IUT de Lannion
Networking & Telecoms Dept.

Dalhousie University
Faculty of Computer Science

Internship report

Undergraduate research assistant

29th April – 15th July 2024

Intern	Supervisors
Morgan MOOTOOSAMY 2nd Year BUT Network engineering & Telecoms IUT de Lannion	**Nur ZINCIR-HEYWOOD** Distinguished Research Professor & Associate Dean Research Faculty of Computer Science **Samer LAHOUD** Associate Professor Faculty of Computer Science **Stéphanie LE MELEDER** Language coordinator & English teacher IUT de Lannion

Internship report
Undergraduate research assistant

29th April – 15th July 2024

Intern	Supervisors
Morgan MOOTOOSAMY 2nd Year BUT Network engineering & Telecoms IUT de Lannion	**Nur ZINCIR-HEYWOOD** Distinguished Research Professor & Associate Dean Research Faculty of Computer Science **Samer LAHOUD** Associate Professor Faculty of Computer Science **Stéphanie LE MELEDER** Language coordinator & English teacher IUT de Lannion

Acknowledgement

I sincerely appreciate Dalhousie University from welcoming me and offering me an outstanding opportunity to work in Halifax.

I am grateful to Nur ZINCIR-HEYWOOD receiving me in NIMS Lab and promoting my project.

I want to express my deepest appreciation to Samer LAHOUD for his guidance and his feedback through my internship but also for giving me an interesting subject that corelates with my professional career and my studies.

Many thanks to NIMS Lab's team for their kindness and for my integration in the laboratory and in Halifax.

Special thanks to Stéphanie LE MELEDER for her support in my internship.

I would like to thank Cécilia LEFEBVRE, Lannion's IUT and Dalhousie University's administration for their great help and their guidance.

Table of contents

Introduction

Today, many people use the Internet to entertain themselves, to search for information, to work, to use social media and to communicate. Since the end of the 20th century, wired connections are widely used to have access to the Internet. As the years passed, in the early 2000s, new innovative technologies emerged to expand the coverage of the Internet through wireless technologies such as cellular networks like 5G, Bluetooth and WiFi. With the use of access points, urban spaces (homes, roads, parks…) especially are covered with wireless networks in high data rates.

However, with the increasing number of users, restrictions are made to limit the use of wireless communications overseen by CRTC in Canada. Furthermore, wireless technologies face new security challenges to protect users and providers from attacks.

Currently an undergraduate student in my 2nd year of BUT Network engineering and Telecoms in a cybersecurity course (equivalent to a bachelor degree) in Lannion's IUT in France, I have to complete my year with an internship. So, I have done it in Canada, in Halifax at Dalhousie University in the Faculty of Computer Science as an undergraduate research assistant in NIMS Lab supervised by Dr. Samer Lahoud and Dr. Nur Zincir-Heywood.

In this report, I will present to you first Halifax, Dalhousie University and my role in the laboratory. Then I will present my project, the organisation along with the different stages. Finally, I will conclude and review my internship. Detailed information is presented in the annex at the end of the document.

1 – Presentation of the context

I will start by presenting Dalhousie University and the Faculty of Computer Science, then the city of Halifax and finally my role and missions in NIMS Laboratory during my internship.

1.1. Halifax, Nova Scotia, Canada

Halifax is located in the province of Nova Scotia, on the east coast of Canada. With an urban area of 238.29 km², Halifax has more than 400,000 inhabitants and is the most popular municipality in Atlantic Canada. The city holds a variety of key infrastructures with its port, shipyard, naval military base and outposts, government offices, private companies and universities.

Nova Scotia is historically known to be the first province where the first transatlantic radio message was transmitted in 1902 from Guglielmo Macaroni, an Italian inventor and electrical engineer. The system was further developed in the early 20th century for communication between stations and ships at sea. Mostly notably, the role of Macaroni Co. in the sinking of the Titanic raised awareness of the importance of radio communications in the world.

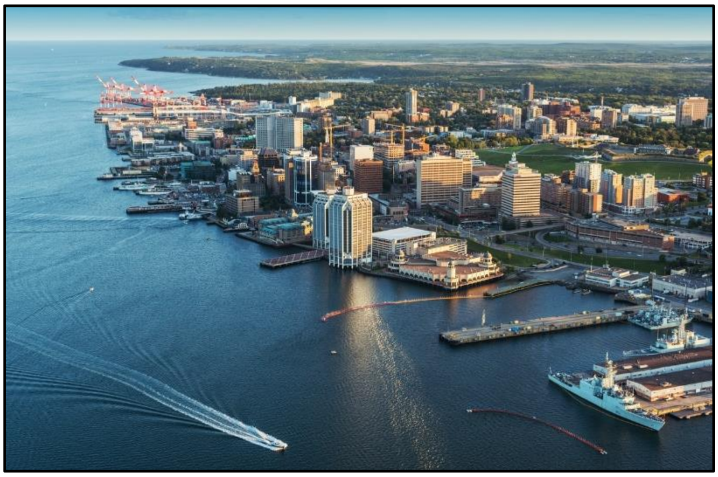


Figure 1. Halifax, Nova Scotia, Canada

Figure 2. Guglielmo Macaroni

1.2. Dalhousie University

Dalhousie University was founded in 1818 by George Ramsay. It highly focuses on research and attracts over 21,000 students across the country as well as the world with $214 million in research funding each year. Dalhousie University is one of the top leading research-intensive universities of Canada with 13 academic Faculties.

Figure 3. Dalhousie University sign

1.3. Faculty of Computer Science

Founded in 1997, the Faculty of Computer Science of Dalhousie University is the top research institution in Information Technology in Atlantic Canada. It specialises on deep technical, problem solving and leadership skills on computing technologies.

The Faculty of Computer Science (FCS) holds multiple research playgrounds with different specialisations mainly focused on Big Data Analytics, DeepSense and innovation.

Figure 4. Goldberg FCS building

1.4. NIMS Laboratory

Network Information Management and Security (NIMS) Laboratory is supervised by Dr. Malcom Heywood and Dr. Nur Zincir-Heywood. The laboratory is composed of undergraduate, graduate, PhD students and professors from many countries such as France, Ghana, Iran, Turkey and China. NIMS Lab is cosmopolitan and diverse focused on different academic research projects in Internet of Things (IoT), instant messaging applications, cybersecurity, artificial intelligence and other wireless technologies.

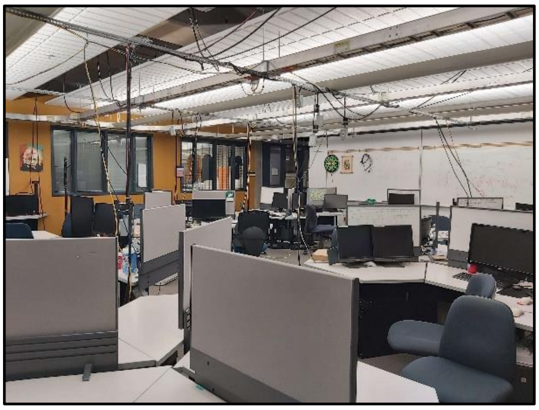


Figure 5. NIMS Playground

1.5. My role, undergraduate research assistant

An undergraduate research assistant helps professors and PhD students by working on their academic research projects. It consists of running experiments, gathering data and results and conducting surveys and reporting it directly to the professors and the PhD students.

Initially, my internship's goal was to conduct a survey about jamming and anti-jamming techniques on WiFi 6 supported devices and access points. But actually, my main objective was to create a WiFi coverage heatmap of Halifax.

I had multiple stages and missions in my internship which consisted of studying the WiFi technology and analysing data from the WiFi coverage heatmap in which I will explain further in this report.

2 – Creation of a WiFi coverage heatmap

My project consisted of creating a WiFi coverage heatmap of Halifax, with the use of multiple devices, software and knowledge on my disposal. I will first explain to you what is WiFi, the regulations that should be respected, the devices that were used and finally the heatmap analysis.

2.1. WiFi technology

Before conducting any experiments, it is important to understand the main topic of the project which is WiFi. WiFi is a wireless local area network that uses radio frequency signals to transmit and receive data in a certain distance.

2.1.1 Physical layer

Common techniques are used so that devices and access points know how to interpret on which frequency the signals should be transmitted and received.

WiFi uses different modulation techniques to share connection between devices and access points. In common wireless networks, OFDM (Orthogonal Frequency-division multiplexing) is used, which divides the bandwidth/channel into equally spaced subcarriers for each station to use. A bandwidth is like a network of tunnels spaced equally and a subcarrier is like one tunnel that can be used to transmit data.

Today most commonly in WiFi version 4, 5 and 6, two main frequencies are used to exchange data: at 2.4 GHz and 5 GHz.

The channel can vary, most commonly it can be 20MHz wide but could also be 40, 80 to 160 MHz wide, the channel is then divided to subcarriers that are 318,5 kHz or 78,125 kHz wide.

There is up to 14 channels depending of the country. Most commonly, channel 1, 6 and 11 are used to avoid overlapping and interference which degrades performance when there are data transmissions. This is why there is spacing and specific widths for subcarriers and channels.

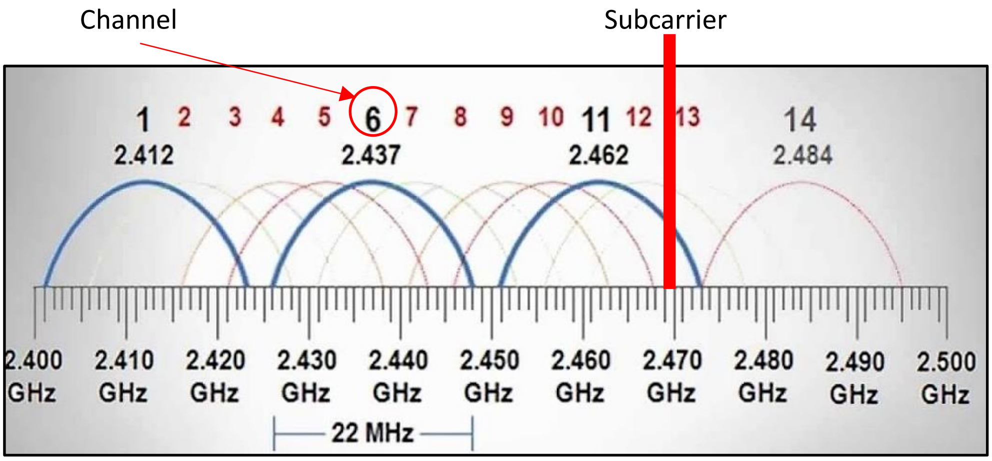


Figure 6. 2.4GHz WiFi Channels

2.1.2. MAC layer

So that stations and access points (AP) communicate with the lowest amount of interference and errors, protocols are defined through messages that are transmitted using the appropriate frequencies.

Connection

To establish a connection, first the access points need to notify the stations (clients) of their presence nearby.

To do this access points scan passively, they broadcast beacons with information such as their Service Set Identifier (SSID) that represents the name of the network. Once a station receives the beacons, it can identify the nearby access points.

The other scanning method is active, basically the station directly sends a probe request in its radius, access points will respond with probe responses that contain information like SSID and capabilities.

Both scanning methods can be used, they both follow the same procedures to establish a connection.

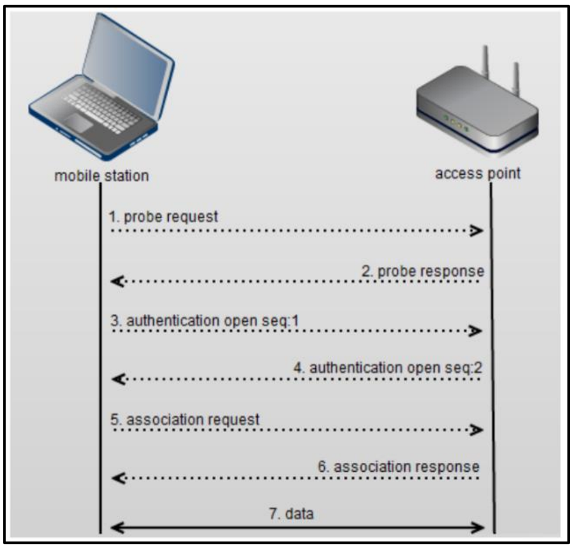


Figure 7. WiFi Connection phases with active scanning

After different authentication methods can be used to create a secure connection between the station and the access point depending of the type of encryption like WEP, WPA, WPA2 and WPA3.

Roaming

The station sends a disassociation frame, which announces a disconnection from the access point 1 and sends a Reassociation frame to connect to the other access point 2 and authenticates. Factors like the signal strength can be a reason to roam and change access point.

Disconnection

To disconnect either the station or the access point sends a disassociation frame. The access point could either send in broadcast or to a station in particular with MAC address that identifies the station.

2.1.3. Protection methods

WEP (Wired Equivalent Privacy): Provides authentication and encryption protection however it is out of date, and can be easily cracked by malicious entities. It is recommended not to use WEP encryption.

PROS	CONS
- Easy Setup: WEP is supported by almost all WiFi devices, especially older ones, and is relatively easy to set up. - Legacy Support: Some very old devices that don't support newer protocols can still use WEP, making it useful in specific legacy situations.	- Weak security: WEP is extremely vulnerable to attacks. - Not recommended for standard use.

WPA/WPA2 (Wireless Protected Access): In addition to what WEP can provide, WPA/WPA2 can verify integrity of messages and provides a series of keys to encrypt and decrypt data. There are still vulnerabilities but less than WEP encryption.

PROS	CONS
- Improved Security: WPA was introduced as an improvement over WEP, addressing some of its vulnerabilities by using TKIP (Temporal Key Integrity Protocol) to dynamically change keys. As for WPA2, AES (Advanced Encryption Standard) is used which is a stronger encryption method. - Compatibility: WPA can work with older hardware that supports WEP, making it an easier transition from WEP. Many devices also support WPA and WPA2 encryption standards.	- More secure than WEP, WPA and WPA2 are still vulnerable to certain attacks.

WPA3: Offers high protection with automatic encryption and prevents unauthorised access from unauthenticated or not associated devices. A new protection method that is recommended to use today however not many devices supports WPA3 encryption.

PROS	**CONS**
- Enhanced Security: WPA3 introduces stronger encryption standards, including SAE (Simultaneous Authentication of Equals), which replaces WPA2's PSK and protects against dictionary attacks. - Forward Secrecy: WPA3 provides forward secrecy, ensuring that even if the current encryption key is compromised, previously captured data cannot be decrypted. - Better Protection for Open Networks: WPA3 includes a feature called OWE (Opportunistic Wireless Encryption), which encrypts data even on open networks without requiring a password. - Resilience to Brute-Force Attacks: WPA3 includes protections that make it more resistant to brute-force attacks.	- Compatibility Issues: WPA3 is not supported by all devices, especially older hardware, requiring newer devices or firmware upgrades.

2.2. Regulations

When conducting experiments on wireless networks, it is important to conduct them in the safest ways possible and respect the regulations and laws.

2.2.1. Personal information

Personal information identifies an individual, it can be their ID, age, name, medical records, opinions, beliefs, social status, employee files, credit records, acquired goods and services etc.

2.2.2. Personal Information Protection and Electronic Documents Act

In Canada, scanning Wi-Fi networks without explicit permission could be seen as a violation of privacy laws or unauthorized access. If the scanning is part of cybersecurity practices on networks you own or manage, it's generally acceptable. However, if it is done on someone else's network without consent, it could be considered illegal and a violation of the Personal Information Protection and Electronic Documents Act (PIPEDA)**.**

Since April 2000, private-sector organisations and federally-regulated businesses are to follow PIPEDA when collecting data, using data and disclosing personal information regarding their profit and commercial activities in Canada.

This also applies to all businesses that operate in Canada regardless of the territory they are based in, so it also applies to foreign organisations.

There are 10 key principles to protect personal information:

1) **Accountability**: Organisations must designate one or more individuals to be accountable for the organization’s compliance with privacy laws and standards.

2) **Identifying purposes**: Organisations must clearly identify and document the purposes for which personal information is collected at or before the time of collection.

3) **Consent**: Individuals must give informed consent before their personal information is collected, used, or disclosed.

4) **Openness**: Organisations must make their policies and practices related to the management of personal information and should be informed to individuals.

5) **Limiting collection**: The collection of personal information must be limited to what is necessary for the purposes identified by the organisation.

6) **Limiting use, disclosure, and retention**: Personal information should only be used or disclosed for the purposes for which it was collected unless the individual consents otherwise, or as required by law.

7) **Accuracy**: Personal information must be as accurate, complete, and up-to-date as necessary for the purposes for which it is to be used.

8) **Individual access**: Individuals have the right to access their personal information.

9) **Safeguards**: Organisations are to protect personal information with the proper security against risks like modification, copying and unauthorised access.

10) **Challenging compliance**: Organisations must have procedures in place to receive and respond to complaints or inquiries about their handling of personal information.

2.2.3. Canadian Radio-television and Telecommunications Commission

Formed in 1968, the Canadian Radio-television and Telecommunications Commission (CRTC) is an administrative tribunal under the federal government that implements the laws and regulations set by the Parliament that creates policies and laws. The CRTC also supervises broadcasts and telecommunications in Canada which represents over 2,000 broadcasters, companies and radio stations. They are engaged to enhance the safety of Canadians by enforcing regulations and laws.

2.3. Devices

There are multiple ways to collect data to create heatmaps with satellites, phones, antennas or smaller devices. So, to be able to collect and study data it is important to use the appropriate devices and software to first locate and to scan the neighbouring wireless networks.

2.3.1. Hardware

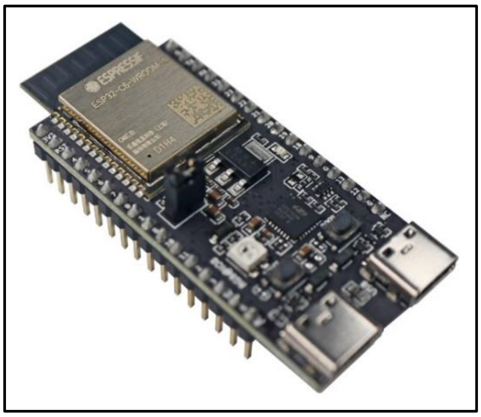


Figure 8. ESP32-C6-DevKitC-1

ESP32-C6-DevKitC-1 is a ESP32 development board with complete WiFi, Bluetooth, Zigbee and Thread functions. Initially, I used this board to learn basics with Arduino software to scan neighbouring networks but it does not have a GPS module in order to locate the scans. The device costs roughly $9.

Figure 9. LILYGO Model T-Beam v1.1

LILYGO Model T-Beam V1.1 is a ESP32 LoRa development board with a GPS module for real-time positioning and tracking and LoRa transceiver for long-range communication with a built-in WiFi and Bluetooth functionality. The board is compatible with Arduino IDE to develop and program applications on the board using an extensive library. For me, the GPS module as well as the WiFi functionality are used to scan the surrounding networks and to pinpoint the location of the scan. The scan is then sent directly in a text format to the connected device like a phone or a computer. The device costs roughly $41.

2.3.2 Software

Figure 10. Arduino IDE

To configure and develop the boards, I used Arduino IDE (Integrated Development Environment) which supports the languages C and C++. It supplies a library with many different common input and output procedures. With two basic functions, the code can be interpreted to scan WiFi networks for example in a loop and to locate where the board is using GPS coordinates provided by satellites.

Figure 11. Spyder

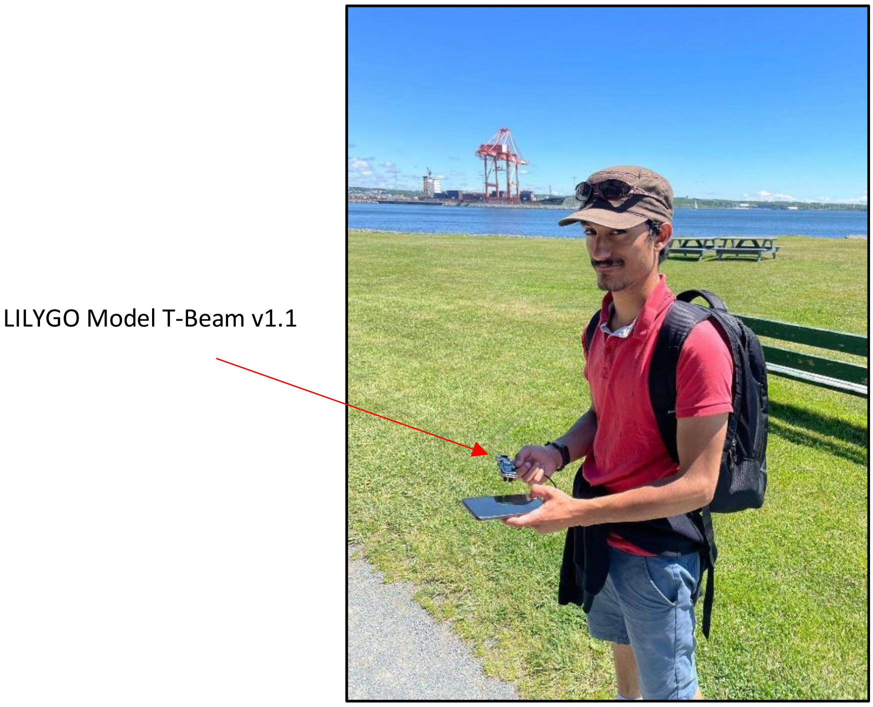
To analyse the data received from the board in a plain text format, I used Spyder which is an IDE written in Python language. The IDE provides also many libraries to use for data exploration and analysis. I used Spyder primarily to create the heatmap, the GUI (Graphical User Interface) and statistics.

Figure 12. DB Browser for SQLite

In order to manage data, I require to store them in a database with DB Browser for SQLite. It is an open-source tool designed to create, search and edit SQLite database files and so importing formatted data into the designed database helps to create plots, graphs, sort data and filter them with ease using SQL language.

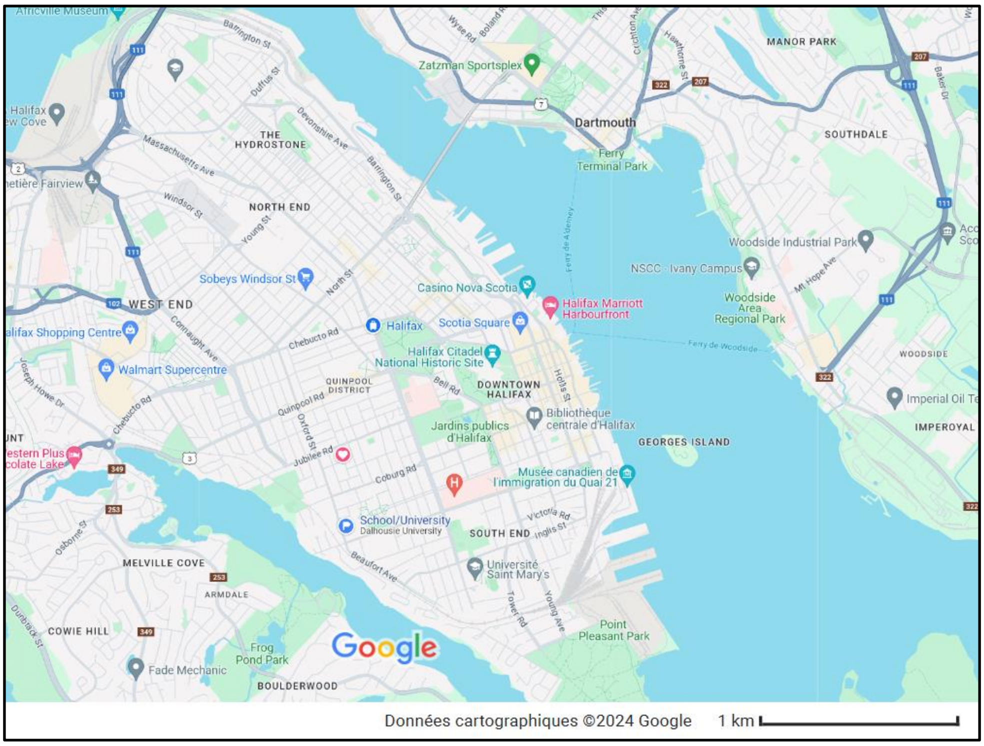
2.4. Heatmap analysis

To log my network scans, I connected the LILYGO Model T-Beam v1.1 to my smartphone to also navigate in areas that were not previously visited. This requires to walk across the city which represented a distance of at least 150km to obtain scans in the main areas of the city.



LILYGO Model T-Beam v1.1

Figure 13. Scanning networks with LILYGO device and smartphone, in Halifax



Données cartographiques ©2024 Google 1 km

Figure 14. Map of Halifax

2.4.1 Heatmap

In many different fields, heatmaps are used as 2D data representations on a map, commonly used to display magnitude, temperature, population density or the weather for example. With the use of different colour schemes to illustrate, the heatmap accurately shows the data depending of certain parameters like the intensity or the degree that often ranges from cold colours like blue to hot colours like red. It can reveal different patterns and anomalies that are easier to picture and to analyse on a surface.

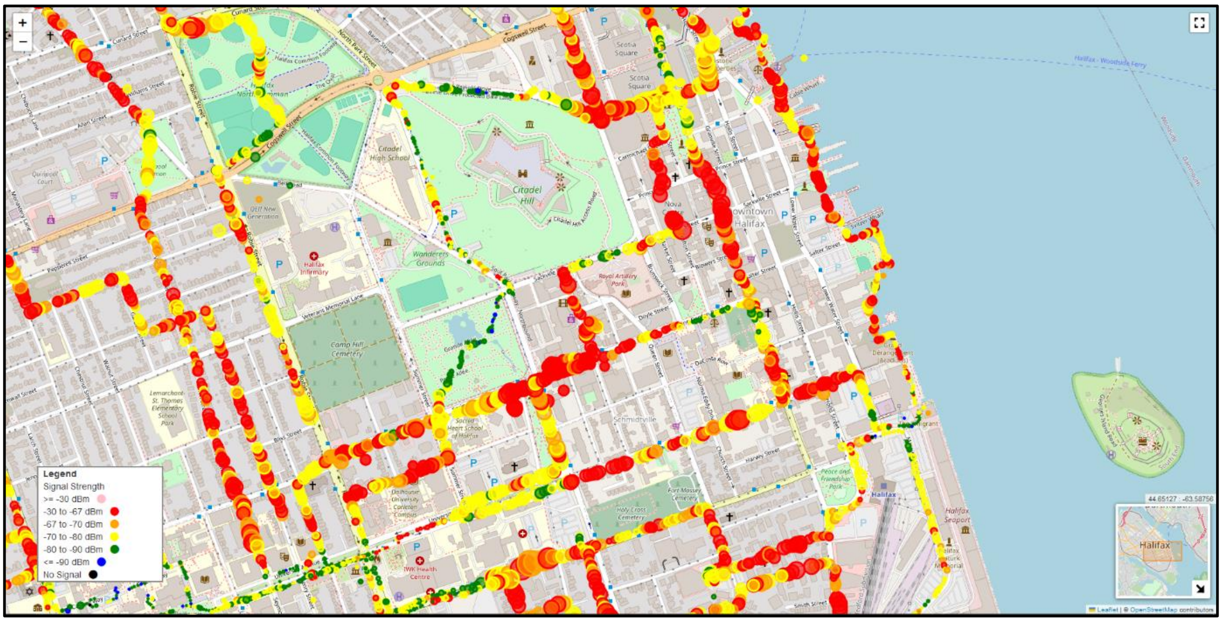
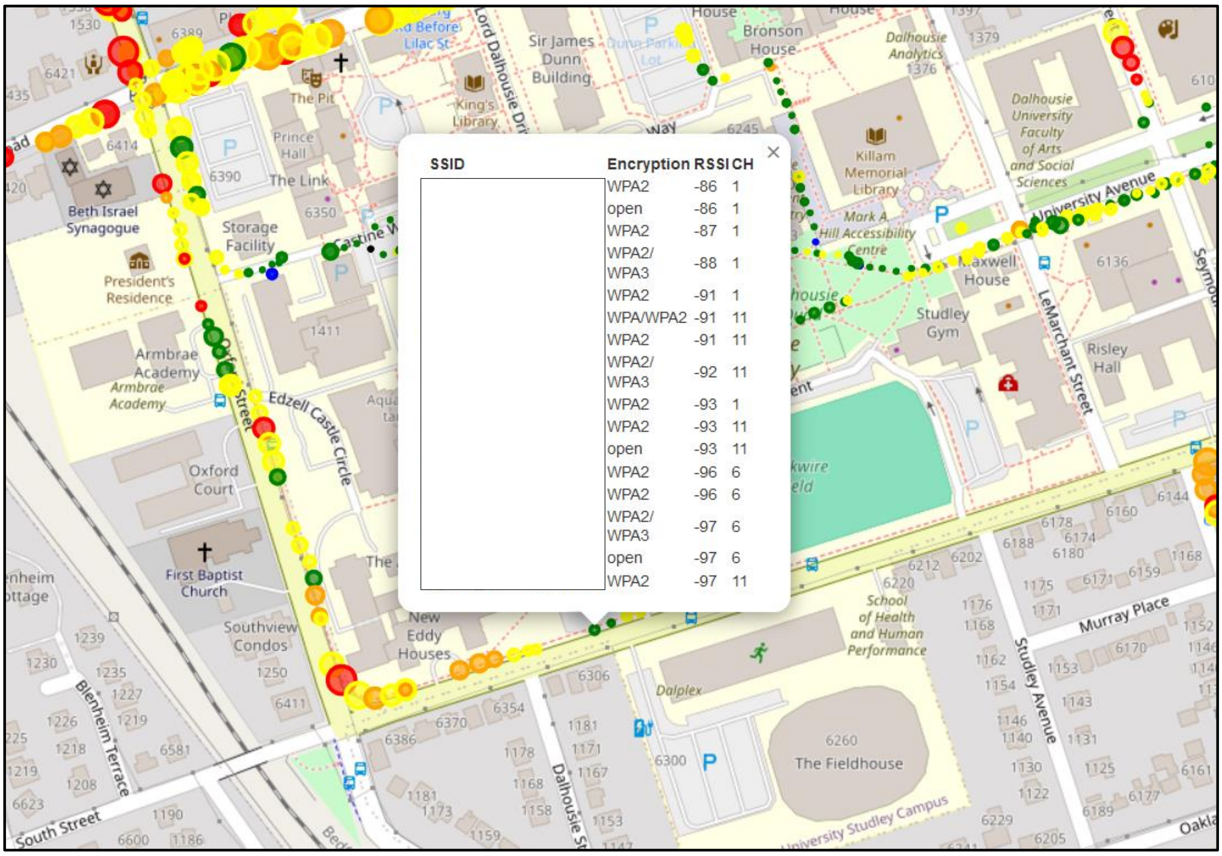


Figure 15. South of Citadel Hill, central Halifax

On this map we can see the different colour variations which represents the strongest WiFi strength ever scanned in the area. It varies between red colours, representing strong signal strengths to black colours that represent areas where no WiFi signals were found. The circle radius also is affected to the number of signals that were scanned in the area. The bigger the radius, the more WiFi signals were scanned.

Signal strength (RSSI) is measured using dBm units. On the heatmap, it represents the power of the received signal. The signals are from the probes that are sent from the access points. In Canada, access points can emit signals with a power output of maximum 1W (30dBm) and in France, the maximum power output is 100mW (20dBm) indoors and outdoors.

When selecting a network scan point, information can display like the SSID, the encryption type, the RSSI and channel the access points use. This information can later be relevant to locate certain networks depending of certain attributes which is why I decided to use a GUI in order to display specified information.



SSID	Encryption	RSSI	CH
	WPA2	-86	1
	open	-86	1
	WPA2	-87	1
	WPA2/ WPA3	-88	1
	WPA2	-91	1
	WPA/WPA2	-91	11
	WPA2	-91	11
	WPA2/ WPA3	-92	11
	WPA2	-93	1
	WPA2	-93	11
	open	-93	11
	WPA2	-96	6
	WPA2	-96	6
	WPA2/ WPA3	-97	6
	open	-97	6
	WPA2	-97	11

Figure 16. Example of a network scan point located in Halifax

2.4.2 Graphical User Interface (GUI)

A Graphical User Interface is a user interface that allows users to interact with a machine, it can simply be an application with graphical elements like icons on a smartphone, games, music and media players. GUI is used to simplify actions, instead of writing commands, interacting with a GUI can execute commands and functions with buttons, icons, menus etc. Using Python on Spyder, I made a GUI to filter the data on the heatmap.

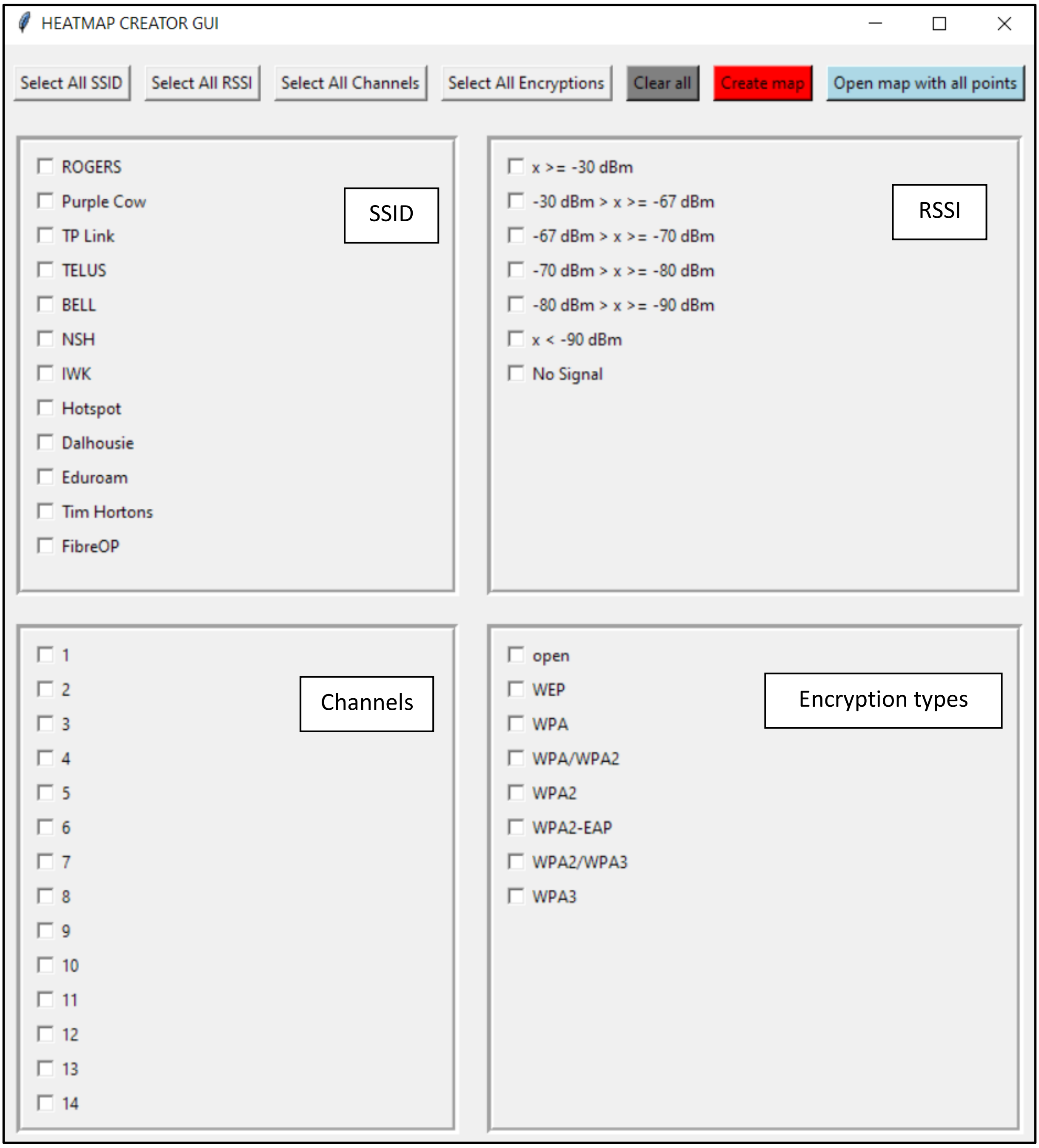


Figure 17. Heatmap GUI

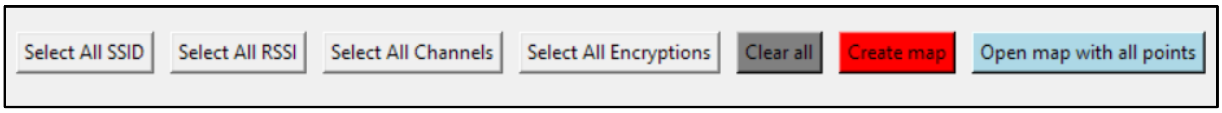


Figure 18. Buttons on the Heatmap GUI

<u>Select All SSID:</u> The button selects all the SSIDs that are presented to the user.

<u>Select All RSSI:</u> The button selects all the different received power measured.

<u>Select All Channels:</u> The button selects all the channels that are used for 2.4GHz WiFi networks.

<u>Select All Encryptions:</u> The button selects all types of encryptions that are used today.

<u>Clear all:</u> The button deselects all the selected parameters on the GUI.

<u>Create map:</u> The button creates the map with the selected parameters.

<u>Open map with all points:</u> The button displays the map with all the data collected.

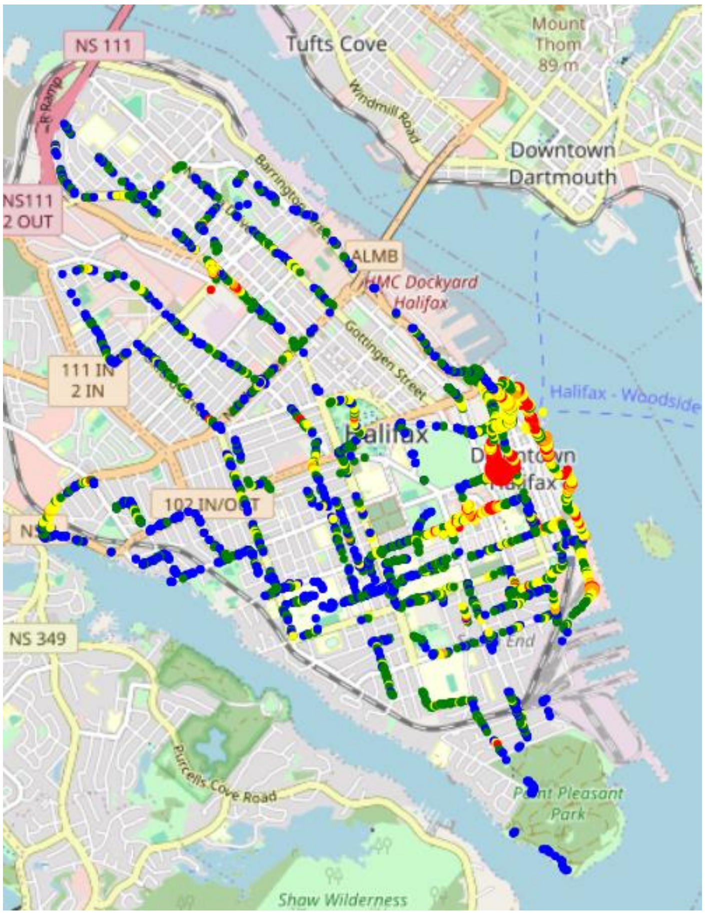


Figure 19. Heatmap of open networks in Halifax (when selecting "open" in encryption types)

2.4.3 Results

First, as explained previously, channels represent the different frequencies access points and stations share to transmit data.

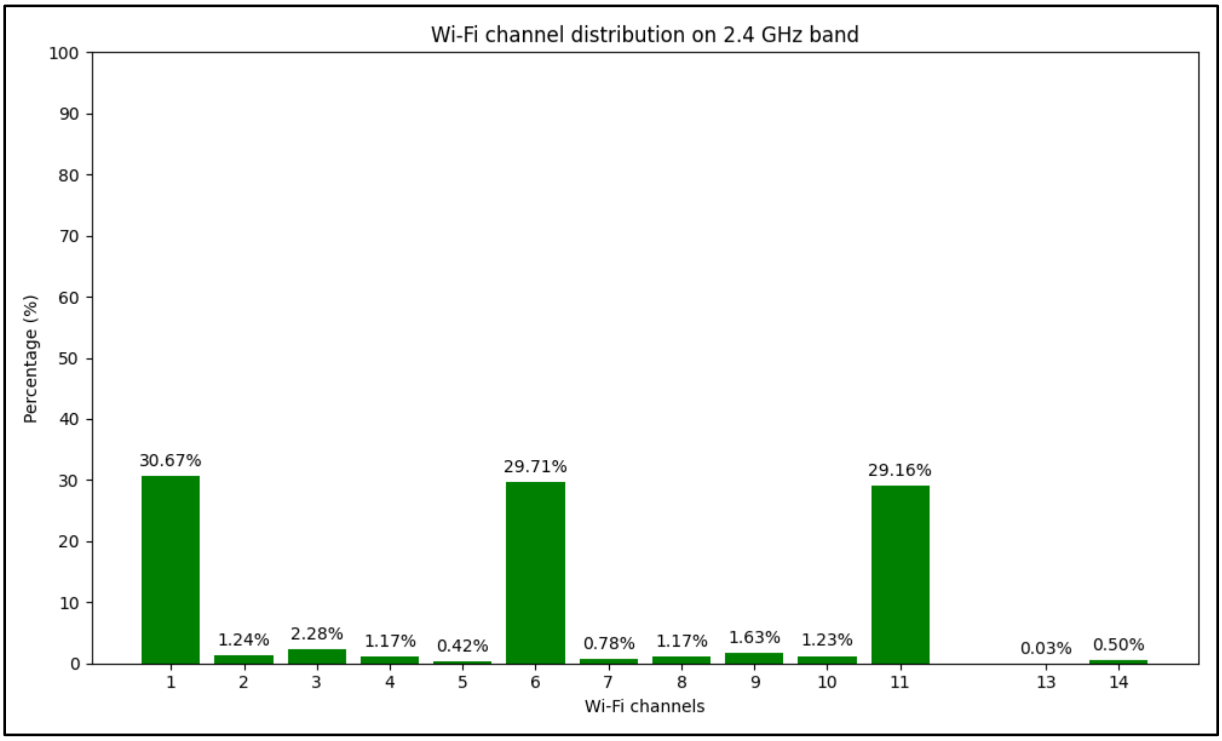


Figure 20. WiFi channel distribution on 2.4GHz band

The diagram shows that channels 1, 6 and 11 are mostly used with high percentages of 30.67%, 29.71% and 29.16%. These channels are commonly used to avoid overlapping to avoid interference between each other channels to optimise data transmissions as explained previously. There is a minimal use of channels in between, channels 2 to 5 and channels 7 to 10 compared to the main channels. Channels 12 to 14 are close to none because in Canada, North America specifically, 11 channels are mainly used.

The diagram highlights the importance of strategic channel selection in Wi-Fi networks to avoid interference and managing congestion. While channels 1, 6, and 11 are the preferred choices to avoid overlapping, their heavy usage indicates that network performance could still be compromised due to congestion. This is why 5GHz band is also used with less crowded channels for a dense environment like a city.

The diagram presents the distribution of WiFi encryption methods used in networks. The methods are crucial for securing wireless communications, protecting data from unauthorised access and to ensure network integrity.

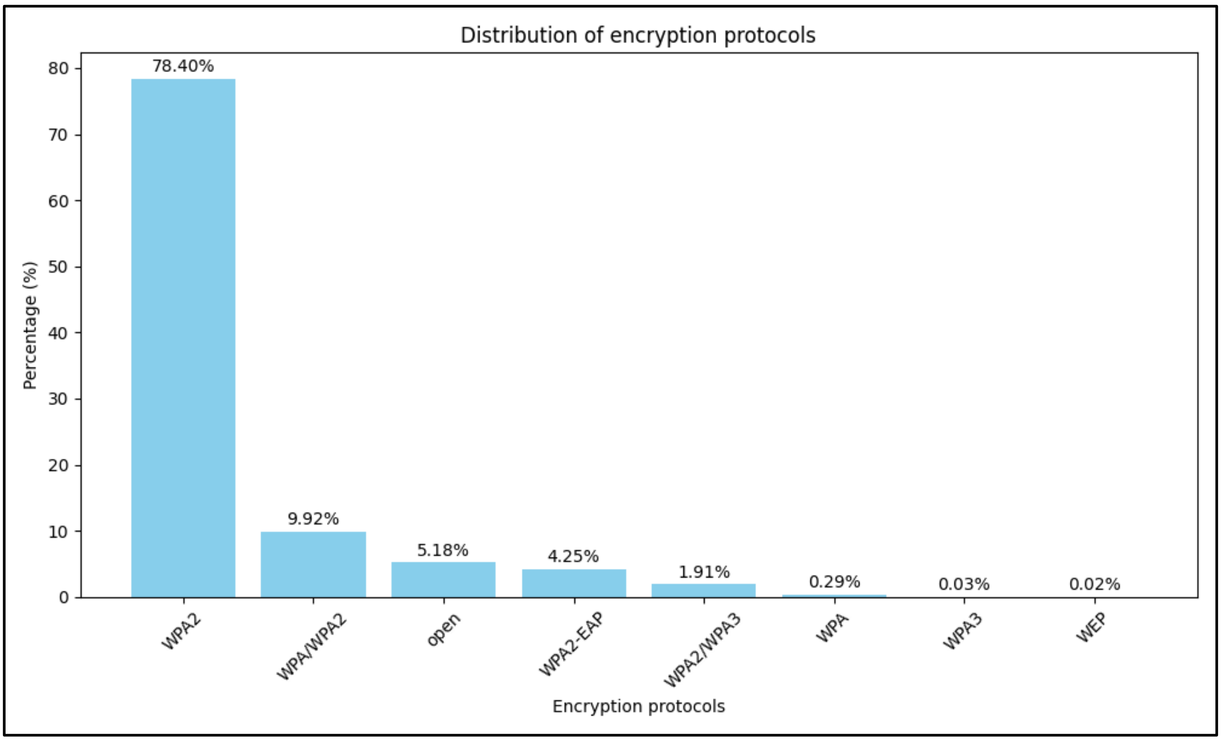


Figure 21. Distribution of encryption protocols

The diagram shows that WPA2 encryption dominates the other encryption methods with 78.40% for all the registered networks. This is expected because WPA2 has been a standard for many years, which is a robust encryption against most attacks.

Next is WPA/WPA2 mixed modes which represents 9.92% of the registered networks. This allows compatibility with devices supporting WPA or WPA2, it is less a standard because of the risks it may have because of WPA encryption especially.

Then there are open networks that represent 5.18% of the registered networks, these networks are not secured to use, they are mainly public networks with no passwords. As for WPA2-EAP, typically companies and private corporations use it to provide extra security compared to the standard WPA2 encryption. It offers an extra layer of protection with the use of RADIUS servers to authenticate the user.

Finally, the other encryption protocols represent a minority because of the security it offers which is obsolete regarding WPA and WEP encryption protocols but also the new standard WPA3 that is not supported by many devices.

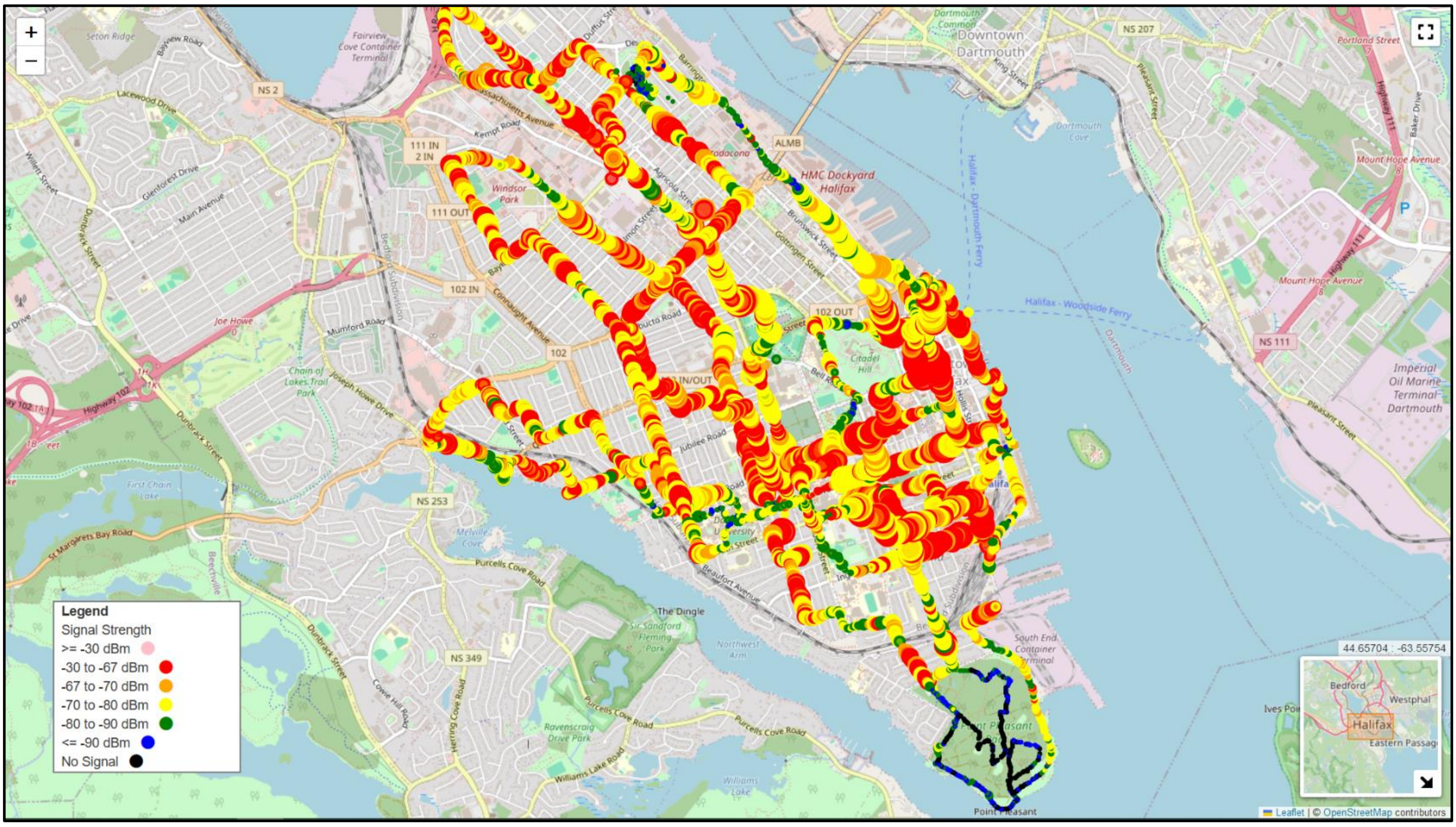


Figure 22. Heatmap of Halifax with all the data

On one hand, we can distinguish areas that are less dense represented in smaller circles such as parks, fields and near military bases. There are multiple factors that can explain the low density like physical obstacles like walls, trees and distance from access points which result in slower internet speeds, frequent disconnections or also the incapacity to connect to the network.

On the other hand, in highly dense areas represented in bigger circles in mainly in the centre of the city and also in inhabited places, the environment can also lead to interference, degraded performance and congestion.

There is also a correlation between signal strength (RSSI) and network density because in most cases, areas with strong RSSI represents areas with a high number of wireless networks which could lead to potential interference particularly for networks operating on overlapping channels.

However, areas with weaker signals indicate that fewer networks have been detected which can lead to less interference but a poor connectivity due to the lack of signal strength.

2.4.4. Solutions

To optimise wireless 2.4GHz network usage it is important to verify that the network is using the appropriate channels that do not overlap other channels such as channel 1,6 and 11 to minimise interference with other neighbouring networks. As for places with weak signal strengths, using signal boosters and amplifiers improve coverage. The placement of the access point and the users can also determine the connectivity, in areas that have physical barriers such as walls, gates and trees the signal can be obstructed. The use of 5GHz band can also be a solution to minimise interference between other neighbouring networks.

3 – Organisation of my project

In order to finish my project in my internship with the request of Prof. Samer Lahoud, I had to create a timetable. Depending of my pace and my tasks, we changed some stages that will be shown after the initial plan. The main steps I had to follow initially are shown below:

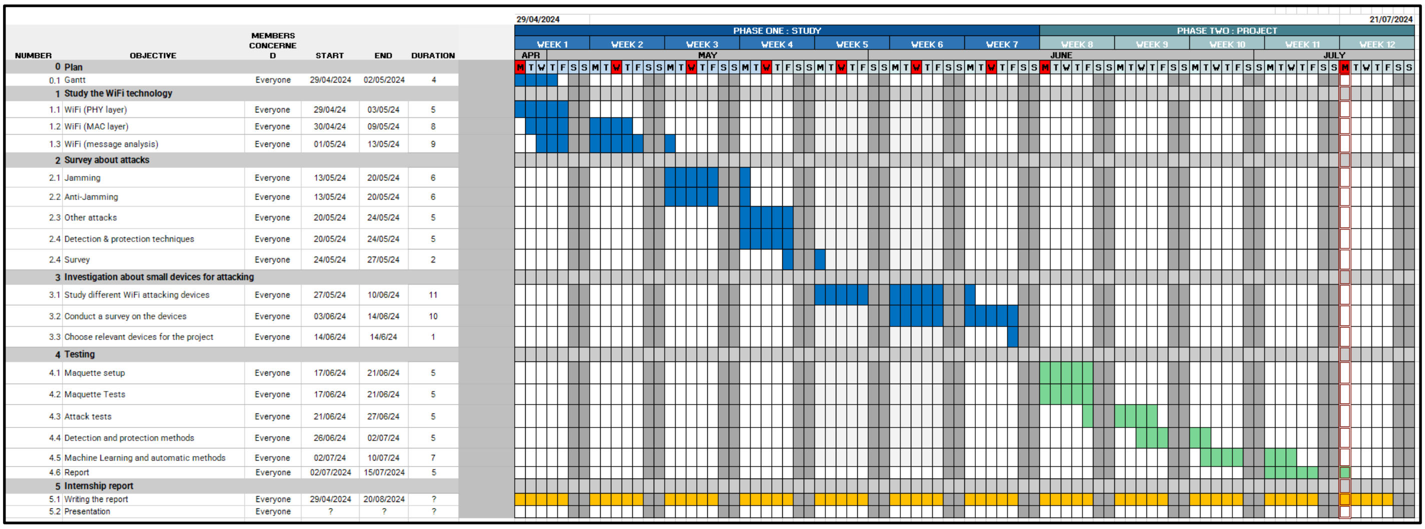
Step 1: Study the WiFi technology, including the physical and MAC layer aspects.

Step 2: Conduct a survey on attacks targeting local wireless access networks, with a specific focus on WiFi.

Step 3: Investigate the capabilities of small devices for jamming and conducting attacks on wireless networks, such as WiFi.

Step 4: Implement and test the functionality of these devices to detect and mitigate jamming attacks.

3.1. The planned timetable

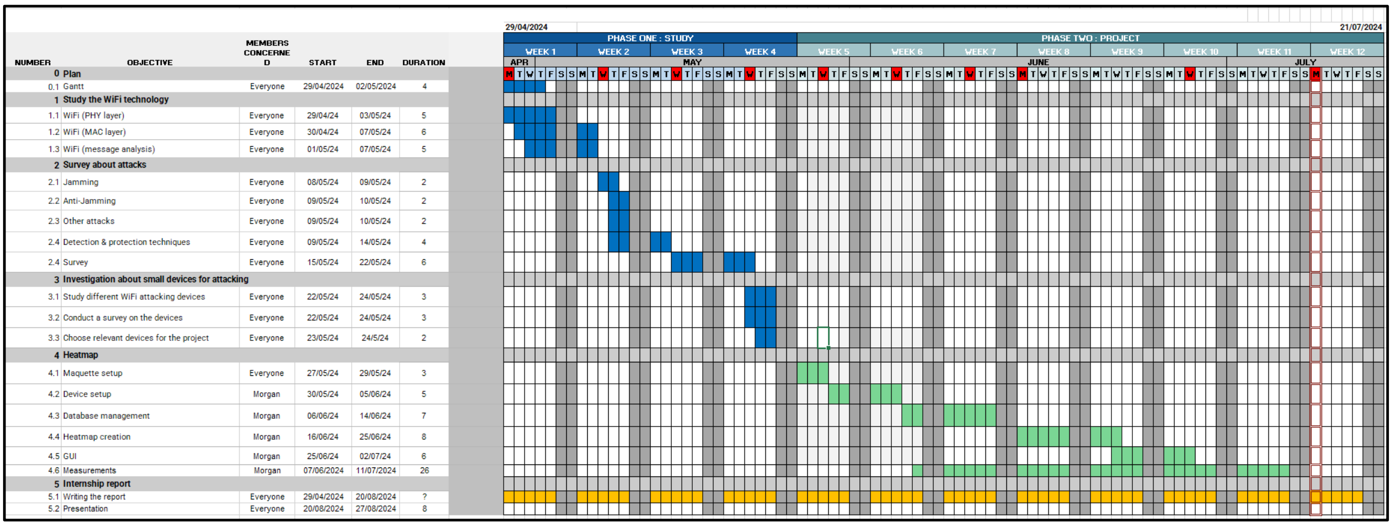


NUMBER	OBJECTIVE	MEMBERS CONCERNED	START	END	DURATION
0	**Plan**				
0.1	Gantt	Everyone	29/04/2024	02/05/2024	4
1	**Study the WiFi technology**				
1.1	WiFi (PHY layer)	Everyone	29/04/24	03/05/24	5
1.2	WiFi (MAC layer)	Everyone	30/04/24	09/05/24	8
1.3	WiFi (message analysis)	Everyone	01/05/24	13/05/24	9
2	**Survey about attacks**				
2.1	Jamming	Everyone	13/05/24	20/05/24	6
2.2	Anti-Jamming	Everyone	13/05/24	20/05/24	6
2.3	Other attacks	Everyone	20/05/24	24/05/24	5
2.4	Detection & protection techniques	Everyone	20/05/24	24/05/24	5
2.4	Survey	Everyone	24/05/24	27/05/24	2
3	**Investigation about small devices for attacking**				
3.1	Study different WiFi attacking devices	Everyone	27/05/24	10/06/24	11
3.2	Conduct a survey on the devices	Everyone	03/06/24	14/06/24	10
3.3	Choose relevant devices for the project	Everyone	14/06/24	14/6/24	1
4	**Testing**				
4.1	Maquette setup	Everyone	17/06/24	21/06/24	5
4.2	Maquette Tests	Everyone	17/06/24	21/06/24	5
4.3	Attack tests	Everyone	21/06/24	27/06/24	5
4.4	Detection and protection methods	Everyone	26/06/24	02/07/24	5
4.5	Machine Learning and automatic methods	Everyone	02/07/24	10/07/24	7
4.6	Report	Everyone	02/07/2024	15/07/2024	5
5	**Internship report**				
5.1	Writing the report	Everyone	29/04/2024	20/08/2024	?
5.2	Presentation	Everyone	?	?	?

Figure 23. Planned timetable

Me and Kenzo Froger, a student who was also in the same internship as me have decided to separate our tasks into multiple stages and substages. First part, representing the study of WiFi technology and the second part which consists of conducting our project. The days in red represent the weekly meetings that are scheduled with Prof. Lahoud.

3.2. Final timetable



NUMBER	OBJECTIVE	MEMBERS CONCERNED	START	END	DURATION
0	**Plan**				
0.1	Gantt	Everyone	29/04/2024	02/05/2024	4
1	**Study the WiFi technology**				
1.1	WiFi (PHY layer)	Everyone	29/04/24	03/05/24	5
1.2	WiFi (MAC layer)	Everyone	30/04/24	07/05/24	6
1.3	WiFi (message analysis)	Everyone	01/05/24	07/05/24	5
2	**Survey about attacks**				
2.1	Jamming	Everyone	08/05/24	09/05/24	2
2.2	Anti-Jamming	Everyone	09/05/24	10/05/24	2
2.3	Other attacks	Everyone	09/05/24	10/05/24	2
2.4	Detection & protection techniques	Everyone	09/05/24	14/05/24	4
2.4	Survey	Everyone	15/05/24	22/05/24	6
3	**Investigation about small devices for attacking**				
3.1	Study different WiFi attacking devices	Everyone	22/05/24	24/05/24	3
3.2	Conduct a survey on the devices	Everyone	22/05/24	24/05/24	3
3.3	Choose relevant devices for the project	Everyone	23/05/24	24/5/24	2
4	**Heatmap**				
4.1	Maquette setup	Everyone	27/05/24	29/05/24	3
4.2	Device setup	Morgan	30/05/24	05/06/24	5
4.3	Database management	Morgan	06/06/24	14/06/24	7
4.4	Heatmap creation	Morgan	16/06/24	25/06/24	8
4.5	GUI	Morgan	25/06/24	02/07/24	6
4.6	Measurements	Morgan	07/06/2024	11/07/2024	26
5	**Internship report**				
5.1	Writing the report	Everyone	29/04/2024	20/08/2024	?
5.2	Presentation	Everyone	20/08/2024	27/08/2024	8

Figure 24. Final timetable

We were effective when studying WiFi technology, we managed to study the devices, the different layers, the attacks and protection methods on WiFi in a shorter period of time which gave us more flexibility to conduct our projects and tests.

When setting up the maquette to conduct jamming attacks and anti-jamming attacks it was necessary to not be in range of any WiFi networks to avoid jamming them.

Multiple solutions were proposed such as using a Faraday cage (Annex 1) to block incoming signals and outcoming signals in the box however measurements in the box would become obsolete because the signals inside the box would reflect and cause interference making measurements not relevant.

Next solution was to create a WiFi coverage heatmap to locate isolated areas where WiFi signals are not in range and so jamming attacks would not cause interference with other neighbouring networks.

After the meeting on the 29th May 2024, Prof. Lahoud and Prof. Zincir-Heywood brought the idea to focus on the heatmap creation and data collection. For the rest of the internship my primary goal was to create the WiFi coverage heatmap and create a database of the scanned networks. More ideas emerged such as the creation and use of a Graphical User Interface to easily filter data on the heatmap.

Now that you have seen the project and how it was organised, I will review my internship.

4 – Internship review

In my opinion, my internship was very captivating and fascinating because of the project I had but also because of the country, the people I have met throughout the past months. There weren't any difficulties to be integrated in Halifax and Dalhousie University. This final part summarises the technical, professional and social competences I have acquired and what I've learnt in this internship.

4.1. Canada & Dalhousie University

When I arrived at Halifax in April, I was warmly welcomed at the university. The students and professors were supportive and made me feel fully integrated in the team from the start. The environment in the lab was very positive all along my internship. I managed to learn the current academic projects, present my work in front of the lab as well as members of the National Defence. Take part in meetings and discuss about scientific and technical topics. My transition into the internship was smooth and enjoyable which I am very grateful for.

I have met and talked to many people outside the university as well. I learnt new cultures, work cultures and habits that I find marvellous. All the social interactions were as interesting as the project, always learning new things and creating memorable moments.

In summary, my internship was fully complete and corresponds to my current course in France. Learning how life is in a lab, in a workplace as an undergraduate research assistant in a foreign country.

4.2. New technical competences

An undergraduate research assistant's mission is to assist professors and PhD students in their academic projects and research. It is important to understand the research topics in order to complete measurements, analyse data and conduct surveys. Regarding WiFi technology, I had to first study it before conducting any tests.

Configuring ESP32 devices

At first, I was sceptical because I never learnt how to configure ESP32 devices but with the help of tutorials, explanations on forums and help from the lab team I managed to create a functional WiFi scanner which also registers GPS coordinates. But at first, to understand C programming language, I learnt it through basics such as using a built-in led or connecting the device to an access point.

Reading scientific papers in English

Scientific papers focus on a specific problem in which tests, measurements, statistics and references are used in order to communicate the outcomes to a targeted audience who can understand in a clear manner the document. So, in order to understand certain topics in WiFi technology it is important to also search and understand the terms which for me at first it wasn't an easy task but I was curious to further understand them in WiFi. This also improved my technical vocabulary in English.

Being independent

On the first days of my internship, I needed help to understand WiFi technology, attacks and protection methods. Day by day, I was able to develop competences to use the tools, devices and understand the results from the tests. I was able to freely decide my objectives day by day in order to complete my project which created a sense of self-direction. I learnt how WiFi technology functions and it was a good topic for my course because of the weak knowledge I had regarding telecommunications. This did not prevent me from learning further and asking questions to members of the lab and my supervisors.

4.3. Professional competences

Social interactions in the lab

There are many interactions in the workplace. For example, reporting my finds to my supervisors through Microsoft Teams or directly at their office. Also taking part in meetings with other members of the lab to discuss about concerns, faced problems and propose solutions in related projects. Also, assisting other students in their research such as taking measures or verifying their equipment. Personally, interactions with many different people in the lab developed my social competences and also improve my English.

Behaviour and habits in the lab

Everyday when arriving at the lab in the morning, it is important to greet co-workers, it is the least thing to do. It is also crucial to arrive at the workplace in a proper dress code and communicate with co-workers in a correct manner. This behaviour seems normal but it should be applied in the lab and also in other workplaces.

4.4. Summary

I learnt many technical, professional and social fundamentals in this internship in Canada. The experience was absorbing and was very interesting in which built many positive and a few negative points in my perspective.

Positive points

- An internship in a foreign country which improves my resume
- A new experience in cybersecurity and research domains
- Acquired new technical and scientific knowledge in English
- An environment that motivates me to take part in other similar projects

Negative points

- The length of the internship which prevented me to participate further in the projects
- The cost to do an internship in a foreign country outside Europe

Research field

- Use of technical knowledge from my course in the IUT
- Building a sense of curiosity and being passionate in certain scientific projects
- Creating a good relation with other researchers and helping each other

Future career

To have the opportunity to work in a foreign country in networking, cybersecurity, telecommunications and other interesting subjects corresponds to my goal for my future career. I am planning to work in the customs as an operating systems programmer which consists of supervising networks and maintaining equipment and participating in big projects between European countries. So, I find it important for me to work with foreigners to improve my technical English but also to understand cultures and traditions which I find important to know when working abroad. I am planning to also obtain a Master degree in the cybersecurity, networking or programming domains.

Conclusion

My internship at Dalhousie University lasted three months between end of April to July 2024. In the university my purpose as an undergraduate research assistant was to create a WiFi coverage heatmap of Halifax which in the long run could be used for academic projects related to telecommunications and network security. Dalhousie University is primarily oriented towards research in a variety of domains.

As an intern in the NIMS lab, I managed to learn how WiFi functions, how to configure devices, how to organise my project with the help of my supervisors and the lab. I am capable to study research documents and use the knowledge to conduct experiments and surveys.

The project that was supervised by Prof. Samer Lahoud and Prof. Nur Zincir-Heywood gave me the opportunity to work with other students, develop my technical knowledge and social interactions in English.

In a theoretical point of view, the project was a guide to study new technologies, potential attacks, protection methods and detection methods and it helped me to understand how to read scientific documents and analyse results.

In a technical point of view, I learnt how to configure devices using different programming languages and also improved my vocabulary through meeting sessions and interactions with other researchers.

In summary, my time at Dalhousie University and in Canada was not just an internship; it was a comprehensive learning experience that equipped me with the technical, professional, and social skills necessary for my future career. The challenges I faced and the knowledge I gained have made this experience truly absorbing and invaluable, setting the stage for the next steps in my academic and professional career.

Index

Glossary

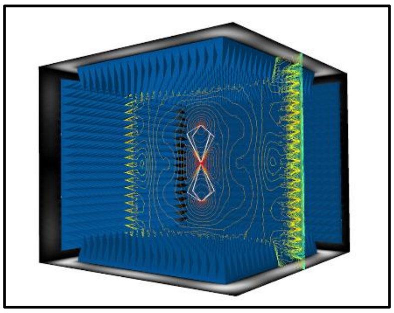
Name	Definition
WiFi	WiFi is a wireless technology that uses radio waves to provide internet access with the use of access points.
AP	**A**ccess **P**oint: a networking device that allows other WiFi devices to connect to a network.
GPS	**G**lobal **P**ositioning **S**ystem: a satellite-based navigation system that provides geolocation and time information to a GPS receiver or module.
CRTC	**C**anadian **R**adio-television and **T**elecommunications **C**ommission
SSID	**S**ervice **S**et **Id**entifier: it represents the name of a wireless network.
RSSI	**R**eceived **S**ignal **S**trength **I**ndication: it represents a measure of the power observed when receiving a signal often in dBm.
dBm	Decibel-milliwatts: a unit of power expressed.
MAC	Unique identifier assigned to a network interface. It can also signify the data-link layer.
WPA/WPA2/WPA3	**Wi**-Fi **P**rotected **A**ccess: security certification program to secure wireless networks.
WEP	**W**ired **E**quivalent **P**rivacy: a security algorithm for wireless networks.
SAE	**S**imultaneous **A**uthentication of **E**quals: a password-based authentication and password-authenticated key agreement method.
PSK	**Pre**-**S**hared **k**ey: a long series of random letters and numbers generated when a device connects to a wireless network through an access point.
TKIP	**T**emporal **K**ey **I**ntegrity **P**rotocol: a security protocol used in wireless networks; it was designed to replace WEP.
AES	**A**dvanced **E**ncryption **S**tandard: an encryption standard used in wireless networks.
OWE	**O**pportunistic **W**ireless **E**ncryption: A WiFi standard which ensures protected communications between endpoints.
Brute Force attack	It consists of submitting a certain number of passwords in order to guess it correctly.
IDE	**I**ntegrated **D**evelopment **E**nvironment: a software application that provides tools, libraries and guides to edit code, debug programs and execute code.
GUI	**G**raphical **U**ser **I**nterface: a user interface that allows users to interact with a device through graphical and visual elements like buttons.

Table of figures

Annex

1 – The concept of a Faraday cage

Faraday Cage is an enclosure that prevents certain types of electromagnetic radiation such as signals from entering or exiting with the use of certain materials like tin foil around the enclosure.



Annex 1. Example of a Faraday cage

Summary

My internship was in Canada, at Dalhousie University in the Faculty of Computer Science in NIMS laboratory from April to July 2024. The internship is mandatory to complete my 2nd year of my BUT Network engineering and Telecoms (equivalent to a bachelor degree). I decided to do my internship in a foreign country and discover research in network security and telecommunications domains as an undergraduate research assistant.

The Faculty of Computer Science founded in 1997 is focused towards many domains such as artificial intelligence, Big Data Analytics and innovations. I had the opportunity to assist professors and PhD students in their research in wireless networking and cybersecurity. As undergraduate research assistant supervised by Prof. Samer Lahoud and Prof. Nur Zincir-Heywood I was able to study scientific documents, take part in meetings, take measurements and data to create a WiFi coverage heatmap. I had to study WiFi technology first in order to conduct the tests and analyse the results.

After studying, I learnt with the help of the lab, the supervisors and tutorials to configure ESP32 devices with Arduino IDE to receive data from wireless network scans and GPS coordinates to locate myself. Once the data was collected, I was able to manage it in a SQL database and used it to create an interactive heatmap with a graphical user interface (GUI) in Python. Initially, my goal was to conduct jamming and anti-jamming experiments on WiFi networks which needed to be done in the safest ways possible to avoid interfering neighbouring networks. Multiple solutions were proposed such as using a Faraday cage and the WiFi coverage heatmap was the most convenient solution to locate areas with no WiFi signal. My supervisors decided and supported me to make the heatmap for future analysis and studies.

This internship was my first experience in a foreign country in research. I am highly interested to learn about telecommunications and networking technologies, academic projects conducted by researchers and discover the rich diversity the country has which has motivated me to work further abroad with foreigners. I acquired many competences throughout the internship which completes my 2nd year at Lannion's IUT.