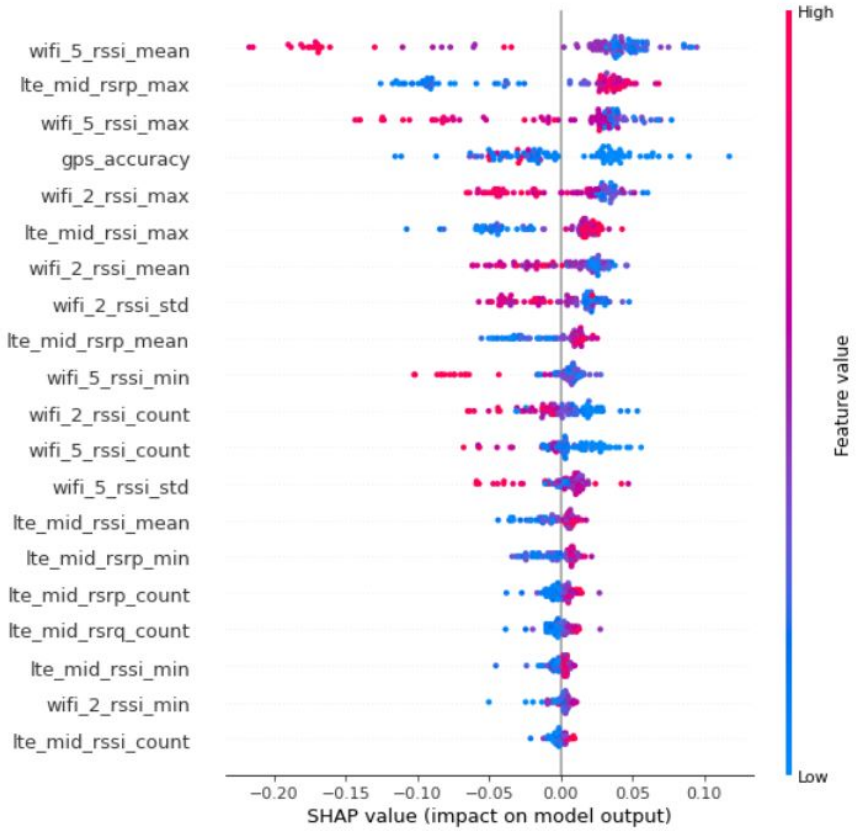


Figure 8.16: Random Forest: Feature Importance

model with the learning rate of 0.001, and the optimizer used is Adam with the number of epochs as 100 and batch size as 200. The test accuracy of the DNN model is 98.7%, and test F1-Score is 99.1%. DNN is performing on-par with other ML models. Since this is a simple tabular classification problem, ensemble ML models are sufficient.

8.3.3 Test Scenarios

The previous section demonstrated that Random Forest performed extremely well in the indoor/outdoor classification task when tested in the conventional way against a training and test set where the test data set consisted of measurements from the same environments that were included in the training data set. In this section, we are interested in testing the ML model on data collected in environments that were not included in developing the ML

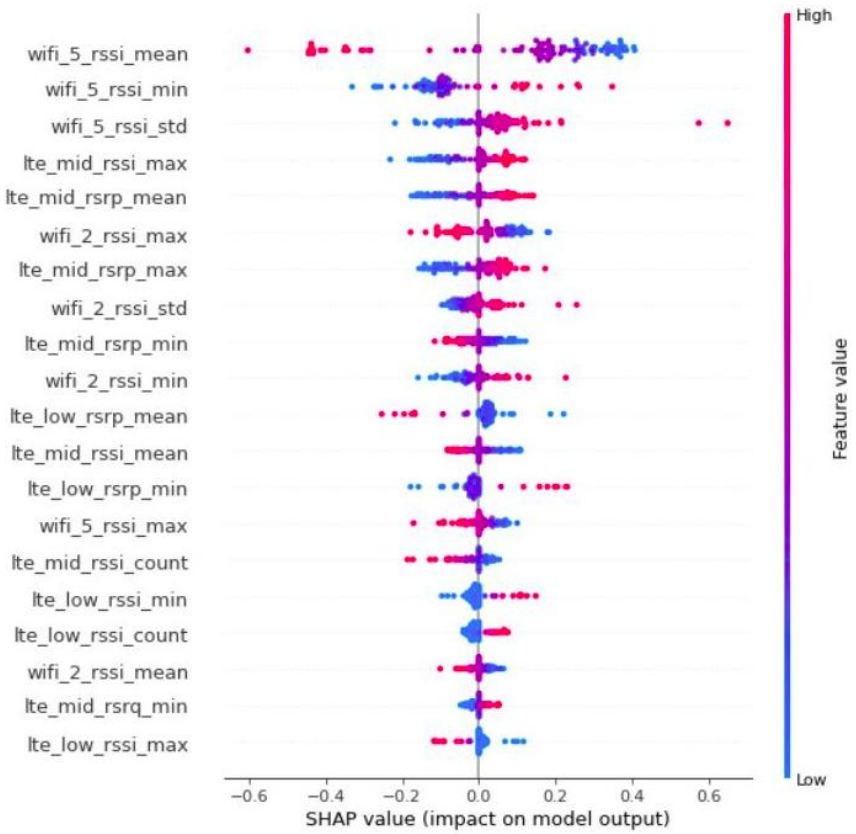


Figure 8.17: LDA: Feature Importance

models. To do so, we studied two different test cases described below. The app was used to collect data both indoors and outdoors in these environments.

- **Location 1**, TacoBell is a restaurant, with very large glass windows facing the street as shown in Figs. 8.18a and 8.18b.
- **Location 2**, WholeFood is a grocery store, again with very large glass windows facing the street as shown in Figs. 8.18c and 8.18d.

Table 8.9 summarizes the classification performance in these two environments, first without including any of the data in building the trained model and then adding 20% of the new data to retrain the ML model. The overall F1-scores using the ML model trained on the original data were 67% and 61% in TacoBell and WholeFood respectively. These improved

(a) TacoBell Outdoor

(b) TacoBell Indoor

(c) WholeFood Outdoor

(d) WholeFood Indoor

Figure 8.18: Test Cases: TacoBell and WholeFood

to 79% and 71% when 20% of the data was used to retrain the model. Interestingly, we observe that the TPR (probability of classifying outdoors correctly) was 100% in all cases, while the TNR (probability of classifying indoor correctly) was quite low. We believe that this is due to two reasons: (i) in both locations, the large street-side windows caused the indoor environment to appear more like an outdoor one in terms of the RF signal levels perceived at the phone; and (ii) our data-set has more and diverse outdoor records than indoor records. From an interference potential perspective, the ML algorithm performance is actually desirable: an indoor device near a window or open door has the same interference potential as an outdoor device as was noted in a recent filing to the FCC where devices near windows or open doors had very high interference levels at incumbent receivers [70].

There are two ways to address the ML performance in such scenarios: (i) increase the representation of diverse indoor environments in the data set. We see that including just 20% of the data from the new environment in the training set improved classification accuracy,

Table 8.9: Performance of Random Forest in classifying TacoBell and WholeFood

Location	**ML model**	**Accuracy**	**F1-Score**	**TPR**	**TNR**
TacoBell	Original	53%	67%	100%	11%
TacoBell	With 20%	75%	79%	100%	53%
WholeFood	Original	54%	61%	100%	24%
WholeFood	With 20%	69%	71%	100%	51%

even though this was a very small percentage (.04%) of the overall training set; or (ii) create three classes: indoors, indoors near windows and outdoors. The second approach would be the best to address the application we are interested in where we use device environment to determine transmit power levels: a device near a window could be subject to a transmit power requirement in between a fully indoor and fully outdoor device. Both options require creating a more diverse data set, especially of indoor measurements since indoor environments tend to be more diverse than outdoor ones. Just as image recognition performance improved dramatically as image databases grew larger and incorporated diverse images, we are confident that as these types of RF data-sets grow, RF based indoor/outdoor classification will improve as well.

8.4 Summary and List of Accomplishments

We've conducted comprehensive studies exploring machine learning (ML) algorithms for two crucial challenges in wireless resource management. First, we analyzed various ML algorithms for real-time detection of active Wi-Fi access points based solely on energy values. This novel approach outperforms conventional energy and auto-correlation detection methods, demonstrating its potential to improve LTE-U duty cycle adaptation and broader Wi-Fi frequency management.

Secondly, we utilized SigCap, our API-based tool, to collect a wide range of RF parameters for ML-based indoor/outdoor classification. Thorough model evaluation revealed

Random Forest's superior performance. However, this approach has shortcomings when differentiating diverse environments (*e.g.*, stadiums, tall buildings), thus we plan to expand our dataset by capturing complex signal dynamics with specialized indoor classes. We envision that such ML-based methods, coupled with data collected by API-based tools, can play a pivotal role in future rule-making. By enabling devices to accurately self-identify their indoor/outdoor status, they can seamlessly adhere to appropriate 6 GHz power regimes and optimize spectrum usage.

The following papers has been published in the topic of machine learning in wireless networks:

- Adam Dziedzic et al. "Machine Learning enabled Spectrum Sharing in Dense LTE-U/Wi-Fi Coexistence Scenarios". In: *IEEE Open Journal of Vehicular Technology 1* (2020), pp. 173–189

- Arun Ramamurthy et al. "ML-Based Classification of Device Environment Using Wi-Fi and Cellular Signal Measurements". In: *IEEE Access 10* (2022), pp. 29461–29472.

CHAPTER 9

CONCLUSION AND FUTURE DIRECTIONS

In this chapter, we provide a summary of the contributions, discuss open issues and future directions, and finally conclude.

9.1 Summary of Contributions

1. **The Device-Based Measurement Methodology:** We developed a framework for a comprehensive analysis of deployed wireless networks (*i.e.*, 4G, 5G, Wi-Fi) called device-based measurement. This methodology framework provides the basis of all of our measurement works. In particular, it consists of two approaches: API-based and root-based. Our API-based tool, SigCap, provides an easy-to-use solution for cellular and Wi-Fi signal information using standard Android APIs. For scenarios requiring deeper signal analysis, we employ root-based tools like Network Signal Guru, Accuver XCAL, and QualiPoc. These root-based tools offer detailed data access using root privileges but face challenges in setup, cost, and data extraction. We flexibly tailor our approach: SigCap for general analysis, while root-based tools for specialized investigation. This allows us to maximize the benefits of each approach while mitigating their limitations. Our API-based methodology has been utilized in the FCC's pilot wireless measurement program as a part of the Broadband DATA Act [46], and in the SpectrumX's Broadband Map US project [59].

2. **LTE and Wi-Fi Coexistence Studies:** We initially utilized our device-based measurement methodology to rapidly validate simulation findings and explore real-world network behavior. Simulations suggested potential Wi-Fi and LAA throughput and latency gains when Wi-Fi lowers its LTE energy detection threshold to -82 dBm. This treats LTE-LAA/LTE-U as coexisting Wi-Fi rather than noise. Our methodology,

applied to actual LAA and Wi-Fi deployments, confirmed this finding. We observed Wi-Fi throughput degradation and connectivity problems due to the default asymmetrical energy detection threshold, especially when Wi-Fi primary channel and LAA channel overlap.

3. **The Wi-Fi 6E (6 GHz) Deployment Studies:** We have significantly advanced our device-based approach, focusing on the API-based tool, SigCap. Our first of their kind, large-scale measurement campaigns across two university campuses (UMich and UND), reveal negligible interference from LPI APs to the 6 GHz fixed point-to-point links. Outdoor RSSI values range from -64 to -95 dBm (median -89 dBm), with significant attenuation caused by double-pane low-emission windows (12-16 dB loss) and brick walls (25-33 dB loss). Focusing on walking measurements, median RSSI values were -82 dBm (UMich) and -79.5 dBm (UND). These values equal or exceed proposed C2C activation thresholds, suggesting potential unintended outdoor activation. Even considering the highest observed RSSI (-45 dBm), calculated interference-to-noise ratios remain well below harmful levels for fixed point-to-point links. The low 5% detectability of indoor BSSIDs outdoors further reinforces the minimal impact of LPI on incumbents.

4. **Survey and Analysis of 5G Deployments:** We thoroughly examined various aspects of 4G and 5G deployments across low-band, mid-band, and high-band/mmWave using our device-based methodology. In downtown Chicago, we confirmed the dense 5G mmWave deployments have delivered a significantly higher data rate than 4G+LAA/CBRS. This throughput gain are linked to wider channels and beamwidth, but distance, body blockage, thermal throttling, and obstructions remain to be limitations in mmWave deployments. Next, 5G mmWave beam selection analysis revealed that open fields generally enable optimal beam choices, while urban canyons lead to sub-optimal beams and an average 3.6 dBm signal loss. This highlights beamforming challenges in complex urban environments. In low- and mid-bands, 4G with LAA/CBRS aggregation

can match or exceed 5G mid-band throughput, though coexistence (LAA) and TDD synchronization (CBRS) challenges remain. When analyzed individually (*i.e.*, ignoring aggregation), 5G mid-band outperforms other bands in both downlink and uplink. Higher bandwidth, deployment density, and beam count are major drivers of throughput growth, with slight increase in MIMO performance. On the other hand, we observe missing new 5G features such as MU-MIMO and 1024-QAM modulation. Lastly, T-Mobile's NR-SA demonstrates superior latency compared to NR-NSA and LTE due to lower signaling overhead and denser mid-band deployments.

5. **Cellular Coexistence in the 3 GHz Spectrum:** Building on our 4G/5G analysis, we identified potential adjacent channel interference (ACI) and co-channel interference (CCI) within the 3 GHz spectrum. Our comprehensive device-based study on CBRS and C-Band ACI revealed severe throughput degradation due to lack of guard bands, power disparities, and asynchronous TDD. A 20 MHz gap significantly improved throughput (CBRS: 60% to 21%, C-band: 43% to 30%), highlighting the impact of out-of-band interference. Next, our South Bend CBRS study found that secondary coexistence among GAA CBSDs, even within the same network, can limit performance. Concentrated use of certain frequencies, coupled with adjacent CBRS and C-Band deployments, caused issues. Collaborating with the CBRS provider, we demonstrated that changing a CBSD's frequency improved signal quality. However, SAS limitations hindered rapid adjustments, revealing the need for dynamic, measurement-driven channel allocation. Importantly, aggregated 4G CBRS outperformed 5G C-band, underscoring the value of CBRS for both large and small providers.

6. **Machine Learning in Wireless Networks:** Our research focuses on using machine learning (ML) for two key challenges in wireless resource management. Firstly, we explored ML algorithms for real-time Wi-Fi access point detection using solely energy values. This outperforms traditional methods, showing promise for LTE-U duty cycle

adaptation and broader Wi-Fi management. Secondly, we used our API-based tool, SigCap, to collect diverse RF parameters for ML-based indoor/outdoor classification. Random Forest performed best, but differentiating complex environments (e.g., stadiums, tall buildings) remains a challenge. We'll expand our dataset and specialize indoor classes to improve model accuracy. We believe ML methods, supported by API-based data collection, can revolutionize future spectrum rule-making. By enabling devices to self-identify their indoor/outdoor status, they can optimize 6 GHz power usage for improved spectrum efficiency.

9.2 Future Directions

- **Scaling Up the Device-based Methodology for Nation-wide Survey of Wireless Network:** 5G/NextG deployments continue to expand, with the US National Telecommunications and Information Administration (NTIA) announcing the intent to study the lower 3 GHz (3.1-3.45 GHz), the 7 GHz band, and other potential bands for future wireless broadband uses. This underscores the needs of continuous monitoring of new spectrum and features deployments, quantifying their performance improvements to inform future standards development. To this end, infrastructures (*i.e.*, servers) are required to scale-up and streamline our methodology, enabling a seamless, large-scale wireless measurement. The large-scale dataset collected in this campaign can be publicly released to advance research in areas like machine learning predictions. For this, we collaborate with undergraduate students across multiple universities within the SpectrumX group, to conduct extensive surveys of cellular and Wi-Fi deployments throughout the US. There are challenges in student onboarding, data collection, and analysis processes. Currently, we address these challenges by distributing pre-configured measurement phones, utilizing a centralized data repository, along with scripts and tools like ArcGIS for analysis.

- **TDD Synchronization Problem:** The lack of synchronization between radio access technologies (RATs) using TDD channels creates the potential for overlapping and adjacent channel interference. To address this, we aim to determine the precise timing of DL and UL slots and subframes in a TDD system. We will use both Software Defined Radio (SDR) to capture I/Q samples for detailed spectral analysis and Accuver XCAL to pinpoint RB allocations in the frequency and time domains. With this combined information, we can determine the exact timing of DL and UL transmissions, allowing us to develop strategies to synchronize subframes and mitigate collision-based interference.

- **Prediction of Backhaul Throughput Performance using Wi-Fi Performance:** Current home broadband measurement techniques often require an Ethernet connection to avoid the potential bottleneck of Wi-Fi, adding a barrier of technical setup for users. In some homes, particularly rental units, Wi-Fi may be the only connectivity option readily available. This raises the question: can we reliably predict whether a Wi-Fi connection will likely be a bottleneck for broadband performance tests, using readily accessible information from the Wi-Fi chipset itself? To investigate this, we plan to collect data from South Bend homes using Raspberry Pi devices. These devices will conduct hourly throughput tests over both Ethernet and Wi-Fi, while simultaneously capturing Wi-Fi information such as version, transmission rates, number of MIMO layers, RSSI, and the number of neighboring access points. We will then explore machine learning techniques to analyze this data with the goal of reliably predicting Wi-Fi performance limitations.

- **6 GHz Client-to-Client Sensitivity Threshold6 GHz Client-to-Client Sensitivity Threshold:** The FCC is actively exploring techniques to safely increase utilization of the 6 GHz spectrum while protecting fixed-link incumbents. One promising approach is Client-to-Client (C2C) communication, which enables direct links between

indoor client devices without relying on an access point (AP). To avoid interference with incumbents, it's crucial for devices to remain restricted to indoor environments. Since C2C relies on an "enabling signal" transmitted from the AP, clients need to determine their eligibility for C2C based on the received signal strength (RSSI) of this signal. Setting an appropriate RSSI threshold is critical for this process. A threshold that is too high risks allowing outdoor clients to communicate at LPI levels, potentially interfering with incumbents. Conversely, a threshold that's too low could prevent some eligible indoor clients from using C2C, reducing its effectiveness. We plan to conduct experiments in dense 6 GHz deployments to help the FCC determine the optimal enabling signal level for C2C..

9.3 Concluding Remarks

We have introduced a device-based methodology to evaluate the performance of wireless networks. We demonstrated that the methodology which includes SigCap and root-based apps, is capable of actively and passively measure network performance of an actual operator deployment at a user device. We also shown the flexibility of this methodology with the measurements of multiple radio technologies (*i.e.*, Wi-Fi, 4G, 5G) within different use cases (*i.e.*, network performance analysis, coexistence study, mmWave beam analysis, ML-based classification).

This device-based approach holds significant promise for the future of wireless networks. By capturing data directly from user devices operating within operational networks, we gain valuable insights into real-world network behavior under dynamic conditions. While powerful, our device-based methodology can be further enhanced by establishing connected infrastructures that streamline data capture and analysis. The analysis extracted from our device-based measurements can guide informed spectrum allocation decisions, facilitate the development of robust coexistence strategies, optimize network configurations, and ulti-

mately accelerate the design of future next-generation wireless systems that deliver enhanced user experiences.

REFERENCES

[1] 3rd Generation Partnership Project. *3GPP Release-15*. http://www.3gpp.org/release-15/. 2016.

[2] 3rd Generation Partnership Project. *3GPP Release-16*. http://www.3gpp.org/release-16/. 2021.

[3] 3rd Generation Partnership Project. *TS 38.101-1 5G; NR; User Equipment (UE) radio transmission and reception; Part 1: Range 1 Standalone 17.5.0 Release 17*. 2022.

[4] 3rd Generation Partnership Project. *TS 38.214 5G; NR; Physical layer procedures for data version 17.1.0 Release 17*. 2022.

[5] 3rd Generation Partnership Project. *TS 38.306 5G; NR; User Equipment (UE) radio access capabilities 17.0.0 Release 17*. 2022.

[6] 3rd Generation Partnership Project. *TS 38.331 5G Radio Resource Control (RRC) version 16.1.0 Release 16*. 2020.

[7] 802.11 WG - Wireless LAN Working Group. *IEEE 802.11ax-2021*. https://standards.ieee.org/ieee/802.11ax/7180/. Accessed: Apr. 2024.

[8] Accuver. *XCAL - PC based Advanced 5G Network Optimization Solution*. https://www.accuver.com/sub/products/view.php?idx=6. Accessed: Apr. 2024.

[9] Md Navid Akbar et al. "Capacity Enhancement of Indoor 5G mmWave Communication by Beam Steering and Narrowing". In: *2018 10th International Conference on Electrical and Computer Engineering (ICECE)*. IEEE. 2018, pp. 85–88.

[10] Monica Alleven. *AT&T takes advantage of early C-band clearing*. Accessed: Nov. 2023. 2023. URL: https://www.fiercewireless.com/5g/att-takes-advantage-early-c-band-clearing.

[11] Monica Alleven. *T-Mobile's 5G network gets capacity boost from MU-MIMO: report*. https://www.fiercewireless.com/tech/t-mobiles-5g-network-gets-capacity-boost-mu-mimo-report. Accessed: Apr. 2024.

[12] João Almeida et al. "Mitigating adjacent channel interference in vehicular communication systems". In: *Digital Communications and Networks* 2.2 (2016), pp. 57–64.

[13] Android. *Android Developers: Documentation for HardwarePropertiesManager*. https://developer.android.com/reference/android/os/HardwarePropertiesManager, accessed October 2021.

[14] Android. *Android Developers: Documentation for TelephonyManager*. https://developer.android.com/reference/android/telephony/TelephonyManager, accessed July 2021.

[15] R. Bendlin (AT&T). *Common Preamble Design in the 6 GHz Band – Merits and Challenges*. 2019.

[16] Wissal Attaoui et al. “Beam alignment game for self-organized mmwave-empowered 5g initial access”. In: *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE. 2019, pp. 2050–2057.

[17] AWS. *AWS Local Zones*. `https://aws.amazon.com/about-aws/global-infrastructure/localzones/`. Accessed: Apr. 2024.

[18] Jason Carpenter et al. “Multi-Modal Vehicle Data Delivery via Commercial 5G Mobile Networks: An Initial Study”. In: *2023 IEEE 43rd International Conference on Distributed Computing Systems Workshops (ICDCSW)*. IEEE. 2023, pp. 157–162.

[19] Diogo V Carvalho, Eduardo M Pereira, and Jaime S Cardoso. “Machine learning interpretability: A survey on methods and metrics”. In: *Electronics* 8.8 (2019), p. 832.

[20] Celona, Inc. *Basics of Celona MicroSlicing for Private Cellular*. `https://www.celona.io/5g-lan/network-and-micro-slicing`. Accessed: Apr. 2024. 2022.

[21] Eugene Chai et al. “LTE in unlicensed spectrum: Are we there yet?” In: *Proc. of ACM 22nd Annual International Conference on Mobile Computing and Networking*. 2016, pp. 135–148.

[22] Mingzhe Chen et al. “Artificial neural networks-based machine learning for wireless networks: A tutorial”. In: *IEEE Communications Surveys & Tutorials* (2019).

[23] Yanping Chen et al. “The ucr time series classification archive”. In: (2015).

[24] M. Dano. *FierceWireless: Verizon touts 1.4 Gbps LTE speeds with unlicensed spectrum, carrier aggregation*. Accessed: Dec. 2019.

[25] Mike Dano. *The quiet brilliance of T-Mobile’s 5G spectrum strategy*. Accessed: Nov. 2023. 2022. URL: `https://www.lightreading.com/5g/the-quiet-brilliance-of-t-mobile-s-5g-spectrum-strategy`.

[26] *Derf’s Test Media collection*. 2021. URL: `https://media.xiph.org/video/derf`.

[27] Android Developers. *Build Location-Aware Apps*. `https://developer.android.com/training/location`, accessed March 2020.

[28] Android Developers. *Wi-Fi Scanning Overview*. `https://developer.android.com/guide/topics/connectivity/wifi-scan`, accessed March 2020.

[29] Seda Dogan-Tusha et al. “Evaluating the interference potential in 6 GHz: An extensive measurement campaign of a dense indoor Wi-Fi 6E network”. In: *Proceedings of the 17th ACM workshop on wireless network testbeds, experimental evaluation & characterization*. 2023, pp. 56–63.

[30] Seda Dogan-Tusha et al. “Indoor and Outdoor Measurement Campaign for Unlicensed 6 GHz Operation with Wi-Fi 6E”. In: *2023 26th International Symposium on Wireless Personal Multimedia Communications (WPMC)*. IEEE. 2023, pp. 1–6.

[31] Adam Dziedzic et al. “Band-limited Training and Inference for Convolutional Neural Networks”. In: *Proc. of International Conference on Machine Learning*. 2019, pp. 1745–1754.

[32] Adam Dziedzic et al. "Machine Learning enabled Spectrum Sharing in Dense LTE-U/Wi-Fi Coexistence Scenarios". In: *IEEE Open Journal of Vehicular Technology* 1 (2020), pp. 173–189.

[33] EPiQ Solutions. *PRiSM: Handheld network scanner and spectrum analyzer*. https://epiqsolutions.com/rf-sensing/prism/. Accessed: Apr. 2024. 2023.

[34] EPRI. *FirstEnergy 6 GHz additive interference study*. https://www.epri.com/research/products/000000003002025484. Accessed: Jun. 2023. 2022.

[35] EPRI. *FirstEnergy 6 GHz additive interference study: Phase 2 Winter*. https://www.fcc.gov/ecfs/document/10509026197735/1. Accessed: Jun. 2023. 2023.

[36] Ericsson. *T-Mobile, Ericsson exceed 1 Gbps with LAA demo*. 2017.

[37] ETSI/BRAN. *Draft ETSI EN 303 687 v0.0.13 (2021-06-24)*. 2021.

[38] Evergy. *6 GHz interference study*. https://www.fcc.gov/ecfs/document/10301057343002/2. Accessed: Jun. 2023. 2023.

[39] Evergy. *Wi-Fi 6E and 6 GHz microwave testing*. https://www.fcc.gov/ecfs/document/12082732114548/2. Accessed: Jun. 2023. 2022.

[40] FCC. *Report and Order and Further NPRM, 3.45 - 3.55 GHz*. https://docs.fcc.gov/public/attachments/DOC-366780A1.pdf. Accessed: Apr. 2024.

[41] FCC Licence Search. *Microwave Industrial/Business Pool License-WQVS717*. https://wireless2.fcc.gov/UlsApp/UlsSearch/licenseSiteMap.jsp?licKey=3696758. Accessed: Jun. 2023.

[42] FCC Licence Search. *TV Intercity Relay License- WLD493*. https://wireless2.fcc.gov/UlsApp/UlsSearch/licenseSiteMap.jsp?licKey=989128. Accessed: Jun. 2023.

[43] FCC, Notice of Proposed Rule making: In the Matter of Expanding Flexible Use of the 12.2 - 12.7 GHz band. https://docs.fcc.gov/public/attachments/FCC-21-13A1.pdf. 2021.

[44] FCC, Report and Order and Further Notice of Proposed Rule making: In the Matter of Unlicensed Use of the 6 GHz Band. https://docs.fcc.gov/public/attachments/FCC-20-51A1.pdf. 2020.

[45] FCCAPPs. *FCC Speed Test*. https://play.google.com/store/apps/details?id=com.samknows.fcc&gl=US&pli=1. Accessed: Apr. 2024.

[46] Federal Communications Commission. *REPORT TO THE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION OF THE SENATE AND THE COMMITTEE ON ENERGY AND COMMERCE OF THE HOUSE OF REPRESENTATIVES*. https://www.fcc.gov/sites/default/files/report-congress-usps-broadband-data-collection-feasibility-05242021.pdf. Accessed: Apr. 2024.

[47] Filipa Fernandes et al. "Beam Management in mmWave 5G NR: an Intra-Cell Mobility Study". In: *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. IEEE. 2021, pp. 1–7.

[48] Rostand AK Fezeu et al. “Mid-Band 5G: A Measurement Study in Europe and US”. In: *arXiv preprint arXiv:2310.11000* (2023).

[49] Bevin Fletcher. *CBRS boosts Verizon 4G speeds 79% but power levels show limits*. https://www.fiercewireless.com/tech/cbrs-boosts-verizon-4g-speeds-79-power-levels-show-limits. Accessed: Nov. 2023.

[50] Raul Garreta and Guillermo Moncecchi. *Learning scikit-learn: machine learning in python*. Packt Publishing Ltd, 2013.

[51] Camillo Gentile et al. “Millimeter-Wave Channel Measurement and Modeling: A NIST Perspective”. In: *IEEE Communications Magazine* 56.12 (2018), pp. 30–37. DOI: 10.1109/MCOM.2018.1800222.

[52] Monisha Ghosh. *Re: Ex Parte Notification for Unlicensed Use of the 6 GHz Band, OET Docket No. 18-295*. https://www.fcc.gov/ecfs/document/107211592305290/1. Accessed: Apr. 2024.

[53] Monisha Ghosh et al. “Coexistence of LTE-LAA and Wi-Fi: Analysis simulation and experiments”. In: *P802. 11 Coexistence SC Workshop*. 2019.

[54] Monisha Ghosh et al. *Comment on ”Unlicensed Use of the 6 GHz Band; and Expanding Flexible Use in Mid-Band Spectrum Between 3.7 and 24 GHz”*. https://www.fcc.gov/ecfs/document/10328785722855/1. Accessed: Apr. 2024.

[55] Moinak Ghoshal et al. “Performance of Cellular Networks on the Wheels”. In: *Proceedings of the 2023 ACM on Internet Measurement Conference*. 2023, pp. 678–695.

[56] Marco Giordani et al. “A tutorial on beam management for 3GPP NR at mmWave frequencies”. In: *IEEE Communications Surveys & Tutorials* 21.1 (2018), pp. 173–196.

[57] Lorenza Giupponi et al. “Simulating LTE and Wi-Fi coexistence in unlicensed spectrum with ns-3”. In: *arXiv preprint arXiv:1604.06826* (2016).

[58] Trevor Hastie et al. “Multi-class adaboost”. In: *Statistics and its Interface* (2009), pp. 349–360.

[59] Zoey Howell-Brown. *SpectrumX Announces New Partnership for Speed Tests with Historically Black Colleges*. https://broadbandbreakfast.com/spectrumx-announces-new-partnership-for-speed-tests-with-historically-black-colleges/. Accessed: Apr. 2024.

[60] Intel. *C2C triggering based on LPI signal strength*. https://www.fcc.gov/ecfs/document/1027285708759/1. Accessed: Jun. 2023. 2022.

[61] *iPerf3 - The TCP, UDP and SCTP network bandwidth measurement tool*. https://iperf.fr/. Accessed: Apr. 2024.

[62] Naru Jai et al. “Optimal channel allocation in the CBRS band with shipborne radar incumbents”. In: *DySPAN*. IEEE. 2021, pp. 80–88.

[63] Ish Kumar Jain, Raghav Subbaraman, and Dinesh Bharadia. "Two beams are better than one: Enabling reliable and high throughput mmWave links". In: *arXiv preprint arXiv:2101.04249* (2021).

[64] Manav Kohli et al. "Outdoor-to-Indoor 28 GHz Wireless Measurements in Manhattan: Path Loss, Environmental Effects, and 90% Coverage". In: *arXiv preprint arXiv:2205.09436* (2022).

[65] Eva Lagunas, Christos Tsinos, and Symeon Sharma Chatzinotas. "5G cellular and fixed satellite service spectrum coexistence in C-band". In: *IEEE Access* (2020).

[66] Andrew Lavin and Scott Gray. "Fast algorithms for convolutional neural networks". In: *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition*. 2016, pp. 4013–4021.

[67] Yu-Ngok Ruyue Li et al. "Beam management in millimeter-wave communications for 5G and beyond". In: *IEEE Access* 8 (2020), pp. 13282–13293.

[68] Dennis V Lindley. "Fiducial distributions and Bayes' theorem". In: *Journal of the Royal Statistical Society. Series B (Methodological)* (1958), pp. 102–107.

[69] Lockard & White, Inc. *PGEENG230227-6GHz interference attachment*. `https://www.fcc.gov/ecfs/document/10425175025173/1`. Accessed: Jun. 2023.

[70] Lockard & White, Inc. *Test Report on the Effects of 6 GHz Unlicensed RLAN Units on Fortson to Columbus Microwave Link*. `https://www.fcc.gov/ecfs/document/106231367519302/2`. Accessed: Apr. 2024.

[71] LTE-U Forum. *LTE-U CSAT Procedure TS V1.0*. 2015.

[72] Scott M Lundberg and Su-In Lee. "A unified approach to interpreting model predictions". In: *Proceedings of the 31st international conference on neural information processing systems*. 2017, pp. 4768–4777.

[73] Scott M Lundberg et al. "From local explanations to global understanding with explainable AI for trees". In: *Nature machine intelligence* 2.1 (2020), pp. 56–67.

[74] Morteza Mehrnoush et al. "Analytical modeling of Wi-Fi and LTE-LAA coexistence: Throughput and impact of energy detection threshold". In: *IEEE/ACM Transactions on Networking* 26.4 (2018), pp. 1990–2003.

[75] Morteza Mehrnoush et al. "On the fairness of Wi-Fi and LTE-LAA coexistence". In: *IEEE Transactions on Cognitive Communications and Networking* 4.4 (2018), pp. 735–748.

[76] Arvind Narayanan et al. "A Comparative Measurement Study of Commercial 5G mmWave Deployments". In: *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. 2022, pp. 800–809.

[77] Arvind Narayanan et al. "A variegated look at 5G in the wild: performance, power, and QoE implications". In: *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*. 2021, pp. 610–625.

[78] Arvind Narayanan et al. "Lumos5G: Mapping and Predicting Commercial mmWave 5G Throughput". In: *Proceedings of the ACM Internet Measurement Conference*. 2020, pp. 176–193.

[79] National Telecommunications and Information Administration. *The National Spectrum Strategy*. https://www.ntia.gov/sites/default/files/publications/national_spectrum_strategy_final.pdf. Accessed: Apr. 2024. 2023.

[80] Viet Nguyen. *5G Continues Robust Momentum Growth and Drives Demand for More Wireless Spectrum*. https://www.5gamericas.org/5g-continues-robust-momentum-growth-and-drives-demand-for-more-wireless-spectrum/. Accessed: Apr. 2024.

[81] Catherine Sbeglia Nin. *Four drivers of Wi-Fi 6E adoption*. https://www.rcrwireless.com/20231129/fundamentals/four-drivers-of-wi-fi-6e-adoption. Accessed: Apr. 2024.

[82] Yong Niu et al. "A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges". In: *Wireless networks* 21.8 (2015), pp. 2657–2676.

[83] ns-3 developers. *ns-3-dev-lbt repository*. https://bitbucket.org/ns3lteu/ns-3-dev-lbt/src/master/.

[84] Monica Paolini and Senza Fili. "CBRS: Should the enterprise and venue owners care?" In: *Senza Fili* (2019).

[85] Fabian Pedregosa et al. "Scikit-learn: Machine learning in Python". In: *the Journal of machine Learning research* 12 (2011), pp. 2825–2830.

[86] Ziao Qin and Haifan Yin. "A Review of Codebooks for CSI Feedback in 5G New Radio and Beyond". In: *arXiv preprint arXiv:2302.09222* (2023).

[87] QTRun Technologies. *Network Signal Guru*. https://play.google.com/store/apps/details?id=com.qtrun.QuickTest. Accessed: Apr. 2024.

[88] Imran Latif (Quantenna). *Efficient and Fair Medium Sharing Enabled by a Common Preamble*. 2019.

[89] Arun Ramamurthy et al. "ML-Based Classification of Device Environment Using Wi-Fi and Cellular Signal Measurements". In: *IEEE Access* 10 (2022), pp. 29461–29472.

[90] Theodore S. Rappaport et al. "Overview of Millimeter Wave Communications for Fifth-Generation (5G) Wireless Networks—With a Focus on Propagation Models". In: *IEEE Transactions on Antennas and Propagation* 65.12 (2017), pp. 6213–6230. DOI: 10.1109/TAP.2017.2734243.

[91] Theodore S. Rappaport et al. "Wideband Millimeter-Wave Propagation Measurements and Channel Models for Future Wireless Communication System Design". In: *IEEE Transactions on Communications* 63.9 (2015), pp. 3029–3056. DOI: 10.1109/TCOMM.2015.2434384.

[92] Muhammad Iqbal Rochman. *SigCap*. https://people.cs.uchicago.edu/~muhiqbalcr/sigcap/. Accessed: Apr. 2024.

[93] Muhammad Iqbal Rochman, Vanlin Sathya, and Monisha Ghosh. "Impact of changing energy detection thresholds on fair coexistence of Wi-Fi and LTE in the unlicensed spectrum". In: *2017 Wireless Telecommunications Symposium (WTS)*. IEEE. 2017, pp. 1–9.

[94] Muhammad Iqbal Rochman, Vanlin Sathya, and Monisha Ghosh. "Outdoor-to-Indoor Performance Analysis of a Commercial Deployment of 5G mmWave". In: *2022 IEEE Future Networks World Forum (FNWF)*. IEEE. 2022, pp. 519–525.

[95] Muhammad Iqbal Rochman et al. "A Comparison Study of Cellular Deployments in Chicago and Miami Using Apps on Smartphones". In: *Proceedings of the 15th ACM Workshop on Wireless Network Testbeds, Experimental Evaluation & CHaracterization (WiNTECH'21)*. New Orleans, LA, USA, 2022, 61–68. ISBN: 9781450387033.

[96] Muhammad Iqbal Rochman et al. "A comprehensive analysis of the coverage and performance of 4G and 5G deployments". In: *Computer Networks* 237 (2023), p. 110060.

[97] Muhammad Iqbal Rochman et al. "A Comprehensive Real-World Evaluation of 5G Improvements over 4G in Low-and Mid-Bands". In: *arXiv preprint arXiv:2312.00957* (2023).

[98] Muhammad Iqbal Rochman et al. "A Measurement Study of the Impact of Adjacent Channel Interference between C-band and CBRS". In: *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE. 2023, pp. 1–7.

[99] Muhammad Iqbal Rochman et al. "Impact of Device Thermal Performance on 5G mmWave Communication Systems". In: *arXiv:2202.04830* (2022).

[100] Rohde & Schwarz. *QualiPoc Android*. `https://www.rohde-schwarz.com/us/products/test-and-measurement/network-data-collection/qualipoc-android_63493-55430.html`. Accessed: Apr. 2024.

[101] Vanlin Sathya, Muhammad Iqbal Rochman, and Monisha Ghosh. "Hidden-nodes in coexisting LAA & Wi-Fi: a measurement study of real deployments". In: *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE. 2021, pp. 1–7.

[102] Vanlin Sathya, Muhammad Iqbal Rochman, and Monisha Ghosh. "LAA/Wi-Fi Coexistence Issues: Wi-Fi Client Association and Data Transmission". In: (2021).

[103] Vanlin Sathya, Muhammad Iqbal Rochman, and Monisha Ghosh. "Measurement-based coexistence studies of LAA & Wi-Fi deployments in Chicago". In: *IEEE Wireless Communications* (2020).

[104] Vanlin Sathya, Muhammad Iqbal Rochman, and Monisha Ghosh. "Measurement-based coexistence studies of LAA & Wi-Fi deployments in Chicago". In: *IEEE Wireless Communications* 28.1 (2020), pp. 136–143.

[105] Vanlin Sathya et al. "Analysis of CSAT performance in Wi-Fi and LTE-U coexistence". In: *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE. 2018, pp. 1–6.

[106] Vanlin Sathya et al. “Auto-correlation based sensing of multiple Wi-Fi BSSs for LTE-U CSAT”. In: *Proc. of IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. 2019, pp. 1–7.

[107] Vanlin Sathya et al. “”Energy detection based sensing of multiple Wi-Fi BSSs for LTE-U CSAT””. In: *Proc. of IEEE Global Communications Conference*. 2018, pp. 1–7.

[108] Vanlin Sathya et al. “Impact of hidden node problem in association and data transmission for LAA Wi-Fi coexistence”. In: *Computer Communications* 195 (2022), pp. 187–206.

[109] Vanlin Sathya et al. “Standardization advances for cellular and Wi-Fi coexistence in the unlicensed 5 and 6 GHz bands”. In: *GetMobile: Mobile Comp. and Comm.* 24.1 (2020), 5–15. ISSN: 2375-0529. DOI: 10.1145/3417084.3417086. URL: https://doi.org/10.1145/3417084.3417086.

[110] Patrick Schäfer and Ulf Leser. “Fast and Accurate Time Series Classification with WEASEL”. In: *Proc. of ACM on Conference on Information and Knowledge Management*. CIKM ’17. USA, 2017. ISBN: 9781450349185. DOI: 10.1145/3132847.3132980. URL: https://doi.org/10.1145/3132847.3132980.

[111] Karen Schulz. *Verizon turbo charges its 5G network with the addition of more spectrum*. Accessed: Nov. 2023. 2023. URL: https://www.verizon.com/about/news/verizon-5g-network-addition-more-spectrum.

[112] Patrick Schäfer. “Scalable time series classification”. In: *Data Mining and Knowledge Discovery* 30 (Nov. 2015). DOI: 10.1007/s10618-015-0441-y.

[113] Zaid A Shamsan, Lway F Abdulrazak, and Tharek Abd Rahman. “Co-channel and adjacent channel interference evaluation for IMT-Advanced coexistence with existing fixed systems”. In: *RFM*. IEEE. 2008, pp. 65–69.

[114] Signals Research Group. *5G: THE GREATEST SHOW ON EARTH! vol. 33: MU-MIMO and the Tower of Power*. https://signalsresearch.com/issue/5g-the-greatest-show-on-earth-33/. Accessed: Apr. 2024.

[115] Karen Simonyan and Andrew Zisserman. “Very deep convolutional networks for large-scale image recognition”. In: *arXiv preprint arXiv:1409.1556* (2014).

[116] *Snapdragon X60 5G modem-RF system*. 2021. URL: https://www.qualcomm.com/products/snapdragon-x60-5g-modem.

[117] Shu Sun and Theodore S. Rappaport. “Wideband mmWave channels: Implications for design and implementation of adaptive beam antennas”. In: *2014 IEEE MTT-S International Microwave Symposium (IMS2014)*. 2014, pp. 1–4. DOI: 10.1109/MWSYM.2014.6848596.

[118] Yaohua Sun et al. “Application of machine learning in wireless networks: Key techniques and open issues”. In: *IEEE Communications Surveys & Tutorials* (2019).

[119] Tao Tao, Feng Han, and Yong Liu. "Enhanced LBT algorithm for LTE-LAA in unlicensed band". In: *2015 IEEE 26th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*. IEEE. 2015, pp. 1907–1911.

[120] Armed Tusha et al. "A Comprehensive Analysis of Secondary Coexistence in a Real-World CBRS Deployment". In: *arXiv preprint arXiv:2402.05226* (2024).

[121] Anthony Ngozichukwuka Uwaechia and Nor Muzlifah Mahyuddin. "A comprehensive survey on millimeter wave communications for Fifth-Generation Wireless Networks: Feasibility and challenges". In: *IEEE Access* 8 (2020), pp. 62367–62414.

[122] Nicolas Vasilache et al. "Fast convolutional nets with fbfft: A GPU performance evaluation". In: *arXiv preprint arXiv:1412.7580* (2014).

[123] Yuyang Wang et al. "MmWave vehicular beam selection with situational awareness using machine learning". In: *IEEE Access* 7 (2019), pp. 87479–87493.

[124] Zhiguang Wang, Weizhong Yan, and Tim Oates. "Time series classification from scratch with deep neural networks: A strong baseline". In: *Proc. of IEEE International joint conference on neural networks*. 2017, pp. 1578–1585.

[125] Dongzhu Xu et al. "Understanding Operational 5G: A First Measurement Study on Its Coverage, Performance and Energy Consumption". In: *Proceedings of the Annual conference of the ACM for computer communication*. 2020, pp. 479–494.

[126] Shaoyi Xu et al. "Opportunistic coexistence of LTE and WiFi for future 5G system: Experimental performance evaluation and analysis". In: *Ieee Access* 6 (2017), pp. 8725–8741.

[127] Jerry Ye et al. "Stochastic gradient boosted distributed decision trees". In: *Proceedings of the 18th ACM conference on Information and knowledge management*. 2009, pp. 2061–2064.

[128] Xuhang Ying, Milind M Buddhikot, and Sumit Roy. "SAS-assisted coexistence-aware dynamic channel assignment in CBRS band". In: *IEEE Transactions on Wireless Communications* 17.9 (2018), pp. 6307–6320.

[129] Alessio Zappone, Marco Di Renzo, and Mérouane Debbah. "Wireless networks design in the era of deep learning: Model-based, AI-based, or both?" In: *arXiv preprint arXiv:1902.02647* (2019).

[130] Chaoyun Zhang, Paul Patras, and Hamed Haddadi. "Deep learning in mobile and wireless networking: A survey". In: *IEEE Communications Surveys & Tutorials* (2019).

APPENDIX A

SIGCAP API HANDLERS AND LIST OF SIGCAP DATA PARAMETERS.

There are four data collection handlers that collects data from each of the respective API:

Wi-Fi handler collects information from the Wi-Fi API [28]. The Android OS handles various Wi-Fi operations in the background, *i.e.*, scanning, authenticating, etc. On every update, we force the OS to do a Wi-Fi scan using the API and read the results containing list of scanned Wi-Fi AP. However, there is a scan throttling limitation built-in the OS to reduce energy usage. When Wi-Fi scan is throttled, prior scan result is returned instead of new data, thus there can be some stale identical data between update. The app still store the stale data, but it can be ignored in the analysis by comparing the scan result's timestamp. Table A.1 shows the list of Wi-Fi parameters that the Wi-Fi handler collects.

Cellular handler collects 4G LTE and 5G NR data from the Telephony API [14]. On each data update, the Main Service pulls information of multiple LTE channels as described by Table A.2 and NR channels as described by Table A.3. Additionally, we found some NR-NSA-related parameters by casting the "ServiceState" object as a string. The values are described by Table A.4.

We observe a lot of limitations as follows, some of which depends on device model and Android version. Over the duration of our research works, we tested Android version 11, 12, and 13, installed in several phone models, namely, Google Pixel 5, Google Pixel 6, Google Pixel 6 Pro, Samsung Galaxy S21 Ultra, Samsung Galaxy S21+, and Samsung Galaxy S22+.

Limitations on CA designation: Each captured LTE and NR channels are expected to have CA designation that denotes whether the channel is the Primary, Secondary, or Neighboring. The results of API call to of the parameter is either Primary or Other, which does not differentiate between Secondary or Neighboring channels.

Bandwidth limitation: On all versions and models of Android phones that we tested, we observed a valid bandwidth value only for primary LTE channels (cross-checked with root-based apps). Additionally, NR-related API which was implemented in Android 12, does not include NR bandwidth.

NR-NSA limitation in Android 11: At the beginning of 5G deployment around 2019, operators started to deploy mmWave network. At the time, we tested this network using Pixel 5 phones with Android 11. We observe no 5G channels even when the Pixel 5 phone received a downlink speed of 1 Gbps and above, which is typical for a mmWave network. To fix this problem, we implemented a workaround by casting the Telephony API's "Signal-Strength" object [14] to read values related to NR signal strength. However, this method does not contain cell identity information (*e.g.*, PCI, frequency). But we assume that the network is mmWave since it is the only deployed 5G network at the time. Additionally, we kept cross-checking SigCap data with other root-based apps in our works. This problem is resolved when Android 12 is released, but we kept the workaround for compatibility with older devices.

Invalid values: There are parameters that always shows an invalid value even at the latest Android version. We keep collecting this invalid parameters since it may be fixed in the future and will be a good addition to our analysis. These parameters are: LTE CQI, NR CSI-RSRP, NR CSI-RSRP, and NR CSI-SINR.

GPS handler collects GPS location data as shown by Table A.5 from the Location API [27]. The API defines horizontal and vertical accuracy parameters as the estimated accuracy in meters, *i.e.*, there is a 68% probability that the latitude, longitude, and altitude are accurate within the accuracy radius. However, we observe that the GPS latitude and longitude values are already accurate enough for our current work, thus we omit the values in our analysis. In the future, it can be included to increase the precision of our analysis, or it can be utilized a novel way, *e.g.*, as a parameter to predict indoor-outdoor label from a SigCap datapoint.

Sensor handler uses the "device manager" privilege to obtain information from the hardware sensor API [13]. While the "device manager" privilege need to be turned on for the data collection, it is available for all Android device and easier to enable compared to root privilege. Table A.6 shows the list of sensor data collected by SigCap, there are four types of temperature sensors (*i.e.*, CPU, GPU, skin, and battery) with three types of values (*i.e.*, temperature, throttling temperature, shutdown temperature), totalling to 12 parameters. In our observation, "throttling temperature" indicates a threshold value where the device goes to throttling mode (*i.e.*, limiting processing power and cellular capabilities) if the respective temperature value is breached. Similarly, "shutdown temperature" indicates a threshold value where the device will be turned off.

Parameter	**API Call / Derived**	**Explanation**
BSSID	API Call	String denoting AP BSSID, encoded using SHA-256 for privacy.
Primary Frequency	API Call	Center frequency of primary channel in MHz.
Center Frequency	API Call	Center frequency of the whole channel in MHz.
2nd Center Frequency	API Call	Center frequency of a second set of channel in MHz, if using a discontinuous channel pair (*i.e.*, 80+80 MHz).
Bandwidth	API Call	Channel bandwidth in MHz.
Channel Number	Derived	Channel number as specified by the 802.11 specifications, derived from center frequency and bandwidth.
Primary Channel Number	Derived	Primary channel number as specified, derived from primary frequency and bandwidth.
RSSI	API Call	Received Signal Strength Indicator in dBm.
Capabilities	API Call	Describes the authentication, key management, and encryption schemes supported by the AP.
Standard	Derived	Describes which 802.11 amendments that the AP supported (*i.e.*, a/b/g/n/ac/ax). For Android 12 and above, this value can be directly collected from API. If the API call is unavailable, it is determined from the Capabilities, Channel Number, and Bandwidth.
Connected	API Call	Whether the AP is connected to the device.
Link Speed	API Call	Connected AP's link speed.
TX Link Speed	API Call	Connected AP's transmit link speed.
RX Link Speed	API Call	Connected AP's receive link speed.
Max Supported TX Link Speed	API Call	Connected AP's maximum supported transmit link speed.
Max Supported RX Link Speed	API Call	Connected AP's maximum supported receive link speed.

Table A.1: Wi-Fi parameters.

Parameter	**API Call / Derived**	**Explanation**
PCI	API Call	Physical Cell ID as described by the specification.
CI	API Call	Cell Identity as described by the specification.
EARFCN	API Call	E-UTRA (LTE Spectrum) Absolute Frequency Channel Number which describes the center frequency of the downlink channel.
Band	Derived	LTE Band number derived from EARFCN.
Bandwidth	API Call	Channel bandwidth in kHz. In our observation, only primary channel shows a valid bandwidth value.
Frequency	Derived	Center frequency of the channel in MHz, derived from EARFCN.
Wi-Fi-equivalent Channel Number	Derived	Only applies for LAA channels (band 46), derived from EARFCN and assuming 20 MHz bandwidth.
Signal Strength	API Call	Signal strength in dBm. In our observation, this value is always the same as the RSRP.
RSRP	API Call	Average power of multiple LTE Reference Signals (in dBm) received in the channel.
RSRQ	API Call	Quality indicator derived from RSRP (in dB), as described by the specification.
RSSI	API Call	Received Signals Strength Indicator over the the channel in dBm.
RSSNR	API Call	Signal-to-noise ratio of the Reference Signal in dB.
CQI	API Call	Channel Quality Indicator as described by the specification. In our observation, this value is always invalid.
Timing Advance	API Call	Timing Advance value as described by the specification.
Registered	API Call	Whether the channel is registered as the primary channel.
Cell Status	Derived	Describes whether the LTE channel is primary, secondary, or unknown. This value is taken from API call. In the case that the API is unavailable, we try to derive whether the channel is a primary based on the observation of valid bandwidth and "registered" values.

Table A.2: LTE parameters.

Parameter	API Call / Derived	Explanation
PCI	API Call	Physical Cell ID as described by the specification.
NCI	API Call	NR Cell Identity as described by the specification.
NRARFCN	API Call	NR spectrum Absolute Frequency Channel Number which describes the center frequency of the downlink channel.
Band	Derived	NR Band number derived from NRARFCN.
Frequency	Derived	Center frequency of the channel in MHz, derived from EARFCN.
SS-RSRP	API Call	Average power (in dBm) of multiple Reference Signals inside the Synchronization Signal (SS) block.
SS-RSRQ	API Call	Quality indicator (in dB) derived from SS-RSRP, as described by the specification.
SS-SINR	API Call	Signal-to-interference-and-noise ratio (in dB) over the the SS block.
CSI-RSRP	API Call	Average power (in dBm) of multiple Reference Signals inside the Channel State Indicator (CSI) block.
CSI-RSRQ	API Call	Quality indicator (in dB) derived from CSI-RSRP, as described by the specification.
CSI-SINR	API Call	Signal-to-interference-and-noise ratio (in dB) over the the CSI block.
IsSignalStrAPI	Derived	Describes whether the NR channel information is taken from the Signal Strength API.
Cell Status	API Call	Describes whether the NR channel is primary, secondary, or unknown.

Table A.3: NR parameters.

Parameter	API Call / Derived	Explanation
NR Status	API Call	NR connection status (*i.e.*, Connected, Not Restricted, Restricted, None).
NR Available	API Call	Whether NR connection is available.
DC-NR Restricted	API Call	Whether Dual Connectivity between LTE and NR is restricted.
EN-DC Available	API Call	Whether Dual Connectivity between LTE and NR is available.
NR Frequency Range	API Call	Describes the frequency range of the primary NR channel (*i.e.*, low, mid, high/mmWave band).

Table A.4: Additional NR-NSA parameters.

Parameter	API Call / Derived	Explanation
Latitude	API Call	GPS Latitude.
Longitude	API Call	GPS Longitude.
Altitude	API Call	Altitude in meters.
Horizontal Accuracy	API Call	Estimated horizontal accuracy radius in meters of this location at the 68th percentile confidence level.
Vertical Accuracy	API Call	Estimated altitude accuracy radius in meters of this location at the 68th percentile confidence level.

Table A.5: GPS parameters.

Parameter	API Call / Derived	Explanation
CPU Temperature	API Call	Temperature of one or multiple CPU cores in Celsius.
GPU Temperature	API Call	Temperature of one or multiple GPU cores in Celsius.
Skin Temperature	API Call	Temperature of one or more phone skin sensors in Celsius.
Battery Temperature	API Call	Temperature of one or more battery sensors in Celsius.
CPU Throttling Temperature	API Call	Throttling threshold for CPU temperatures.
GPU Throttling Temperature	API Call	Throttling threshold for GPU temperatures.
Skin Throttling Temperature	API Call	Throttling threshold for skin temperatures.
Battery Throttling Temperature	API Call	Throttling threshold for battery temperatures.
CPU Shutdown Temperature	API Call	Shutdown threshold for CPU temperatures.
GPU Shutdown Temperature	API Call	Shutdown threshold for GPU temperatures.
Skin Shutdown Temperature	API Call	Shutdown threshold for skin temperatures.
Battery Shutdown Temperature	API Call	Shutdown threshold for battery temperatures.

Table A.6: Sensor parameters.