Software Defined Radio (SDR) based sensing

By

Ajaya Dahal

Approved by:

Ali C. Gurbuz (Major Professor)
John E. Ball (Co-Major Professor)
Mehmet Kurum
Jenny Du (Graduate Coordinator)
Jason M. Keith (Dean, Bagley College of Engineering)

A Thesis
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Master of Science
in Electrical and Computer Engineering
in the Department of Electrical and Computer Engineering

Mississippi State, Mississippi

May 2024

Name: Ajaya Dahal

Date of Degree: May 10, 2024

Institution: Mississippi State University

Major Field: Electrical and Computer Engineering

Major Professor: Ali C. Gurbuz

Title of Study: Software Defined Radio (SDR) based sensing

Pages of Study: 108

The history of Software-Defined Radios (SDRs) epitomizes innovation in wireless communication. Initially serving military needs, SDRs swiftly transitioned to civilian applications, revolutionizing communication. This thesis explores SDR applications such as Spectrum Scanning Systems, Contraband Cellphone Detection, and Human Activity Recognition via Wi-Fi signals.

SDRs empower Spectrum Scanning Systems to monitor and analyze radio frequencies, optimizing spectrum allocation for seamless wireless communication. In Contraband Cellphone Detection, SDRs identify unauthorized signals in restricted areas, bolstering security efforts by thwarting illicit cellphone usage. Human Activity Recognition utilizes Raspberry Pi 3B+ to track movement patterns via Wi-Fi signals, offering insights across various sectors.

Additionally, the thesis conducts a comparative analysis of Wi-Fi-based Human Activity Recognition and Radar for accuracy assessment. SDRs continue to drive innovation, enhancing wireless communication and security in diverse domains, from defense to healthcare and beyond.

Keywords: Human Activity Recognition, HAR, Wi-Fi, Software Defined Radio, SDR, Raspberry Pi, Intel Wireless 5300 Wi-Fi Card, Channel State Information, CSI, Device Fingerprinting, Location Fingerprinting

ACKNOWLEDGEMENTS

Funding for this work was provided through a non-assistance cooperative agreement with the United States Engineer Research and Development Center (ERDC) - Scorpion Project (Sponsor Award# W912HZ-21-2-0053, MSU Grant# G00006267).

I would like to thank fellow members of the IMPRESS lab for their support in carrying out this work. I would like to thank Dr. Ali C. Gurbuz (Mississippi State University (MSU)), Dr. John E. Ball (MSU) and Dr. Mehmet Kurum(UGA) for their guidance in system design and various experiments. I would also like to thank them for giving me the opportunity to work on these projects and the invaluable experience I have gained as a result of working in the IMPRESS lab.

Finally, I would like to thank my parents Menuka Dahal and Yubaraj Dahal, for their support and patience throughout these years, and my sister, Ankita Dahal, for her encouragement, and constant support in my pursuits.

PUBLICATIONS BASED ON THIS THESIS

[Submitted] **Ajaya Dahal**, Sabyasachi Biswas, Sevgi Z. Gurbuz, and Ali C. Gurbuz. "Comparison Between Wifi-CSI and Radar-based Human Activity Recognition", IEEE Radar Conference (RadarConf24)

[Submitted] **Ajaya Dahal**, Sabyasachi Biswas, Sevgi Z. Gurbuz, and Ali C. Gurbuz. "Robustness analysis of Wi-Fi-based human activity recognition", SPIE Defense + Commercial Sensing (DCS24)

[31] Fahmida Islam, Jason Farmer, **Ajaya Dahal**, Bo Tang, John E. Ball, and Maxwell Young. "Wi-Fi Fingerprinting-Based Room-Level Classification: Combining Short Term Fourier Transform and Imbalanced Learning Method." In Proceedings Volume 12122, Signal Processing, Sensor/Information Fusion, and Target Recognition XXXI, 121220Y, 2022. doi: 10.1117/12.2618717.

[36] Surya Kodipaka, **Ajaya Dahal**, Logan Smith, Nicholas Smith, Bo Tang, John E. Ball, and Maxwell Young, "Adversarial indoor signal detection," in Proc. SPIE 11756, Signal Processing, Sensor/Information Fusion, and Target Recognition XXX, 1175615, 12 April 2021. [Online]. Available: doi: 10.1117/12.2587525.

[69] Logan Smith, Nicholas Smith, Surya Kodipaka, **Ajaya Dahal**, Bo Tang, John E. Ball, Maxwell Young, "Effect of the short time Fourier transform on the classification of complex-valued mobile signals," in Proc. SPIE 11756, Signal Processing, Sensor/Information Fusion, and Target Recognition XXX, 117560Y, 21 May 2021. doi: 10.1117/12.2587664.

[70] Nicolas Smith, Logan Smith, Surya Kodipaka, **Ajaya Dahal**, Bo Tang, John E. Ball, Maxwell Young, "Real-time location fingerprinting for mobile devices in an indoor prison setting," in Proc. SPIE 11756, Signal Processing, Sensor/Information Fusion, and Target Recognition XXX, 1175612, 12 April 2021. doi: 10.1117/12.2587679.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS, ABBREVIATIONS, AND NOMENCLATURE

MSU Mississippi State University

SDR Software Defined Radio

HAR Human Activity Recognition

Wi-Fi Wireless Fidelity

CSI Channel State Information

OFDM Orthogonal Frequency Division Multiplex

ADC Analog to Digital Converter

DAC Digital to Analog Converter

DSP Digital Signal Processing

TX Transmit

RX Receive

RF Radio Frequency

IF Intermediate Frequency

FPGA Field Programmable Gated Array

UHD USRP Hardware Driver

USRP Universal Software Radio Peripheral

NI National Instrument

LNA Low Noise Amplifier

DDC Digital Down Converter

LPF Low Pass Filter

DUC Digital Up Converter

LO Local Oscillator

USB Universal Serial Bus

DVB Digital Video Broadcasting

QPSK Quadrature Phase Shift Keying

QAM Quadrature Amplitude Modulation

UFH Ultra High Frequency

MAC Media Access Control

RSSI Received Signal Strength Indicator

RMSE Root Mean Square Error

ESPRIT Estimation of Signal Parameters via Rotational Invariant Techniques

AoA Angle of Arrival

DoA Direction of Arrival

TDOA Time Difference of Arrival

FDOA Frequency Difference of Arrival

IMU Inertial Measurement Units

UDP User Datagram Protocol

TCP Transmission Control Protocol

WLAN Wireless Local Area Network

CSV Comma Separated Value

DT Decision Tree

RSRP Reference Signal Received Power

MIMO Multiple Input Multiple Output

PCA Principal Component Analysis

MAD Median Absolute Deviation

STF Short Training Field

LTF Long Training Field

STA Space-Time Algorithm

ReLU Rectified Linear Unit

STFT Short-Time Fourier Transform

GUI Graphical User Interface

MLP Multilayer Perceptron

FFT Fast Fourier Transform

IFFT Inverse Fast Fourier Transform

IIR Infinite Impulse Response

DNN Deep Neural Network

RTL Realtek

AR Augmented Reality

VR Virtual Reality

ML Machine Learning

CBRS Citizens Broadband Radio Service

GNSS Global Navigation Satellite System

XM Sirius Satellite Radio

LEO Low Earth Orbit

GEO Geostationary Orbit

MEO Medium Earth Orbit

PC Personal Computer

NUC Next Unit of Computing

UHF Ultra High Frequency

ToA Time of Arrival

FM Frequency Modulation

IQ In-phase and Quadrature

ANT Antenna

CBRS Citizens Broadband Radio Service

4G Fourth Generation (of cellular network technology)

5G Fifth Generation (of cellular network technology)

LPF Low-Pass Filter

FMCW Frequency-Modulated Continuous Wave

CB Convolution Block

CNN Convolutional Neural Network

DNN Deep Neural Network

ESP Espressif (a manufacturer of microcontroller platforms)

NODEMCU Node Micro Controller Unit (a development board for the Internet of Things)

HDF5 Hierarchical Data Format 5

RBF Radial Basis Function

DWT Discrete Wavelet Transform

LSTM Long-Short Term Memory

SVM Support Vector Machine

HMM Hidden Markov Model

kNN K-Nearest Neighbor

RNN Recurrent Neural Network

CHAPTER I

INTRODUCTION

In a world constantly shaped by technological progress, the realm of radio communication has experienced a profound and groundbreaking transition. Traditional radios, marked by their fixed hardware components and limited adaptability, have inspired engineers to invent a revolutionary paradigm known as Software Defined Radio (SDR). This game-changing transition in wireless communication technology brings a unique level of flexibility, versatility, and reconfigurability, effectively redefining the conventional boundaries that once constrained radio systems.

Radio communication has a rich history that covers more than a century, with pioneers like Guglielmo Marconi and Nikola Tesla playing significant roles in its development. In its early days, radio systems relied heavily on analog circuitry, requiring dedicated hardware components for each frequency band and modulation scheme. While these systems were remarkably effective for their time, they struggled to keep up with the rapidly evolving demands of modern communication. The emergence of digital technology represented a major milestone in the evolution of radio communication. The introduction of digital technology marked a significant shift in radio communication. DSP techniques began to replace analog components, bringing with them greater flexibility and enhanced performance. However, substantial changes to radio functionality still demanded physical hardware modifications.

The idea of SDR emerged as a determined solution to the limitations imposed by conventional radio systems. SDR represents a technological paradigm shift by enabling radio systems to be primarily implemented through software. This dynamic reconfiguration of radio functions via software updates eliminates the need for hardware modifications, opening up new possibilities in the world of radio communication. At its core, SDR operates on the premise that Radio Frequency (RF) signals can be digitized and processed using software on a general-purpose computer or dedicated SDR hardware. Moving away from fixed, hardware-dependent functionality to software-driven adaptability has sparked a revolution, profoundly changing the way we approach the design, implementation, and deployment of radio systems.

Software-defined radio offers numerous advantages over traditional radio systems. SDR systems seamlessly navigate various frequency bands, modulation schemes, and protocols, for dynamic communication protocol requirements. The ability to reconfigure radio functionality through software updates minimizes the need for costly hardware modifications, making SDR a cost-effective choice for long-term deployments. SDR systems intelligently manage and optimize spectrum usage, enhancing the utilization of available frequency bands while mitigating interference. SDR platforms have opened the door to experimentation, research, and innovation in a wide array of wireless technology domains.

One of the application of SDR discussed in this thesis is Human Activity Recognition (HAR). HAR is the process of using RF sensors and machine learning algorithms, to identify and understand the actions or movements that people are performing. It involves analyzing data from various sources, such as wearable devices, Radar, or Wi-Fi signals, to determine activities like walking, running, sitting, or more complex actions like cooking or walking, running or falling. This

technology has a wide range of applications, from fitness tracking and healthcare to security and smart home automation.

1.1 Thesis Structure

In this thesis, a diverse collection of SDRs serves as versatile tools for a wide range of applications, demonstrating the transformative potential of this technology. Chapter II, the core focus of this thesis, explores deep into the inner workings of SDR. It details background on SDRs and exposes the fundamental principles that make SDR possible by carefully dissecting the technology that forms its foundation. Starting from Analog to Digital Converter (ADC) to DSP, this chapter offers a comprehensive insight into the complex subsystems that empower SDR to adapt and reconfigure itself in real time. By the conclusion of this chapter, readers will possess a profound understanding of the technical ins and outs at the heart of the world of SDR.

Chapter III showcases a collection of applications developed for this project using a variety of SDRs, serving as real-world examples of how this technology is applied in practical scenarios. This chapter has four distinct applications where SDR exercises a significant influence:

Spectrum Scanning System: This section focuses on how SDR enables the creation of highly efficient spectrum scanning systems. SDR empowers these systems to rapidly and efficiently scan the radio frequency spectrum for various signals, with applications that extend to spectrum management and interference detection. This document describes how a spectrum scanning system can play a crucial role in identifying signals of opportunity for passive microwave remote sensing. By continuously scanning the electromagnetic spectrum, this technology can detect and catalog various radio frequency signals emitted by communication devices, satellites, and other sources.

These signals often inadvertently carry valuable information about the Earth's environment, such as soil moisture, or sea surface conditions. The spectrum scanning system's ability to capture and analyze these signals allows scientists and researchers to leverage existing infrastructure and data sources for passive microwave remote sensing applications, providing a cost-effective and efficient means to monitor and study our planet's dynamic processes and phenomena. In addition, continuous observation of the spectrum can reveal the detection of interferences, or allow spectrum sharing between multiple types of users such as comm and radar/sensing systems.

Human Activity Recognition System: Within this section, readers are introduced to the potential of human activity recognition systems using SDR technology. This application reveals how SDR can be utilized to detect and classify human activities through radio signals, thereby finding applications in healthcare, security, and smart environments. This section also explains how this system helps to detect fall, slip injuries in nursing home with realtime notification.

SDR in Detecting Illegal Cellphones Inside Prisons: This section highlights a socially relevant application of SDR technology. It clarifies how SDR is employed in the detection of illegal cellphones within correctional facilities, such as prisons. The smuggling and use of contraband cellphones by inmates pose significant security threats, enabling unauthorized communication with the outside world and potential criminal activities. SDR emerges as an innovative and effective solution to counteract this challenge.

Chapter IV presents the outcomes and results of the applications detailed in Chapter III, making this section the focal point of this document. This is where theory converges with reality, where the practical implications of SDR become tangible and measurable. It offers an opportunity to witness how SDR technology translates into tangible impact and real-world solutions across a

variety of applications, ranging from enhanced spectrum management to the secure environment of correctional facilities.

Chapter V marks the end of the document by summarizing the main the applications and findings discussed in the thesis. It provides direction for inspiring and guiding future research in the field, facilitating a transition from the presented past research to the exciting possibilities for further work.

1.2 Contributions

The list below summarizes my contributions.

1. Developed a spectrum scanning system for monitoring occupied spectrums in passive microwave remote sensing.
2. Constructed a testbed for contraband cellphone detection within prison facilities, including dataset collection and extensive research on machine learning models.
3. Created a data collection system for HAR utilizing a Wi-Fi-based infrastructure.
4. Trained a CNN-based model for HAR detection.
5. Published research outcomes in multiple conference and journal papers.

CHAPTER II

BACKGROUND OF SDRS

2.1 History of SDRs

The history of SDRs is a story of innovation and adaptability in the world of wireless communication. It began as a concept in the mid-20th century but truly gained momentum in the late 20th and early 21st centuries. In the mid-20th century, radio communication relied on analog components, making it challenging to adapt to changing signal standards. The development of SDR began in the 1970s with pioneering work by researchers like Joseph Mitola, who envisioned a radio that could adapt and evolve through software, rather than being bound by fixed, analog hardware [21] [13][15]. This vision laid the foundation for modern SDR systems. Initially developed for military and defense applications, SDRs found their way into the civilian realm, transforming the way we communicate. The 1990s saw the emergence of open-source software like GNURadio, making SDR technology more accessible to researchers and enthusiasts. Over the years, SDRs have evolved, offering greater flexibility, adaptability, and improved processing power. Today, they are integral to cellular networks, public safety systems, space exploration, and various wireless technologies. SDRs continue to shape the future of wireless communication, enabling rapid advancements in the field.

At its core, a SDR relies on a flexible and reconfigurable hardware platform that distinguishes it from traditional radio systems. Instead of being tied to fixed, dedicated hardware components

for specific frequency bands or modulation schemes, SDR hardware employs a general-purpose processing unit and ADC converters, which can adapt to a vast spectrum of frequencies and communication protocols. Moreover, SDR hardware simplifies the development and deployment of new wireless technologies. Instead of designing complex, specialized hardware for each application, engineers can focus on software development to create innovative communication solutions. This not only accelerates the pace of innovation but also reduces costs associated with hardware manufacturing and maintenance. SDR systems consist of three primary hardware components: the antenna, the ADC, and the DSP. The antenna captures radio-frequency signals, while the ADC converts them into digital data. The DSP then processes this digital data, allowing for real-time signal manipulation and demodulation. Understanding how these components work together is key to unlocking the potential of SDR.

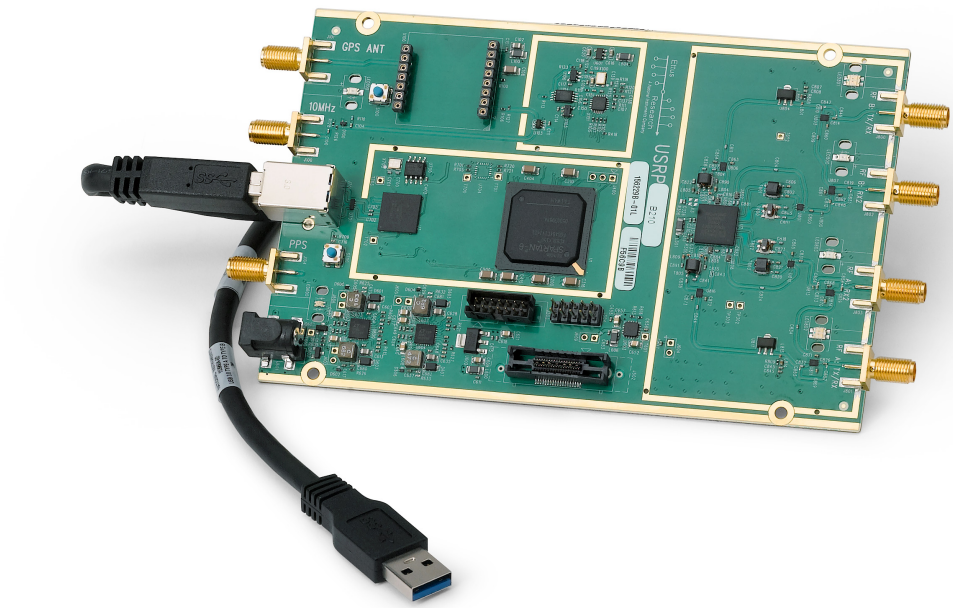


Figure 2.1: B210 SDR from NI/Ettus without enclosure [28]

2.1.1 Antenna

Starting with the antennas, they come in various types and shapes, each tailored to specific frequency bands and applications. For instance, a Yagi-Uda antenna is excellent for directional signal reception, ideal for tasks like amateur radio communication, while a dipole antenna is a versatile choice for a wide range of frequencies. The choice of antenna depends on the intended use of the SDR system and the characteristics of the signals one wishes to capture.

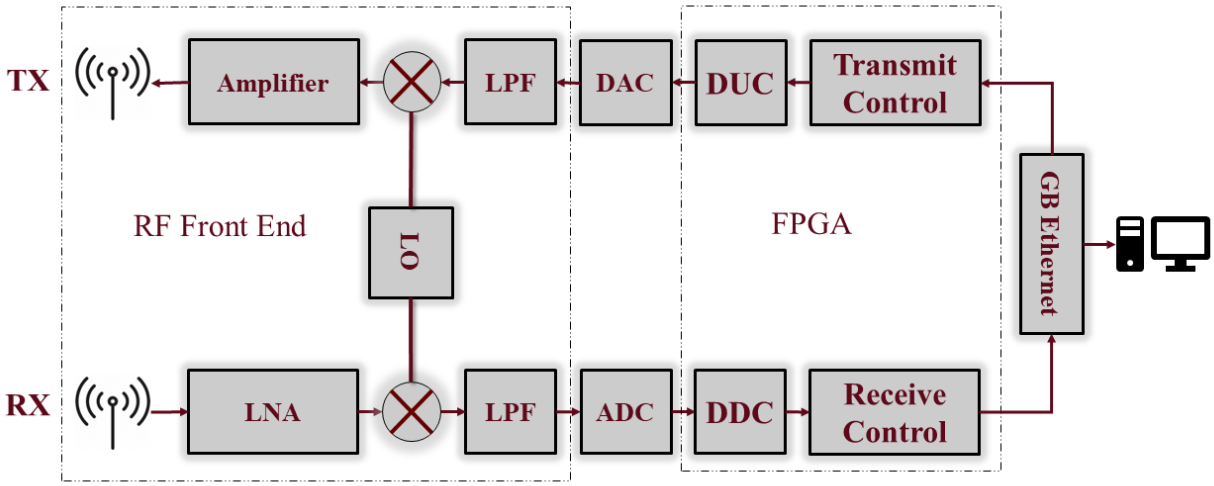


Figure 2.2: SDR block diagram [19]

2.1.2 DSP

Then comes the DSP, lying at the heart of SDR hardware is the Field Programmable Gated Array (FPGA). These components can be programmed and reprogrammed with software to define their functionality, enabling users to rapidly switch between different radio frequencies, modulations, and protocols. This flexibility is invaluable for radio enthusiasts, researchers, and professionals as it allows them to explore and experiment with various radio waveforms, decode different signals, and even design custom communication systems for specific needs. This adaptability is particularly beneficial in scenarios where real-time adjustments are required, such as in military communications, emergency services, or even space exploration.

Let's consider a radio wave carrying an FM broadcast signal. Here, the ADC continuously samples this analog wave, measuring its amplitude at regular intervals. These samples are then quantized into digital values. The ADC's resolution, measured in bits, determines the level of detail in these measurements. Higher-resolution ADCs can capture subtle variations in signal

amplitude with greater precision. When it comes to implementing the ADC in an SDR system, FPGAs are often used. Below are some reasons why FPGAs are used [13] [21]:

- Interface with the ADC: FPGAs can be programmed to control and manage the data flow between the ADC and the DSP chain. They handle tasks such as setting the sampling rate, managing data buffers, and interfacing with other components.
- Data Pre-processing: FPGAs can perform preliminary data processing tasks on the incoming samples, such as filtering, decimation, or digital down-conversion. This can reduce the processing load on the subsequent DSP stages.
- Parallel Processing: FPGAs excel at parallel processing, which is essential in SDR systems that often deal with a multitude of signal channels and complex algorithms. FPGAs can be configured to process multiple channels simultaneously.
- Customization and Adaptability: One of the significant advantages of FPGAs in SDR is their adaptability. Users can reprogram FPGAs to customize and optimize the ADC interface and data processing pipeline for specific applications. This flexibility allows SDR systems to support various signal standards and adapt to changing requirements.
- High-Speed Data Handling: FPGAs are capable of handling high-speed data streams, making them suitable for SDR systems operating in wide bandwidths or requiring real-time processing of large data volumes. They can efficiently manage data flows between the ADC and the DSP components.
- Energy Efficiency: Many modern FPGAs are designed with power-efficient features, making them suitable for portable and battery-operated SDR devices where power consumption is a critical consideration.

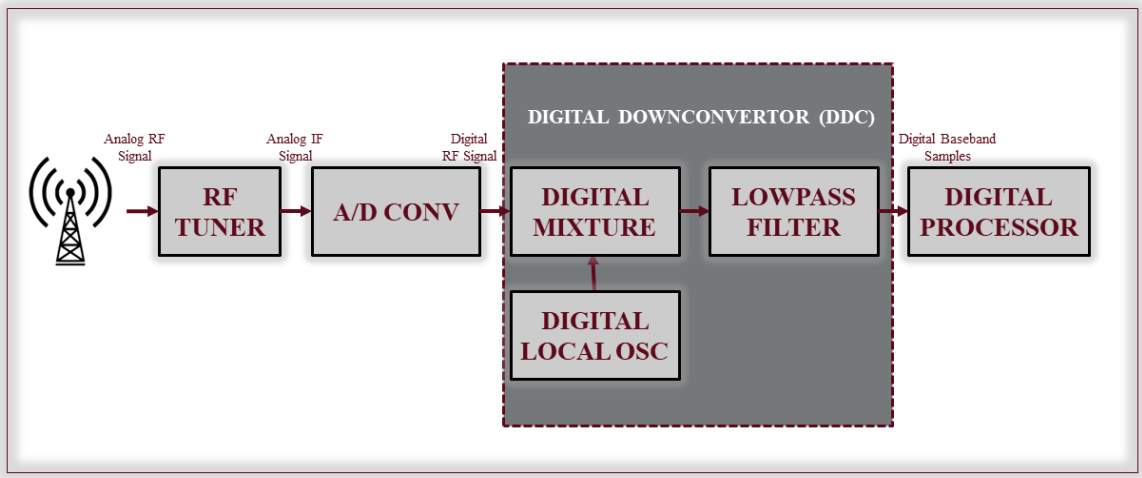


Figure 2.3: SDR functional diagram [48]

Figure 2.4 shows the software component and hardware components inside an SDR.

The next sections describe these components in detail.

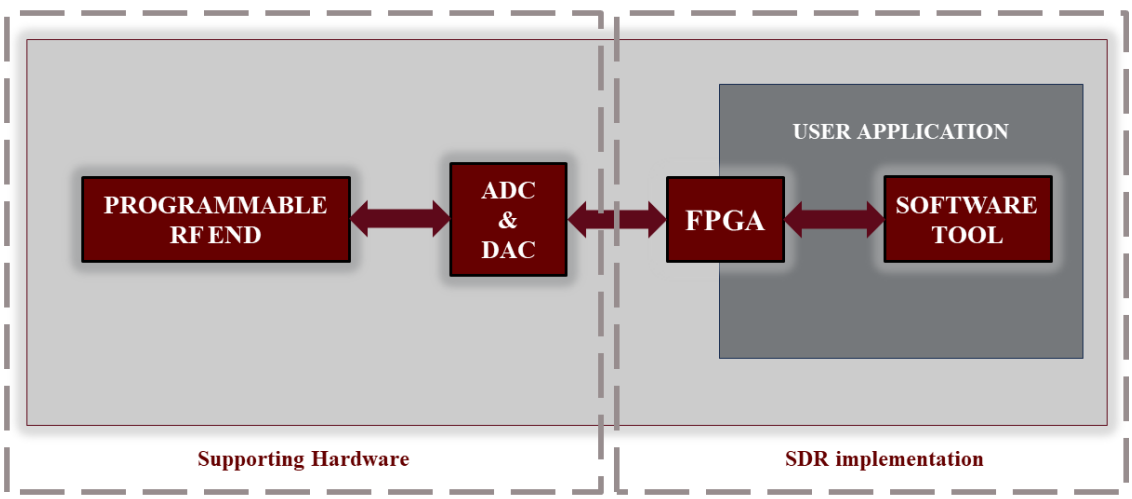


Figure 2.4: Software vs Hardware plus user application space [15]

2.1.3 Hardware Perspective

Now let's look into the hardware perspective of how SDR works under the hood starting from the TX side.

2.1.3.1 TX Chain (Transmit Process)

The TX process in SDR from a hardware perspective is characterized by its flexibility and adaptability, allowing for the generation and transmission of radio signals through reconfigurable hardware components. Here's a detailed description of the TX process in SDR hardware [13] [21]:

- Digital Signal Source: In SDR, the TX process almost always starts with a digital signal source. This could be a digital audio stream, data packet, or any other form of digital information that needs to be transmitted.
- DSP: The digital signal undergoes DSP operations, which involve various algorithms and filters to prepare it for modulation. These operations can include error correction coding, data formatting, and signal conditioning to ensure it meets the requirements of the modulation scheme.
- Modulation: SDRs provide the flexibility to implement various modulation schemes purely through software. The digital signal is modulated according to the chosen scheme, such as Quadrature Phase Shift Keying (QPSK), Quadrature Amplitude Modulation (QAM), or others, by manipulating the phase, frequency, and amplitude of the signal.
- Digital to Analog Converter (DAC): The modulated digital signal is then converted into an analog signal using a DAC. The DAC output is a continuous waveform that represents the modulated signal in the analog domain.
- RF Components: SDR hardware incorporates RF components, such as mixers, filters, and amplifiers, which are often reconfigurable. These components are used to mix the analog signal with a carrier frequency, filter out unwanted frequencies, and amplify the signal to the desired power level.
- Frequency Synthesizer: SDRs typically employ a frequency synthesizer that generates a stable carrier frequency. This component can be reprogrammed to set the desired transmission frequency.
- Antenna: Like in traditional radio transmitters, SDRs use an antenna to radiate the RF signal into space. Antenna selection and design are important factors in determining the signal's propagation characteristics and coverage area.

- Transmission Control and Monitoring: SDRs offer control and monitoring capabilities through software interfaces, enabling users to adjust transmission parameters, such as frequency, modulation type, and power level in real time. These controls ensure compliance with regulatory requirements and adaptability to changing communication conditions.

2.1.3.2 RX Chain (Receive Process)

Similarly, the RX process in SDR from a hardware perspective involves a series of components and steps that enable the reception, demodulation, and processing of radio signals with a high degree of flexibility and adaptability. Here's a detailed description of the RX process in SDR hardware [13] [21]:

- Antenna: The RX process begins with the antenna, which captures incoming radio signals from the environment. The antenna design and characteristics influence the receiver's sensitivity, selectivity, and coverage area.
- RF Front-End: SDR hardware often includes a reconfigurable RF front-end. This component is responsible for tasks like filtering, amplification, and downconversion. Filters remove unwanted frequencies, amplifiers boost the weak incoming signals, and mixers downconvert the RF signals to an IF or baseband.
- ADC: After downconversion, the analog IF or baseband signal is digitized using an ADC. The ADC converts the continuous analog waveform into digital samples, which can be processed and manipulated by the SDR's digital signal processing capabilities.
- DSP : The digitized signal undergoes DSP operations to extract and manipulate the received data. DSP tasks may include filtering, equalization, and synchronization to correct channel impairments and prepare the signal for demodulation.
- Demodulation: SDRs offers the flexibility to implement various demodulation schemes through software. Demodulation reverses the modulation applied by the transmitter, extracting the original information from the received signal. This can include techniques like coherent demodulation for phase-shift keying or frequency demodulation for frequency-modulated signals.
- Digital Signal Source: The demodulated signal is treated as a digital signal source for further processing. This could involve decoding, error correction, or any specific signal processing required for the application.
- Data Processing and Decoding: The digital signal source is processed to extract meaningful data. This could include audio decoding for voice communication, data packet parsing for

digital communication, or any other relevant processing based on the application's requirements.

- Output: The processed data is then made available for use by the application or user. This could involve sending the data to a display, speaker, or another system for further analysis or action.
- Control and Monitoring: SDRs often provide control and monitoring interfaces through software, allowing users to adjust reception parameters, such as frequency, bandwidth, and signal strength. This adaptability is vital for optimizing reception in varying conditions.

2.1.4 Software Perspective

There are various ways SDR can be configured. One popular framework that is used to program SDR is GNURadio. GNURadio is an open-source software toolkit that's like a Swiss Army knife for radio enthusiasts and professionals [20]. With its vast library of signal processing blocks and intuitive graphical interface, GNURadio makes it easy to build and experiment with software-defined radio systems. It can be used to decode digital signals, create various wireless communication protocols, or explore radar applications [13] [21].

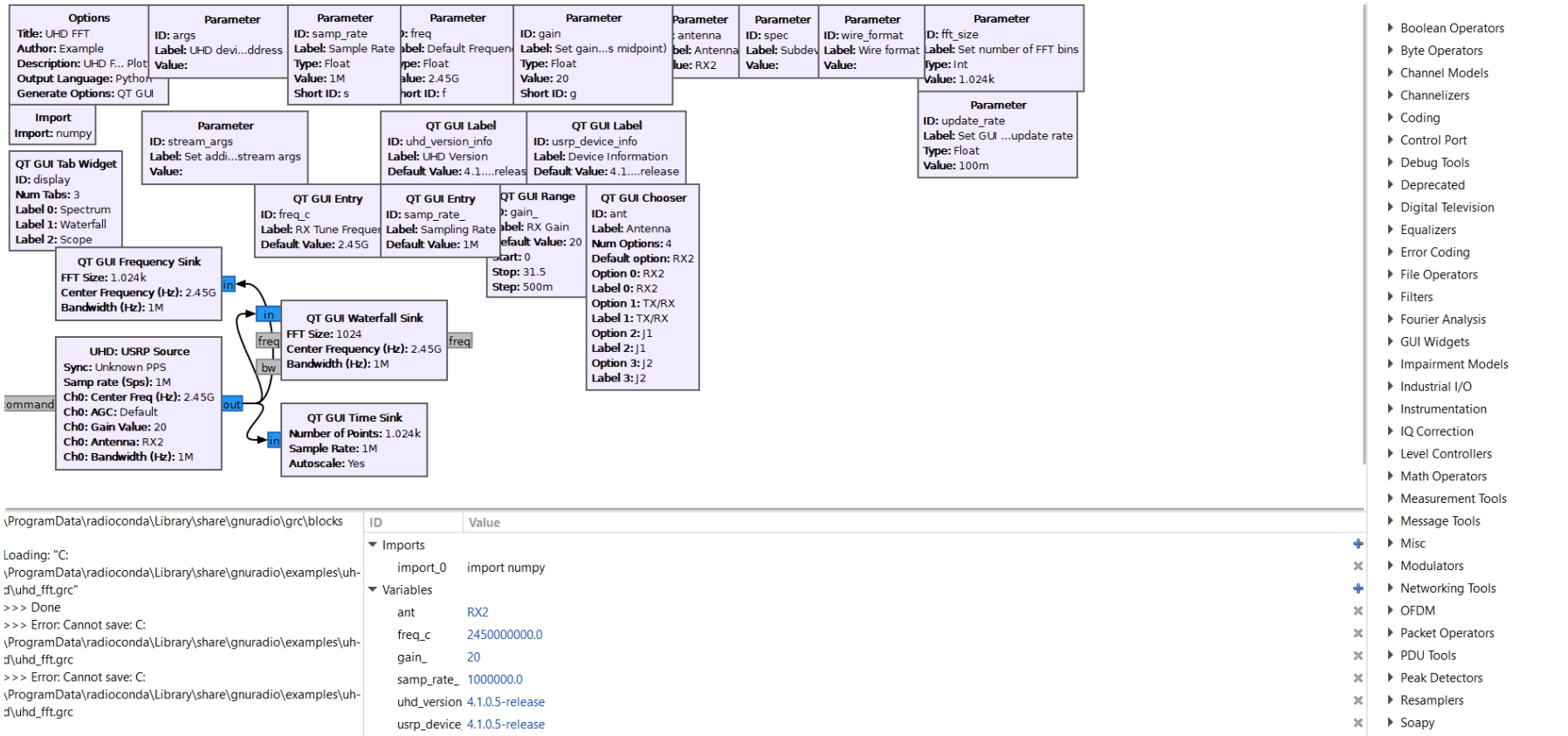


Figure 2.5: GNURadio flowgraph example [71] [70] [20]

What sets GNURadio apart is its ability to let users tinker with radio communication using a computer and a compatible SDR device, making it a playground for innovation and learning in the world of wireless technology. Its active community and Python integration also mean users can get started quickly and find plenty of support along the way. The next section describes how and where exactly software plays a role in ”Software” Defined Radio.

2.1.4.1 TX Chain (Transmit Process)

SDR software plays an equally important role in both the TX and RX processes by offering users the ability to configure, control, and adapt various aspects of the radio communication chain. This software-defined flexibility is a key advantage of SDR, enabling its use in a wide range of applications across diverse wireless communication scenarios [13] [21].

- Signal Source: In the TX chain, the software begins by accessing a digital signal source, which could be a microphone input, pre-recorded audio, or digital data from a source file.
- DSP: The software applies digital signal processing algorithms to the source signal. These algorithms might include filtering, equalization, or compression, depending on the specific application.
- Modulation: SDR software provides the flexibility to choose and configure modulation schemes through software settings. Users can select modulation types like QPSK, QAM, or any other scheme, and adjust modulation parameters as needed.
- DAC: The software sends the modulated digital signal to the DAC, which converts it into an analog signal that can be processed further in the hardware chain.
- RF Hardware Control: Software interfaces allow users to control the RF hardware components, such as frequency synthesizers, filters, and power amplifiers. This enables real-time adjustments of the transmission frequency, bandwidth, and power level.
- Antenna Selection: Users can configure antenna parameters, including antenna selection, polarization, and gain, depending on the application and desired coverage.
- Transmission Control: The software provides control over the transmission process, allowing users to initiate, pause, or terminate transmissions as needed. It can also include features like automatic frequency hopping or adaptive modulation for optimizing communication in changing conditions.

- Monitoring and Feedback: SDR software often includes monitoring tools that display important parameters, such as signal strength, bandwidth utilization, and error rates. This feedback helps users assess the quality of their transmissions in real time.

2.1.4.2 RX Chain (Receive Process)

Now looking from the RX side, this section explains the entire process of how software helps to receive data effectively [13] [21].

- Antenna Selection: SDR software allows users to configure antenna parameters for reception, similar to the TX chain. This includes selecting the appropriate antenna, polarization, and gain settings.
- RF Hardware Control: Users can control the RF front-end components, including the frequency, bandwidth, and gain settings. This adaptability is crucial for optimizing reception in different environments.
- ADC: The received analog signal is digitized by the ADC, producing a digital representation of the signal.
- DSP : The digitized signal undergoes DSP operations, such as filtering, demodulation, and synchronization, to extract the relevant information from the received signal.
- Demodulation: SDR software allows users to select and configure the demodulation scheme through software settings, reversing the modulation applied at the transmitter.
- Data Processing and Decoding: The software processes the demodulated signal to extract meaningful data. This could involve decoding audio, parsing data packets, or any other application-specific processing.
- Monitoring and Feedback: Similar to the TX chain, SDR software provides monitoring tools that display key reception parameters, helping users assess the quality of the received signal.
- Output: The processed data is made available for further analysis, display, or action by the user or the application.
- Control and Adaptation: SDR software continuously adapts reception parameters based on environmental conditions and user-defined settings. This adaptability is a hallmark of SDR technology, ensuring optimal performance in dynamic communication scenarios.

2.1.5 Embedded processes

This section describes the embedded perspective which shows how hardware and software work together to make SDR possible [13] [21].

2.1.5.1 TX Chain (Transmit Process)

In embedded SDR systems, the transition between hardware and software is a dynamic and tightly integrated process, allowing for flexible and adaptable radio communication. Hardware components handle initial signal processing and configuration, while software enables user control, signal manipulation, and adaptability in real-time communication scenarios [13] [21].

- Signal Acquisition: The TX process begins with the acquisition of a digital signal from various sources, such as sensors, audio inputs, or data stored in memory [13] [21].
- DSP : The digital signal is processed within the embedded system's hardware, often involving dedicated DSP or microcontroller units. Here, hardware components perform initial filtering and possibly some basic signal conditioning.
- Modulation Configuration: The embedded system uses software to configure the modulation scheme. The software defines modulation parameters and prepares the hardware components accordingly. These parameters might include modulation type, symbol rate, and carrier frequency.
- DAC: The software instructs the DAC to convert the processed digital signal into an analog waveform, which is then sent to the hardware RF components.
- RF Hardware Control: Software plays a crucial role in controlling the RF hardware components. Users can adjust settings like transmission frequency, power level, and bandwidth through software interfaces, enabling real-time adaptability.
- Antenna Selection: Software settings dictate the antenna configuration, including antenna selection, polarization, and gain. These selections are implemented through hardware control in embedded systems.
- Transmission Control: Software interfaces provide control over the transmission process. Users can initiate, pause, or terminate transmissions through software commands, which are executed by the embedded hardware.

2.1.5.2 RX Chain (Receive Process)

Similarly, this section describes SDR inner workings from an embedded perspective from the RX side [13] [21].

- Antenna Selection: The RX process starts with software configuring antenna parameters. Users specify antenna selection, polarization, and gain through software settings, which are implemented by the embedded hardware.
- RF Hardware Control: Software controls the RX hardware components, allowing users to set parameters like reception frequency, bandwidth, and gain. The software interacts with the hardware to configure these settings.
- ADC: The hardware component, the ADC, digitizes the received analog signal. The digitized signal is then passed to the software for further processing.
- DSP : Within the embedded system's hardware, initial DSP may occur, including filtering and downconversion. The resulting digital signal is then processed by software algorithms to extract meaningful information.
- Demodulation Configuration: The embedded software configures the demodulation scheme, specifying modulation type and parameters. These settings are then applied by the hardware components for demodulation.
- Data Processing and Decoding: The hardware performs initial data processing, and then the software continues processing to extract meaningful data. This might involve audio decoding, data packet parsing, or any other relevant processing tasks.
- Monitoring and Feedback: Monitoring tools and feedback mechanisms collect reception data, which is then processed by the software for display, analysis, or user feedback.

2.1.6 Utilization of Various SDRs in this Study

In this project, 6 different SDRs were experimented with to work on various applications that are discussed in this section. Those SDRs include NI B205 mini, NI B210, NI X310, NI E312, Realtek (RTL) SDR, and HackRF One shown in Figure 2.6a-2.6f. Next details about each utilized SDR are provided:

(a) NI B205-mini [28] (b) NI B210 [28] (c) NI X310 [28]

(d) NI E312 [28] (e) RTL SDR version 3 [59] (f) Hack RF One [22]

Figure 2.6: SDRs used in this thesis work

a. NI B205-mini: Figure 2.6a shows a small form factor SDR designed by NI. The specifications for this model are shown in Table 2.1.

Table 2.1: Specifications for NI B205 mini [28]

Specification	Value
Power output	> 10 dBm
Receive Noise Figure	< 8 dB
TX and RX	2 each Half or Full duplex
MIMO Supported	2x2
Freq range	70MHz – 6MHz
Bandwidth 1x1	Up to 56MHz
Bandwidth 2x2	Up to 30.72MHz
Power Supply	Universal Serial Bus (USB)-powered (5V)
Compatibility	Windows, Linux, macOS
Antenna Connector	SMA (female)
Cost	Typically around 1500 to 1600 (may vary)

b. NI B210: Figure 2.6b shows another popular SDR designed by NI. The specifications for this model are shown in Table 2.2.

Table 2.2: Specifications for NI B210 [28]

Specification	Value
Power output	> 10 dBm
Receive Noise Figure	< 5.5 dB
TX and RX	2 each Half or Full duplex
MIMO Supported	2x2
Freq range	70MHz – 6MHz
Bandwidth 1x1	Up to 56MHz
Bandwidth 2x2	Up to 30.72MHz
Power Supply	USB-powered (5V)
Compatibility	Windows, Linux, macOS
Antenna Connector	SMA (female)
Cost	Typically around 2000 to 2200 (may vary)

c. NI X310: Figure 2.6c shows another popular SDR designed by NI. This one is not as portable as the previously shown models however, it is much more powerful. The specifications for this model are shown in Table 2.3.

Table 2.3: Specifications for NI USRP X310 with UBX 160 daughtercard [28]

Specification	Value
Frequency Range	10MHz to 6MHz (with UBX 160 daughtercard)
ADC Resolution	12 bits (with UBX 160 daughtercard)
Maximum Sample Rate	Up to 200 MS/s
Transmit Channels (TX)	Up to 2
Receive Channels (RX)	Up to 2
MIMO Supported	2x2 (model-dependent)
Antenna Connector	SMA (female)
Power Supply	Typically external (not USB-powered)
Compatibility	Windows, Linux, macOS
Cost	10000 + 2100 = 12,000

d. NI E312: Figure 2.6d shows yet another battery-powered SDR designed by NI. The specifications for this model are shown in Table 2.4.

Table 2.4: Specifications for NI E312 [28]

Specification	Value
Power output	10 dBm approx.
Receive Noise Figure	Varies
TX and RX	2 each Full duplex
MIMO Supported	2x2
Freq range	70MHz – 6MHz
Bandwidth 1x1	Varies
Bandwidth 2x2	Varies
Power Supply	USB-powered (5V)
Compatibility	Windows, Linux, macOS
Antenna Connector	SMA (female)
Cost	Typically around 5500 to 5700 (may vary)

e. RTL SDR Figure 2.6e shows RTL dongle SDR. The origins of RTL-SDR stem from mass-produced Digital Video Broadcasting (DVB)-T TV tuner dongles that were based on the RTL2832U chipset. With the combined efforts of Antti Palosaari, Eric Fry, and Osmocom (in particular Steve Markgraf) it was found that the raw IQ data on the RTL2832U chipset could be accessed directly, which allowed the DVB-T TV tuner to be converted into a wideband software defined radio via a custom software driver developed by Steve Markgraf [59]. The specifications for this model are shown in Table 2.5.

Table 2.5: Specifications for RTL-SDR [59]

Specification	Value
Frequency Range	24MHz to 1.766MHz (approx.)
ADC Resolution	8 bits
Maximum Sample Rate	Up to 3.2 MS/s (model-dependent)
Supported Software	Various SDR applications
Antenna Connector	MCX or SMA (model-dependent)
Power Supply	USB-powered (5V)
Compatibility	Windows, Linux, macOS
Cost	Affordable, typically under $30

f. HackRF One Figure 2.6d shows HackRF One. It is a wide band SDR half-duplex transceiver created and manufactured by Great Scott Gadgets. It can send and receive signals. Its principal designer, Michael Ossmann, launched a successful Kickstarter campaign in 2014 with a first run of the project called HackRF. The hardware and software's open-source nature has attracted hackers, amateur radio enthusiasts, and information security practitioners [22]. The specifications for this model are shown in Table 2.6.

Table 2.6: Specifications for HackRF One [22]

Specification	Value
Frequency Range	1MHz to 6MHz
ADC Resolution	8 bits
Maximum Sample Rate	Up to 20 MS/s (model-dependent)
Supported Software	Various SDR applications
Antenna Connector	SMA (female)
Transmit Power	Approximately 10 mW to 100 mW (model-dependent)
Power Supply	USB-powered (5V)
Compatibility	Windows, Linux, macOS
Cost	Typically around 300 to 350 (may vary)

2.2 Spectrum Scanning System

In the field of remote sensing, various research is being conducted to find soil moisture and soil electrical conductivity for precision irrigation and precision agriculture by using microwave signals. With the advancement in wireless communication and the popularity of designing more wireless devices, it's hard to do active sensing because of the spectrum scarcity. The workaround in agriculture for this problem is passive sensing, meaning using the already available spectrums a.k.a. signals-of-opportunity to collect the reflected signals from the field to find the correlation between the received power and soil moisture and soil electrical conductivity. Some examples of signals of opportunity and their utilized frequencies are shown in Table 2.7. The goal of spectrum sensing is not only passive sensing. Accurate spectrum sensing will lead to other applications like spectrum sharing, interference detection, and co-existence between communication and radar systems.

Table 2.7: Signals of Opportunity Examples [18]

Satellite Name	Frequency	Orbit
ORBCOMM	137-137MHz	Low Earth Orbit (LEO)
Ultra High Frequency (UHF) Follow-On (UFO)	240-270MHz	Geostationary Orbit (GEO)
Multi-User Objective System (MUOS)	360-380MHz	GEO
Global Navigation Satellite System (GNSS) L5	1164-1214MHz	Medium Earth Orbit (MEO)
GNSS L1	1559-1610MHz	MEO
Sirius Satellite Radio (XM) Radio	2322.5-2345MHz	GEO
DirecTV (Ku)	12.2-12.7MHz	GEO
DirecTV (K)	18.3-18.8MHz	GEO

2.3 Contraband Cellphone Detection in Prison

The widespread use of contraband wireless devices, especially cellphones, being smuggled into correctional facilities is a significant issue nationwide. Inmates in these facilities employ these devices to coordinate gang activities, run drug operations, and even plan escapes, all of which pose potential threats to the safety and well-being of other inmates, prison staff, and the general public. Instead of physically searching for unauthorized cellphones, this paper focuses on developing a passive localization system that can identify all potential unauthorized devices using RF location fingerprinting algorithms.

Wi-Fi-based indoor localization holds significant potential in various industries over time [60]. However, achieving precise device localization in indoor environments poses unique challenges compared to outdoor positioning [66]. Indoors, the signal can be subject to fluctuations, blockages, attenuation, noise interference, and multipath propagation. Furthermore, factors like temperature variations, the presence of physical objects, or moving objects can introduce signal interference [66]. This necessitates strong signal coverage and offline processing, which the Global Positioning System (GPS) may not provide indoors.

Recently, Wi-Fi fingerprinting has gained popularity for indoor localization due to its high accuracy [61]. Wi-Fi fingerprinting involves capturing the unique RF signals transmitted by wireless devices such as mobile phones, tablets, and laptops [5]. These Wi-Fi fingerprints encompass various components, including IQ samples, CSI, and Received Signal Strength Indicator (RSSI) data. Many state-of-the-art methods have demonstrated strong localization accuracy using IQ, CSI, and RSSI information [87].

DoA is another crucial element used for indoor localization nowadays. DoA refers to the direction in which a wave typically travels to reach a specific destination [98], which could be the location of a particular device or sensor. Several methods, such as the periodogram [38], MUSIC (Multiple Signal Classification) [74], and Estimation of Signal Parameters via Rotational Invariant Techniques (ESPRIT) algorithm [27], are employed to estimate DoA. Additionally, other techniques like Angle of Arrival (AoA), Time Difference of Arrival (TDOA), Frequency Difference of Arrival (FDOA), and related methods can be employed to determine DoA. Signal DoA is favored for indoor localization not only for its accuracy but also for its computational efficiency. An advantage of DoA is that it doesn't require synchronization between receivers to determine the location [45].

Various alternative sensing technologies, such as LIDAR, Infrared, Inertial Measurement Units (IMU), and camera image-based visual localization, can also be used for indoor positioning [45]. However, these technologies often necessitate specific environmental conditions, like good lighting and flat surfaces. In contrast, SDRs offer a cost-effective solution without these additional constraints [45].

Training a network with data from every point in a room may not be practical, and this research explores the classifier's performance when trained on specific points and tested on different ones.

In this research, raw IQ samples and signal DoA are employed for room-level indoor localization. A custom MLP neural network is utilized for room-level classification. The study investigates room-level localization using data collected from six locations using a four-antenna X300 SDR and two cellphones. This study extends a previous one [30] that focused solely on IQ samples converted to Short-Time Fourier Transform (STFT). It addresses the issue of imbalanced data in

the dataset. The motivation behind this research is the ongoing problem of unlicensed cellphones in prisons, with the goal of assisting security staff in locating such devices in rooms or hallways. Furthermore, the study evaluates the classifier's performance in identifying unknown locations.

2.3.1 Device Fingerprinting

Wireless devices are equipped with unique digital identifiers known as Media Access Control (MAC) addresses, which facilitate communication with wireless networks. However, networks relying solely on MAC addresses are susceptible to unauthorized access, as malicious actors can intercept and mimic legitimate device MAC addresses. This can compromise network security and privacy [70] [69][31].

To address these concerns, recent protocols have introduced MAC address randomization for user privacy. This technology allows devices like iPhones to change their MAC addresses frequently, making it difficult to track user activity across different networks. Consequently, solely relying on a fixed set of allowed MAC addresses is not a viable access control strategy, as even legitimate devices may change their MAC addresses for privacy reasons.

However, each wireless device possesses a unique 'physical fingerprint' that is independent of its digital MAC address. This physical fingerprint is generated by variations in the manufacturing process of the device's hardware components. These variations result in distinct signal characteristics, making it possible to uniquely identify each device. This approach is not affected by MAC address randomization and offers a more reliable means of device identification.

2.3.2 Location Fingerprinting

The STFT is a signal processing technique that can be employed to analyze wireless signals. It involves applying the FFT to different segments of a signal and by applying a window function, enabling the capture of changes in the frequency domain over time. In the frequency domain, variations in the physical fingerprint of each device may be more noticeable, as hardware-related differences can manifest as perturbations in the signal's frequency representation over time [70] [69][31].

RF location fingerprinting explores the idea that the wireless signals received from a device carry unique characteristics related to their transmission paths, known as location fingerprints. In the existing literature, both CSI and RSSI have commonly been used for indoor device localization with strong performance. Our proposed system utilizes cost-effective SDRs capable of capturing raw IQ signals. Unlike previous work, we investigate the use of raw IQ signals, CSI, RSSI, and combinations thereof for device localization. Notably, driven by the recent success of deep learning in various challenging applications, this research work suggests using a Deep Neural Network (DNN) to extract high-level features from the raw signals.

2.4 HAR using Wi-Fi

Wi-Fi-based HAR techniques, as the name suggests, use Wi-Fi signals to detect and recognize human activities. This topic is an emerging research area that has gained significant attention in recent years. This technique is convenient, non-intrusive, and low-cost and utilizes the already existing Wi-Fi signal. In this approach, Wi-Fi-enabled devices such as smartphones, laptops, or access points can be used to monitor and analyze Wi-Fi signals to recognize human activities which can be further used for various applications described in the motivation in section 2.4.5.

2.4.1 Wi-Fi Technology and Its Capabilities

There are various versions of Wi-Fi technologies. Some of the popular ones are 802.11a, 802.11n, 802.11ac, and 802.11ax. They operate mainly on 2.4GHz, 5GHz, or both and have different bandwidths as shown in Table 2.8. For example, 802.11a operates on 5.8GHz and has a max bandwidth of 54MHz [51], and 802.11n has a bandwidth up to 160MHz. To transmit a bitstream through Wi-Fi, Orthogonal Frequency Division Multiplex (OFDM) signals are used. 802.11a OFDM signal generation process is shown in Figure 2.7. OFDM signal format is shown in Figure 2.8. On the x-axis is the frequency domain where a constellation point is matched to one FFT bin whereas on the y-axis is the time domain where the OFDM symbols are separated by guard intervals to prevent inter-symbol interference.

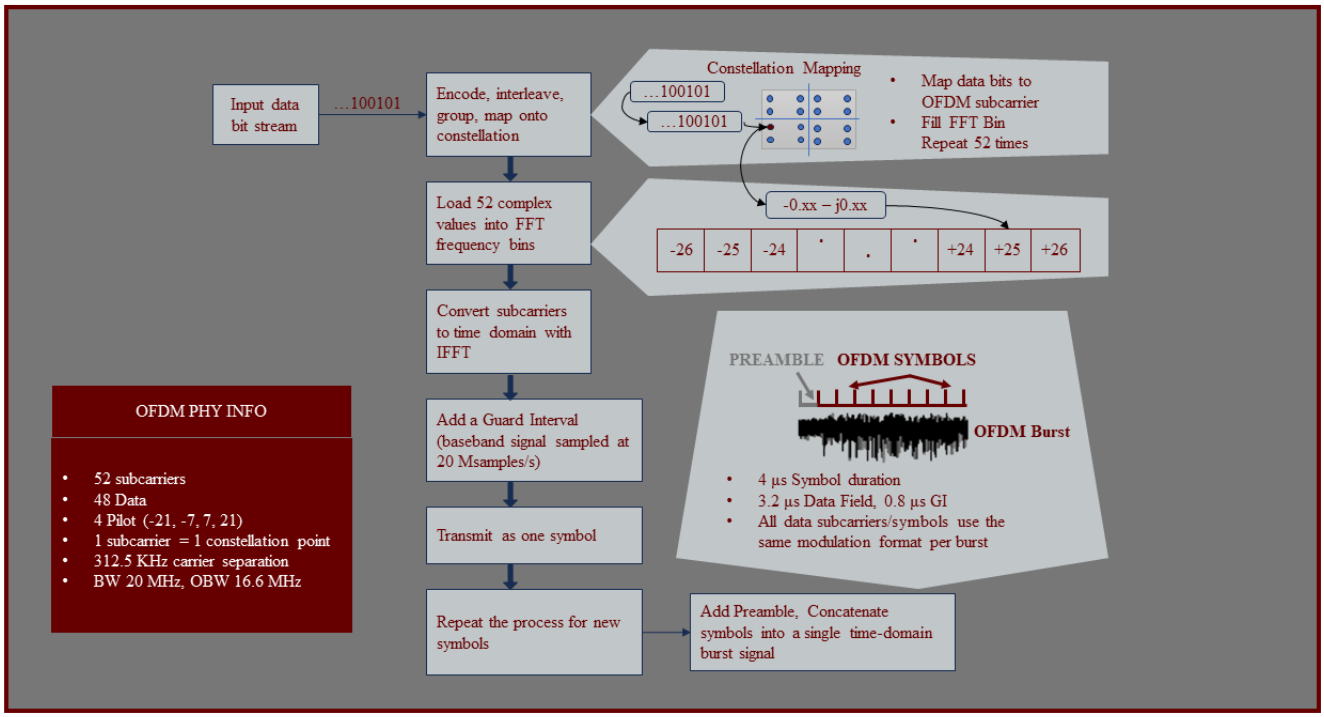


Figure 2.7: 802.11a OFDM signal generation process [34]

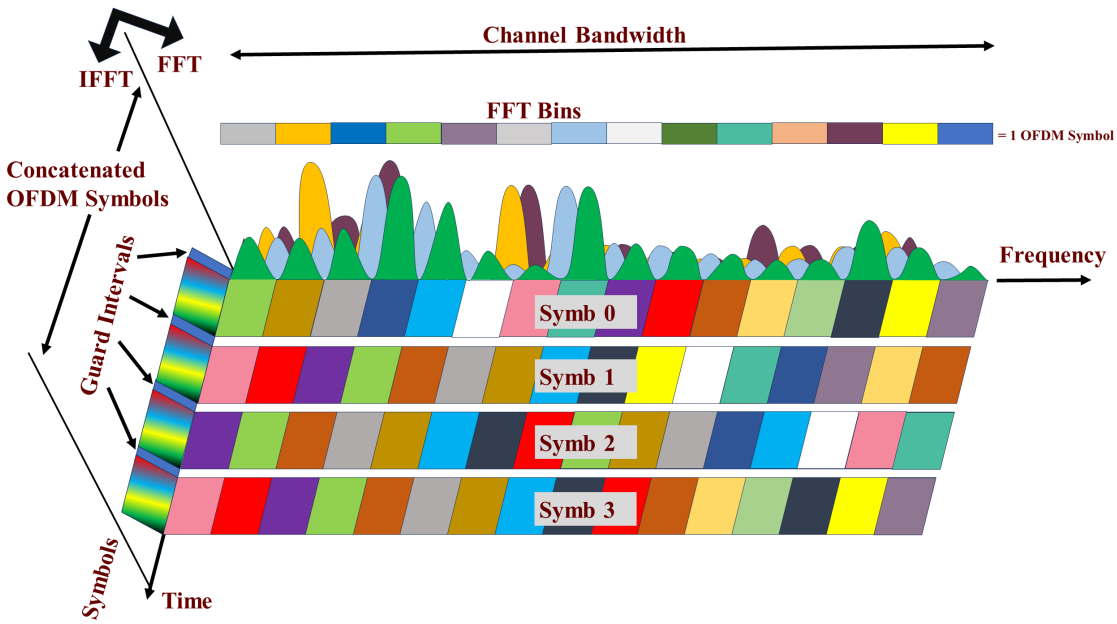


Figure 2.8: Frequency-Time representative of OFDM signal [78]

Table 2.8: Wi-Fi Standard Specifications [2, 7]

Wi-Fi Standard	Frequency Band	Maximum Data Rate	Supported Bandwidth	Number of Subcarriers	Subcarrier Spacing (KHz)	Symbol Duration (µs)	Cyclic Prefix Length (samples)
802.11b	2.4GHz	11 Mbps	20 MHz	64	312.5	3.2	1/4
802.11g	2.4GHz	54 Mbps	20 MHz	64	312.5	3.2	1/4
802.11n	2.4GHz/5GHz	600 Mbps	20 MHz	64	312.5	3.2	1/4
802.11n	2.4GHz/5GHz	600 Mbps	40 MHz	128	156.25	3.2	1/4
802.11ac	5GHz	1 Gbps	20 MHz	64	312.5	3.2	1/4
802.11ac	5GHz	1 Gbps	40 MHz	128	156.25	3.2	1/4
802.11ac	5GHz	1 Gbps	80 MHz	256	78.125	4	1/32
802.11ac	5GHz	1 Gbps	160 MHz	512	39.0625	4	1/32
802.11ax	2.4GHz/5GHz	9.6 Gbps	20 MHz	64	312.5	3.2	1/4
802.11ax	2.4GHz/5GHz	9.6 Gbps	40 MHz	128	156.25	3.2	1/4
802.11ax	2.4GHz/5GHz	9.6 Gbps	80 MHz	256	78.125	4	1/32
802.11ax	2.4GHz/5GHz	9.6 Gbps	160 MHz	512	39.0625	4	1/32
802.11ax	2.4GHz/5GHz	9.6 Gbps	80+80 MHz	512+512	39.0625	4	1/32

This involves converting the bitstream from serial to parallel using a converter for modulation. The resulting modulation is then transformed into a time domain signal through the use of Inverse Fast Fourier Transform (IFFT). An OFDM symbol consists of equally spaced subcarriers that contain those earlier generated parallel data. This process is shown in Figure 2.9.

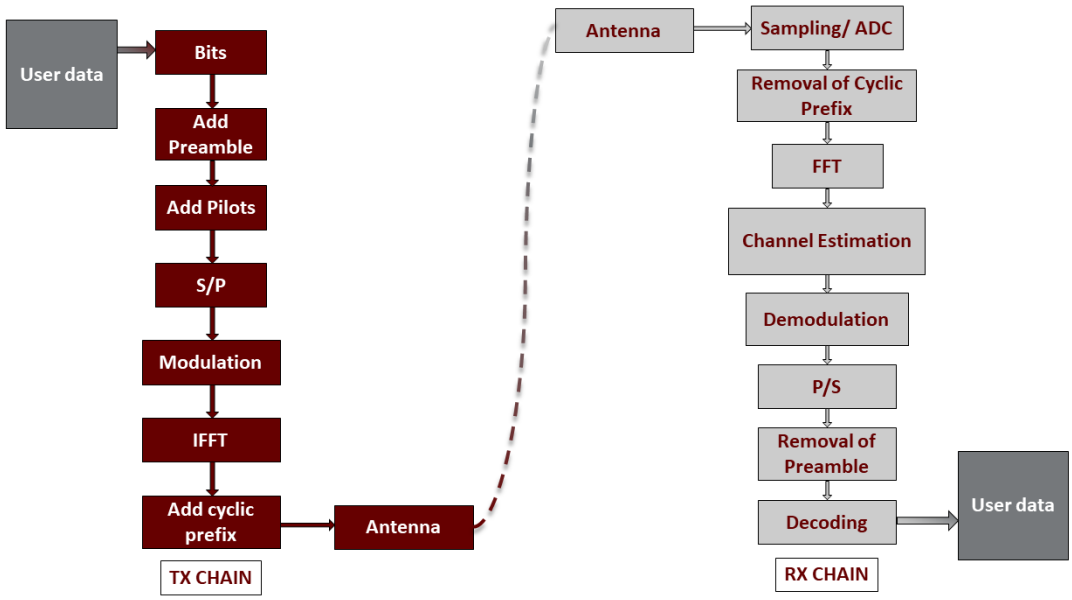


Figure 2.9: Data Transmission overview in Wi-Fi [78]

Looking in detail at an example of Wi-Fi protocol, 802.11n with 40MHz bandwidth has 128 subcarriers each spaced at 156.25KHz. Among those 128, 108 are used for user data transmission whereas others are used as pilot or null tones which act as a reference signal that helps to demodulate the data accurately. These tones are typically a sine wave with a fixed frequency and amplitude. The null tones are there to reduce the interference between the adjacent subcarrier by creating a guard band that separates them. To understand how Wi-Fi can be used in human activity recognition, let's take a look at the key ingredients of Wi-Fi based HAR.

2.4.2 Doppler Shift

The Doppler effect is the change in frequency or wavelength of a wave in relation to an observer who is moving relative to the wave source. The Doppler effect causes a shift in the frequency of the waves which can be detected by measuring the change in wavelength or frequency of the wave. The Doppler shift is given by the equation:

$$f' = f(1 \pm \frac{v}{c}) \tag{2.1}$$

where f is the frequency of the wave in Hz, v is the relative velocity of the source and observer in meters, c is the speed of the wave and $\pm$ is when the source is moving towards or away from the observer.

In terms of human activity in the presence of Wi-Fi, the signals can be affected by the motion due to any activity. When a person moves, the movement causes the body to reflect and scatter Wi-Fi signals, causing a slight change in the frequency of the signal, hence resulting in a Doppler shift. In other words, what exactly happens is when someone moves, the signal reflected from them contains a Doppler shift in the original signal which can be observed in the CSI.

2.4.3 Modeling Wi-Fi Signal for HAR

Human activity recognition using Wi-Fi involves detecting and classifying the physical activities of people based on Wi-Fi signals. This can be done by analyzing the signals emitted by Wi-Fi devices, such as smartphones, laptops, and other wireless-enabled devices, and using machine learning algorithms to identify patterns that are characteristic of different types of human activities. So, that information is used to train a machine learning model to classify different types of activities. CSI provides a more complete picture of the channel state, including both

the frequency and phase response, and often includes information about the channel's gain, delay, and Doppler shift. CSI is used for various purposes in wireless communication systems, such as adaptive modulation and coding, beamforming, and rate adaptation. CSI is represented in the form of a complex-valued matrix, with one matrix element corresponding to each subcarrier in the Wi-Fi signals.

So, how does this CSI look in terms of data? As mentioned earlier in section 2.4.1, Wi-Fi uses OFDM in which the bandwidth is divided equally into subcarriers. Each subcarrier contains either user data or pilot (for phase synchronization) or null tone (reference signal). In a hardware configuration with t number of transmit antennas and r number of receiving antennas, the data looks as follows:

$$CSI_i = \begin{vmatrix} H_{1,1} & \dots & H_{1,r} \\ H_{2,1} & \dots & H_{2,r} \\ . & & . \\ . & & . \\ . & & . \\ H_{t,1} & \dots & H_{t,r} \end{vmatrix} \tag{2.2}$$

where $H_{t,r}$ represents a vector containing complex pairs captured for each subcarrier. The number of subcarriers depends on the hardware configuration as well as the bandwidth of the Wi-Fi protocol as mentioned in Chapter I. The CSI complex pair contains amplitude and phase information that is affected due to multi-path propagation due to:

- Reflection - Change in the phase of the signal bouncing of the signal.
- Scattering - Change in signal shape.

- Attenuation - Degradation in amplitude.
- Superposition - Received direct + indirect paths.

When a human performs an activity (motion), the multipath effect is not the same compared to the reflection from the static objects. Here Doppler shift can be observed when a spectrogram is plotted from the CSI as shown in Figure 2.10.

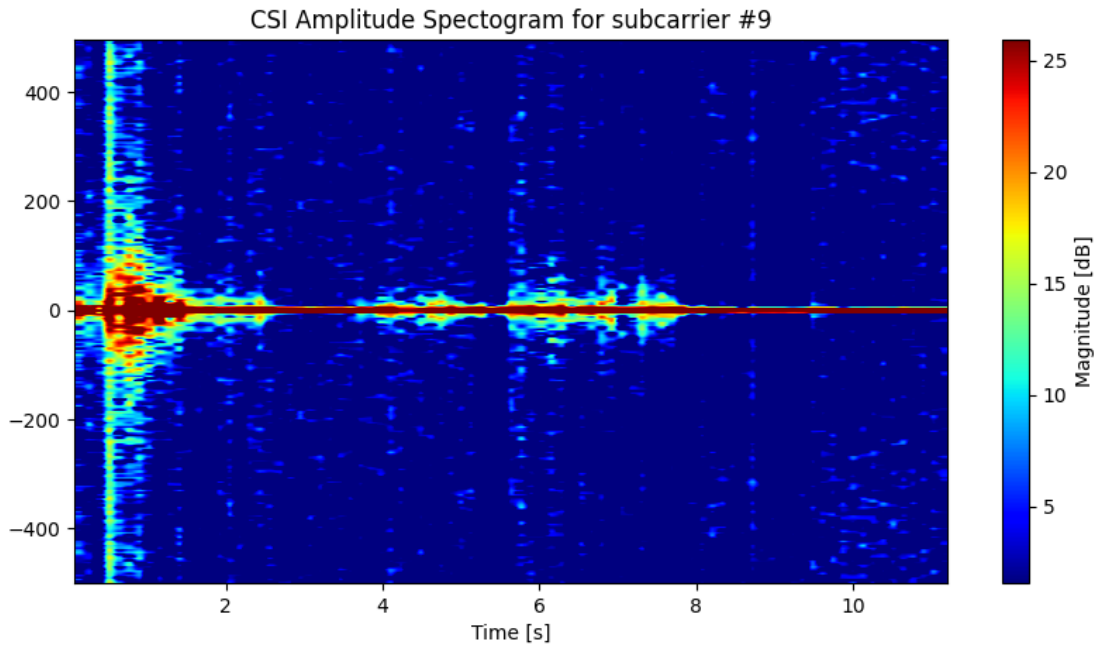


Figure 2.10: Spectrogram of CSI Amplitude. Y-Axis is the FFT point. The figure contains activity between 0 and 2 seconds, and the activity resumes from 4 to 8 seconds with a slight gap before the 5^{th} second. This CSI data was collected using Nexmon Firmware flashed on a Raspberry Pi 3B+.

2.4.4 Amplitude and Phase

Figure 2.11 compares amplitude vs phase spectrogram plot generated for the same subcarrier index for the data collected from the same antenna for the same OFDM symbol. The plot is generated using a publicly available dataset from [93].

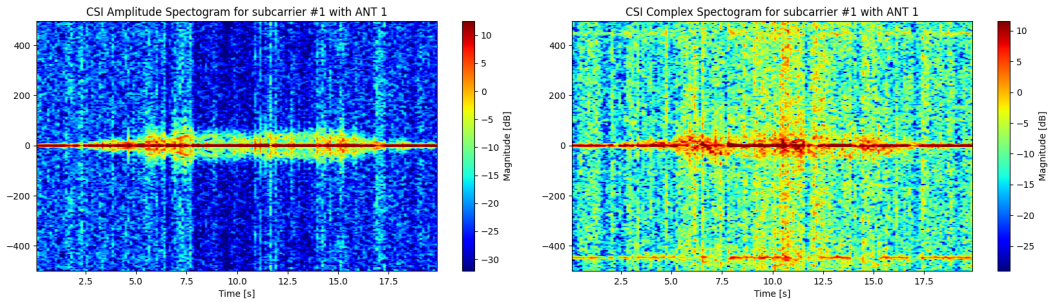


Figure 2.11: Spectogram of CSI Amplitude on the left vs Phase on the right

Before moving forward with the details of motivation and methods, first, it is important to know what it means to recognize human activity using Wi-Fi. More importantly, it is necessary to know what kinds of activities are easy to recognize compared to others. Among the popular research performed so far, various human activities have been classified accurately. Figure 2.12 shows the various spectrogram plots of some of the activities that were classified at Mississippi State University.

2.4.5 Motivation and Practical Applications

Several potential use cases of Wi-Fi-based HAR are provided below.

- Health and Wellness Monitoring – Nursing Home Fall Injury: Gesture recognition helps to detect and prevent fall injuries. According to [16], there were 101,433 falls reported in Nursing homes in 2022. Among those falls, 208 residents died due to insufficient help. This will help to detect residents' movements in real-time and can alert the home staff if they

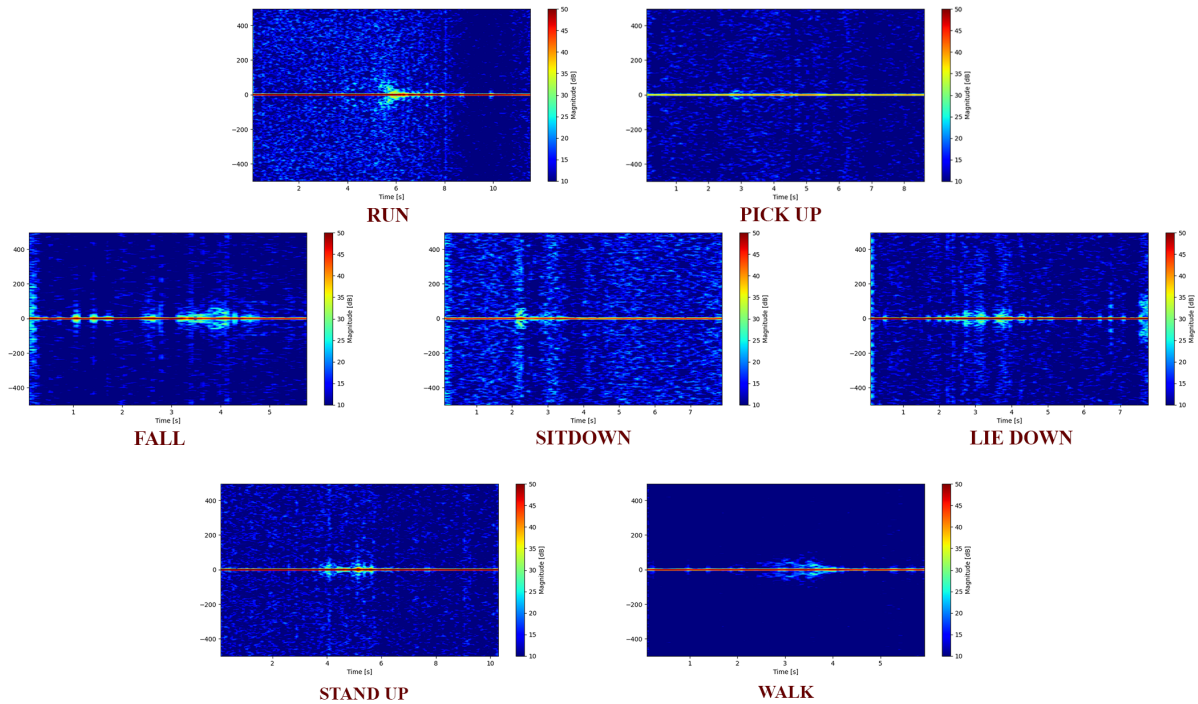


Figure 2.12: Spectrogram of 7 activities generated using Wi-Fi CSI data

detect a fall. This will help the staff to intervene quickly and even prevent falls before they occur.

- Smart Home -Gesture Control for Home Devices: According to [1], the prior methods use some hardware sensor to detect the gesture. Using already existing Wi-Fi removes the need to acquire additional sensors. With gesture control, homeowners can control their electrical appliances without having to physically interact with the said devices. Examples of some of the popular of gesture control applications are turning on and off lights, television, adjusting the temperature, adjusting the volume of the television, sound system, and home security system with a simple gesture such as a wave of a hand. This is getting popular, especially with the Gen Zs who are always busy and are tech-savvy simply because this technology takes away the need to fumble a phone or remote to control these devices. Another major benefit of implementing this technology is that now users don't have to keep looking for the lost remote for hours or even days to gain control of their television instead they can simply wave their hand to change the channel or adjust the volume.

- Commercial and Industrial Applications of Wi-Fi-based HAR: This technology can be used to enhance the business environment as well. For example, retail stores can use Wi-Fi-based gesture recognition to understand customer behavior and optimize store layout. This can be used to analyze foot traffic and customer movement patterns and organize the products accordingly and plan for improvement. Similarly, hotels can use this system to improve the

guest experience by monitoring movements and preferences. Furthermore, in manufacturing environments, this technology can be used to track employee movements and optimize production processes. Floor managers can be benefited from the help of this system to implement the changes which can streamline processes and increase efficiency.

- Augmented Reality (AR)/Virtual Reality (VR) Gaming : Similar to the application to control the home devices for a smart home, additional hardware is needed for gaming. Utilizing the already existing Wi-Fi receivers in the gaming console can remove the need to acquire additional hardware. One way to make the game more interesting is by making it more interactive. Using gesture control makes the player use their hand and body movement instead of relying on traditional controllers or mouse/keyboards. While using natural hand and body movement, the player interacts with the virtual environment which gives a feeling of immersion into the game and leads to a sense of presence inside the game. In addition to that, this allows for more precise and natural movement inside the game which makes the gaming experience more realistic.

- Privacy: Using Wi-Fi to detect the gesture does not require any camera or visual sensors that need to be installed in the home or any other environment where it is being used. This is especially appealing to people who are concerned about their privacy and do not want to be recorded on camera. In addition to that, using Wi-Fi means using radio waves instead of other forms of biometric data which prevents the leakage of personally identifiable information. This technology operates locally and does not use the content of the signal just the channel state information to detect gestures.

CHAPTER III

METHODOLOGY

3.1 Background

The methodology chapter section outlines the testbed and research methods applied in three distinct applications: Spectrum scanning system, Contraband cellphone detection in prison, and Human activity recognition. A specialized testbed was established for the Spectrum scanning system investigation, comprising a wide range of RF equipment and antennas for capturing and analyzing radio frequency signals across a diverse spectrum. Custom software was developed for real-time signal processing and data collection, and various scanning algorithms were employed for signal identification and classification.

In the contraband cellphone detection system in prison, a controlled environment was set up within the Department of Electrical and Computer Engineering at Mississippi State University to assess the effectiveness of different detection technologies. These included location fingerprinting, device fingerprinting, and behavioral pattern analysis. Extensive simulations were carried out to compare with the real-world performance of these methods.

Separate testbeds were designed to study human activity recognition, incorporating Wi-Fi signals to capture data relating to human movements and activities. Machine learning algorithms were applied for data processing and classification, resulting in the development of robust models for recognizing and categorizing different human activities. Moreover, user studies were conducted

to validate the accuracy and reliability of the developed recognition system. A comparison test was performed with Radar which is discussed in section 3.4.6.

3.2 Spectrum Scanning System

The following sections explain the methodology used for the Spectrum scanning system application in detail.

3.2.1 Purpose and Research Objectives

The primary aim of the Spectrum scanning system research is to identify and characterize unoccupied frequency spectrums within the range of 100MHz to 3GHz. This system serves the comprehensive goal of enabling passive microwave remote sensing by repurposing underutilized spectrum resources. Specifically, this research seeks to address the challenges of spectrum congestion and efficient spectrum allocation in the context of passive remote sensing applications.

3.2.2 Equipment and Testbed Setup

To achieve this objective, a specialized testbed was constructed, consisting of key hardware components. These include the B210 NI SDR, an Intel Next Unit of Computing (NUC) for data processing and storage, and a wideband antenna designed to cover the desired frequency range. The B210 SDR and antenna serve as the primary RF signal reception and capture components, while the Intel NUC facilitates real-time data processing and storage.

3.2.2.1 Architectural Design: Hardware

Hardware designing started with component selection. NI B210 SDR was selected for this project due to its portability and compactness. Configuring the B210 to construct a spectrum

scanning system is a meticulous yet highly versatile endeavor. With a frequency range spanning from 100MHz to 3GHz, the B210 offers the capability to scan a wide spectrum for signals. To begin, the system is programmed to initiate the scan in 50MHz bandwidth increments, meticulously sweeping through the specified spectrum. At each interval, FFT is applied to the acquired data block, allowing for a detailed analysis of the frequency components present. These FFT results are then systematically appended, creating a comprehensive wide-band frequency plot that visually illustrates which segments of the spectrum are occupied.

The Intel NUC, short for "Next Unit of Computing", is used as a processing Personal Computer (PC). It is a compact and highly versatile mini-computer that packs a powerful punch despite its diminutive size. These small-form-factor devices are designed by Intel to offer remarkable computing performance in a space-efficient package, typically measuring just a few inches in each dimension. NUCs come in various configurations, catering to a wide range of needs, from basic computing tasks to high-performance applications like gaming and content creation. Equipped with Intel processors, integrated graphics, and customizable storage and memory options, NUCs are capable of handling diverse computing tasks while being easy to transport or mount behind a monitor, making them an excellent choice for home entertainment centers, small office setups, or as the foundation for specialized projects like this one.

Finally, a Wide-band Frequency Antenna is selected that can operate in the target frequency. The Proxicast Fourth Generation (of cellular network technology) (4G)/Fifth Generation (of cellular network technology) (5G)/Citizens Broadband Radio Service (CBRS) Universal Wide-Band 6dBi Omni-Directional Swivel Terminal Antenna, known as the ANT-120-008, is an essential component for spectrum scanning systems. This antenna boasts exceptional compatibility with

leading networking equipment brands. What sets the ANT-120-008 apart is its wide-band design, allowing it to cover a broad spectrum of frequencies as specification shown in Table 3.1. In the context of spectrum scanning, this feature is paramount. Spectrum scanning systems need to sweep through a wide range of frequencies to identify occupied or available spectrum bands accurately. This antenna's ability to handle various frequencies ensures that the scanning system can effectively monitor and analyze diverse frequency ranges, making it indispensable for researchers and professionals in fields like wireless communications and radio frequency research. Its omnidirectional characteristics are also valuable, as it can capture signals from all directions, making it an ideal choice for systems where signal sources may vary in direction, delivering comprehensive insights into spectrum occupancy. In the context of spectrum scanning, the ANT-120-008's wide-band and omnidirectional capabilities significantly enhance the effectiveness and reliability of the scanning process.

Table 3.1: ANT-120-008 Technical Specifications [56]

Feature	Specification
Model	ANT-120-008
Type	Omni-directional swivel terminal antenna
Gain	6 dBi
Frequency coverage	600 - 6000 MHz
Connector type	SMA male
Dimensions	8.7 inches tall
Weight	0.15 lbs
Compatibility	All 4G/LTE, 5G, FirstNet, and OnGo (CBRS)

Figure 3.1: Spectrum scanning testbed

3.2.2.2 Architectural Design: Software

In the development of software designed for spectrum scanning, the seamless integration of three pivotal technologies—Qt [8], Python [17], and USRP Hardware Driver (UHD) [58]—plays a central role. These components collectively contribute to the creation of a versatile and user-friendly application tailored for the analysis of the spectrum.

Qt, a robust cross-platform framework based on C++, assumes a crucial role in shaping the Graphical User Interface (GUI) of the spectrum scanning software. The extensive Qt library empowers the design of visually appealing and highly functional interfaces, amenable to execution across various operating systems. For proponents of the Python programming language, it is worth noting that Qt offers Python bindings, rendering GUI development accessible and efficient.

Python, renowned for its versatility and readability, assumes a central role in orchestrating intricate signal-processing tasks within the software. Python's simplicity, combined with its extensive ecosystem, packed with libraries such as NumPy and SciPy for scientific computation, renders it a superlative choice for signal analysis. When conjoined with Qt, Python facilitates the creation of interactive and user-friendly GUIs, enabling users to exert control over the spectrum scanning process, thereby enhancing the overall user experience.

UHD serves as an indispensable conduit linking the software to the underlying SDR hardware. This open-source driver framework abstracts the lower-level hardware interactions, simplifying the interface for a diverse array of SDR devices, including USRP. Leveraging UHD within the software standardizes the hardware interface across varying platforms, ensuring compatibility and streamlining the interaction with and management of the hardware.

Collectively, these three constituent elements — Qt for GUI development, Python for signal processing and control, and UHD for hardware interoperability— effectively merge to produce a potent toolkit for the construction of a spectrum scanning application. This software not only undertakes signal processing and analysis but also provides an intuitive and user-friendly interface, thus rendering it a vital asset for spectrum analysis and investigation.

3.2.3 Data Collection and Processing

Data collection was executed by scanning the frequency spectrum from 100MHz to 3GHz with a 50MHz increment. This systematic approach allowed for comprehensive coverage and analysis of the entire frequency band of interest. For each bandwidth, FFT was applied to captured signals, generating valuable frequency domain data. These FFT results were then appended to construct

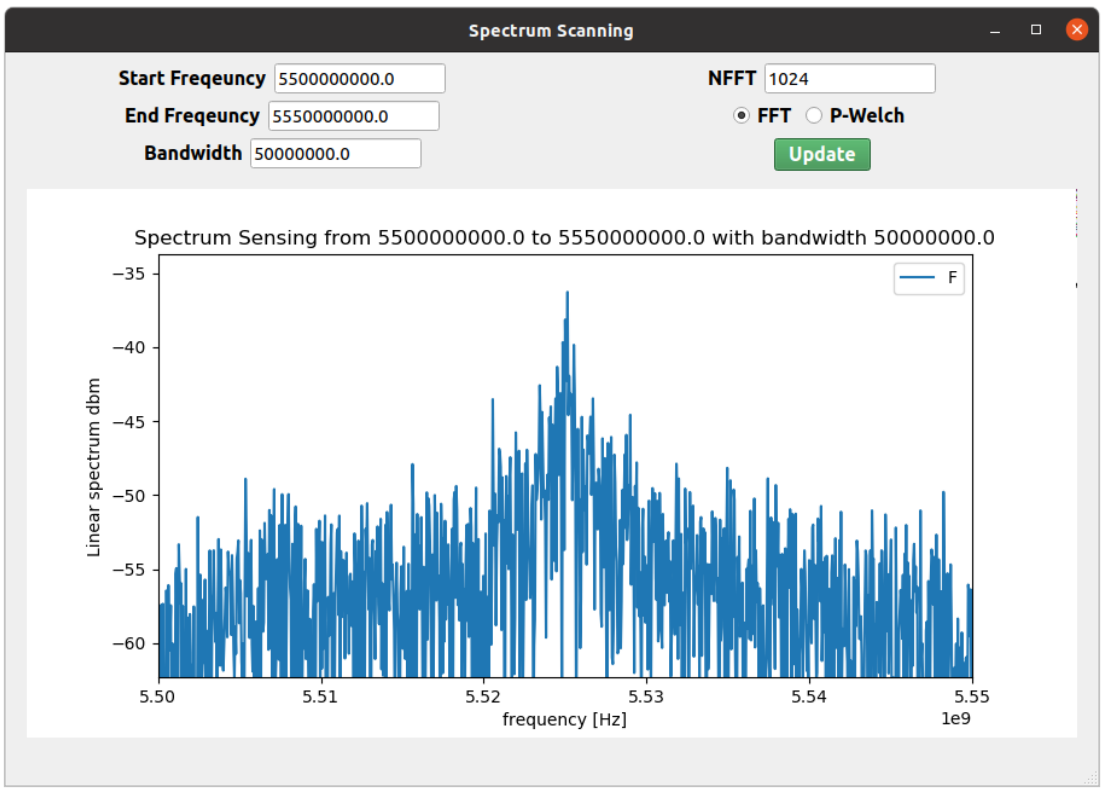


Figure 3.2: User interface created using QT that is capable of reprogramming the SDR to change the spectrum range

a coherent dataset. Subsequently, a user-friendly GUI was developed using QT to visualize and interact with the collected FFT data.

3.2.4 Signal Analysis and Classification

Signal analysis was performed through the utilization of FFT, and STFT. In addition, the Cyclostationary method, Matched filter, and Energy detection method were also looked into which are described later in the future work section 5.2. These algorithms facilitate the identification and categorization of signals within the spectrum, enabling the distinction between occupied and unoccupied frequency bands. The classification process involved the detection of distinct spectral signatures, power levels, and patterns, contributing to the precise characterization of the spectrum.

This methodology laid the foundation for our Spectrum scanning system, allowing for the systematic identification of unoccupied spectrum bands, which can be harnessed to advance passive microwave remote sensing applications.

3.3 Contraband Cellphone Detection

The following sections explain the methodology used for the Contraband cellphone detection application in detail.

3.3.1 Purpose and Research Objectives

The primary aim of a Contraband Cellphone Detection System is to create a robust system for finding and pinpointing illegal cellphones within any unwanted environment. This research is fueled by the pressing need to enhance security within correctional facilities and put an end to illicit communications as described in chapter II.

3.3.2 Equipment and Testbed Setup

For this research, we set up a specialized testbed with specific hardware components. This included the B210 NI SDR, X310s with TwinRX daughterboards, antennas, and a high-powered PC for data processing. These elements formed the core of our contraband cellphone detection system. Figure 3.3 shows the system diagram of the testbed setup.

3.3.3 Data Collection and Processing

To achieve cellphone detection and localization, we used GNURadio (Figure 3.6 explained in section 3.3.3.1) to design a structured data processing pipeline. The process kicked off by analyzing complex samples received by the SDR through a normalized autocorrelation. This helped us spot the Short Training Field (STF) associated with IEEE802.11g based on its repeating pattern.

The Sync Short block was responsible for comparing the autocorrelation results against a user-defined threshold and triggering when the threshold was met. Subsequently, we passed the

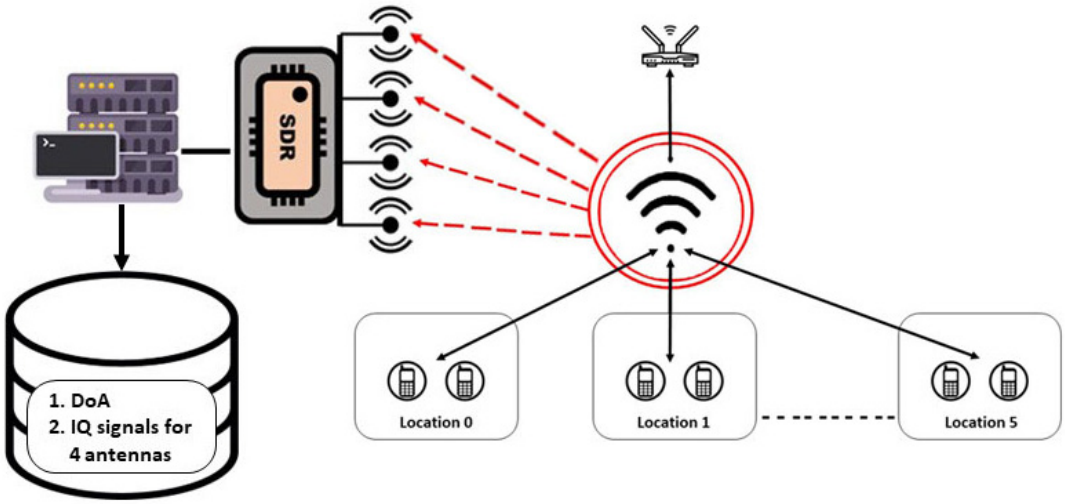


Figure 3.3: System Diagram

next 43,200 samples or 540 symbols, which approximated the size of an IEEE802.11g frame, to the next block after correcting for coarse frequency. The Sync Long block was used to find the start of the frame through cross-correlation with the known sequence for the STF. An example of 802.11g Wi-Fi frame is shown in Figure 3.5. Fine-tuning the frequency and removing the cyclic prefix came next before the signal was subjected to FFT. The FFT used an input size of 64 with a rectangular window. Subcarriers from the FFT's output were directed to the Frame Equalization block. Here, subcarriers were mapped back to their original constellation points, and CSI was calculated using the Space-Time Algorithm (STA). Figure 3.7 shows the data collection setup at MSU.

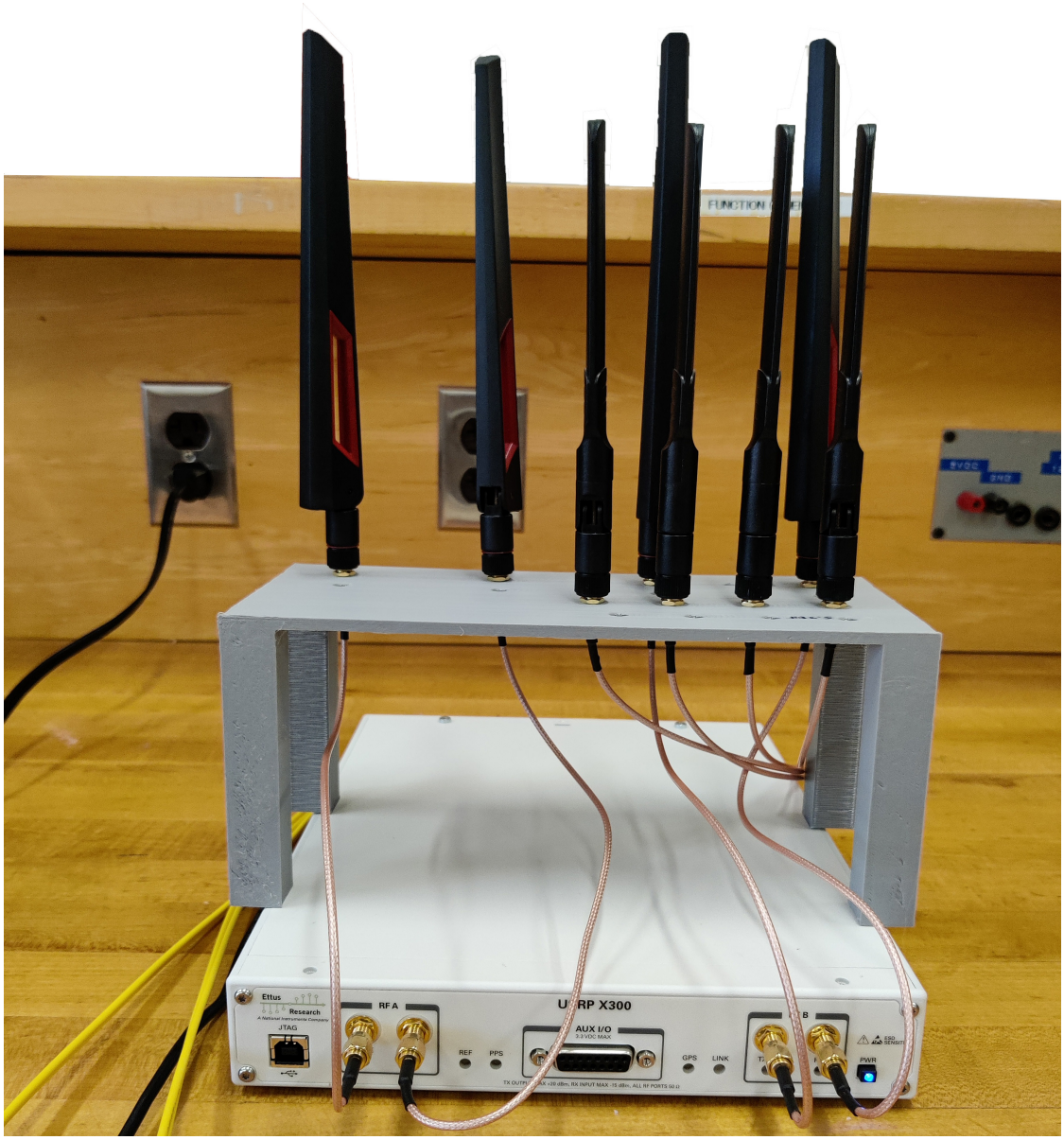


Figure 3.4: SDR setup with four antennas to collect angle of arrival

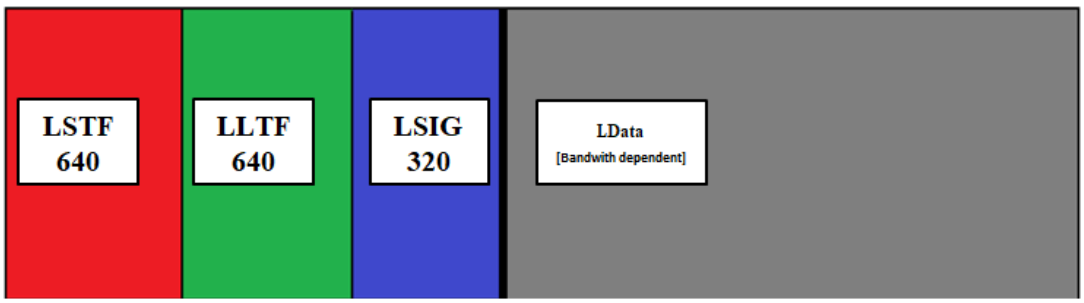


Figure 3.5: 802.11g Wi-Fi frame. LSTF = Legacy Short Training Field 2 OFDM symbols long, LSIG = Legacy Signal 1 OFDM symbols long, LLTF = Legacy Long Training Field 2 OFDM symbols long, LData = Legacy Data. 1 OFDM = 320 IQ samples [49]

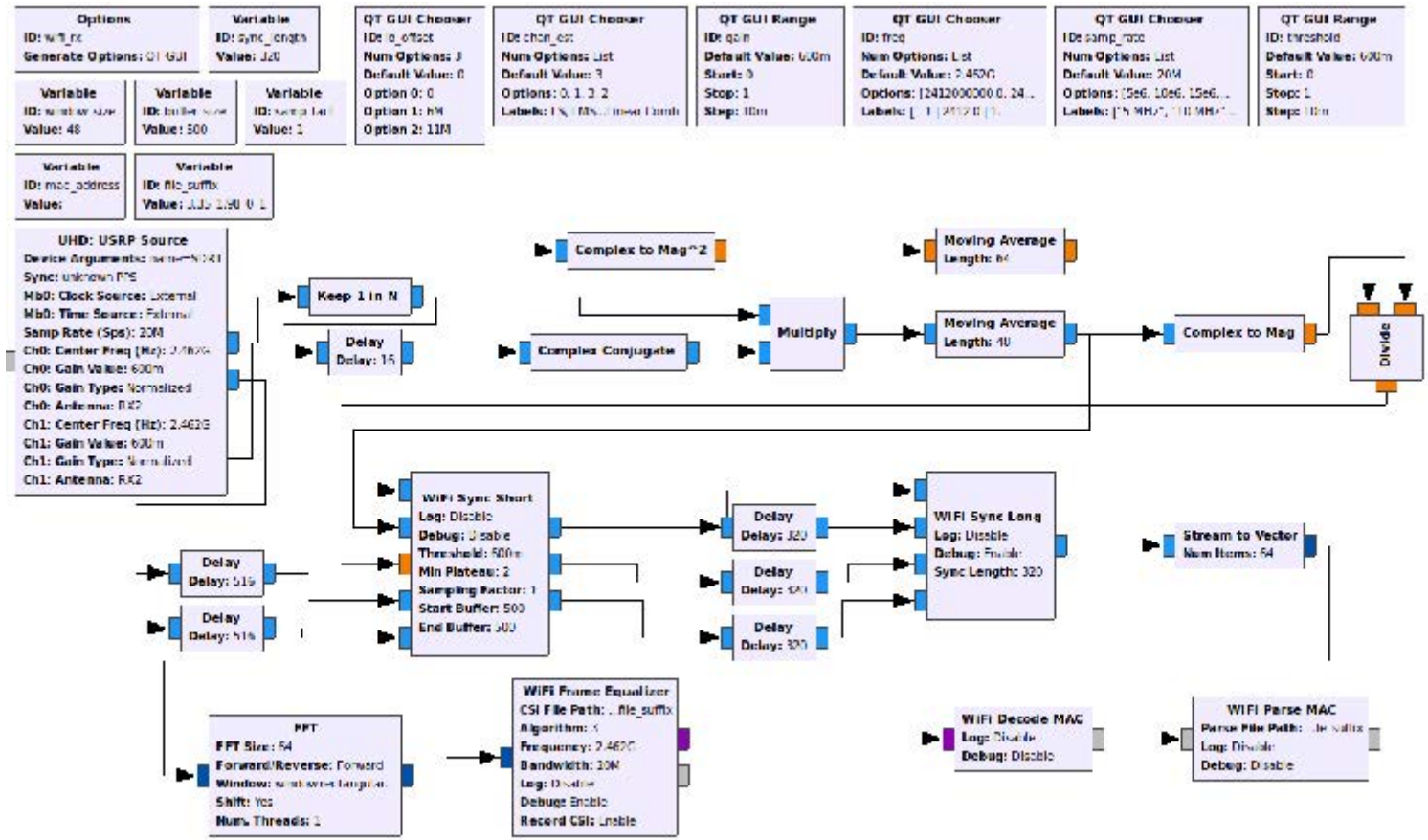


Figure 3.6: GNUradio flowgraph for Wi-Fi sniffer

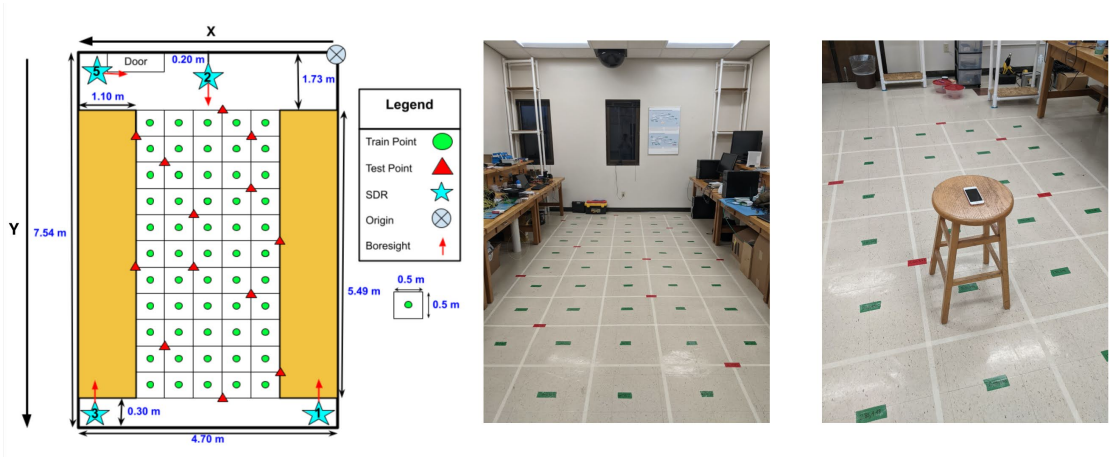


Figure 3.7: First real-world experimental setup in the lab room. Left: the layout of the room illustrating positions of the detectors (SDRs), testing, and training points for sources. Center: The grid layout in our lab room. Right: A phone being tested at a source location. Best viewed in color [71] [68] [69][70].

(a) SDR1 (b) SDR2 (c) SDR3

Figure 3.9: Three SDRs shown in Figure 3.8

Another set of data collection was performed with a different testbed. Data collection utilized an SDR USRP X300 located in the laboratory room. The SDR featured four receive antennas,

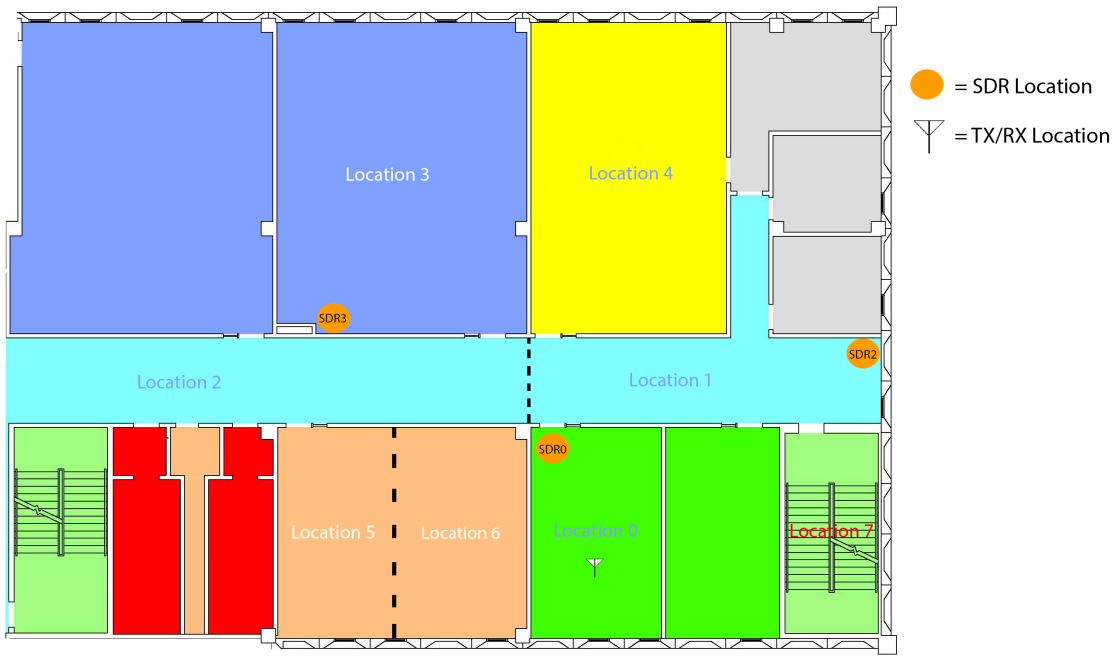


Figure 3.8: Second real-world experimental setup on the third floor of Simrall Hall at MSU. The location position of the experiment. Locations 0, 3, 4, 5, and 6 are laboratory rooms. Locations 1 and 2 are hallways. Location 7 is a stairway. The SDR locations are shown as orange circles. The RX/TX location symbol denotes the wireless access point. Best viewed in color [36].

providing eight complex IQ values (four real and four imaginary values) per data sample. IQ samples were gathered using two cellphones across six distinct room locations, as depicted in Figure 3.8 and Figure 3.4. These locations encompass two laboratory rooms, a hallway, a corridor, and a stair room.

The data collection system consisted of three applications: the transmitter app, server app, and USRP app. The transmitter app, written in C++ with QT for Android and iOS devices, functioned as a User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) client. The server app, developed in MATLAB, served as both UDP and TCP servers. The USRP app, coded in C++ and utilizing the UHD library for NI USRP, acted as a TCP client.

The transmitter app initially listened for UDP broadcasts to obtain the essential IP address and ports for establishing connections with the server app over UDP and TCP. Once these details were acquired, the transmitter app initiated connections with the server using both protocols. It transmitted crucial settings, including MAC addresses, device names, and data collection locations, to the server via TCP. Following acknowledgment from the server, the transmitter app commenced the transmission of Wi-Fi packets to the router through UDP, chosen for its suitability given the nature of the operation. Upon the server app decoding the predetermined number of packets defined in the settings, the transmitter app ceased packet transmission.

Upon initiation, the server app established a connection with the USRP app using the TCP protocol. The USRP app configured the X300 USRP according to the required number of antennas, set up matrices for buffering IQ samples, and cooperated with the server app.

The server app also connected with the transmitter app, receiving all the settings provided by the phone. When the server app received a request to begin the data collection process, it instructed the USRP app to collect samples and transmit them using the TCP protocol. The USRP app gathered these samples and sent them to the server app through TCP. The server app then searched the collected IQ samples for packets, decoding the MAC addresses within the discovered packets and using the first 400 IQ samples (preamble) of each packet with a matching MAC address from the transmitter app to calculate the DoA, storing the results in a file.

The data collection process commenced with the operator configuring all three applications. Some parameters were set in MATLAB before launching the server app, while additional settings were adjusted using the transmitter app on the phone. The phone used for data collection was transported to the desired location, and IQ samples were collected accordingly. When the phone

was relocated to a new position, the operator transmitted the updated location information to the server app using the transmitter app. IQ samples were collected at each location in this manner. MATLAB was utilized to decode the 802.11g frames transmitted from the phone with the Wireless Local Area Network (WLAN) toolbox, and DoA was calculated using the MUSIC algorithm [8].

The MUSIC algorithm, introduced by Schmidt and colleagues in 1979, processed the output data from an array to decompose features, creating orthogonal signal and noise subspaces corresponding to signal components. These subspaces were combined to construct a spectrum function that identified DoA signals through spectral peaks. The mathematical representation of the MUSIC algorithm was as follows:

$$P(\theta) = \frac{1}{\|\mathbf{a}(\theta)^T \mathbf{R}^{-1} \mathbf{a}(\theta)\|^2} \tag{3.1}$$

where:

- θ is the direction of arrival
- a(θ) is the steering vector, which is a vector that represents the response of the antenna array to a signal arriving from direction θ
- R is the covariance matrix of the received signals.

After accumulating a sufficient volume of data, the phone was set to airplane mode, and the data streaming was halted. The same process was repeated for another device across all six different locations, resulting in the collection of 3,120,000 samples in total, ensuring sufficient signal coverage [20].

The collected datasets were stored in Comma Separated Value (CSV) format, with a total size of approximately 603MB. These datasets included fifteen features such as device/cellphone MAC

(Media Access Control) addresses, transmitter IDs, locations, packet IDs, raw IQ values, and signal DoA. The datasets were organized based on the order in which data was collected from the cellphones, with each location containing a total of 600 samples and locations designated from 0 to 5 in the CSV file.

Alongside the real-world data collection, Wireless Insite (explained in section 3.3.3.2) is used to collect a simulated dataset for the prison environment as shown in Figure 3.10.

3.3.3.1 GNURadio

GNURadio [20] is an open-source software toolkit that's like a Swiss Army knife for radio enthusiasts and professionals as mentioned in Chapter I. With its vast library of signal processing blocks and intuitive graphical interface, GNURadio makes it easy to build and experiment with SDR systems. It can be used to decode digital signals, create various wireless communication protocols, or explore radar applications.

3.3.3.2 Wireless Insite

Wireless Insite software is a new software by RemCom [57] as a remarkable solution within the domain of wireless communication and signal propagation analysis. This advanced tool redefines the landscape of wireless systems by allowing precise simulation and visualization of signal behaviors in a wide array of environments, ranging from indoor settings to expansive outdoor terrains. Through the utilization of sophisticated electromagnetic modeling techniques, Wireless Insite empowers engineers and researchers to anticipate how signals propagate, interact with obstructions, and experience attenuation in diverse scenarios. Whether crafting a Wi-Fi network for a smart home or strategizing the deployment of a 5G network in a bustling urban setting,

Wireless Insite imparts invaluable insights for optimizing coverage, signal quality, and overall system performance. Its intuitive interface and robust capabilities render it an indispensable asset for professionals navigating the dynamic realm of wireless technology.

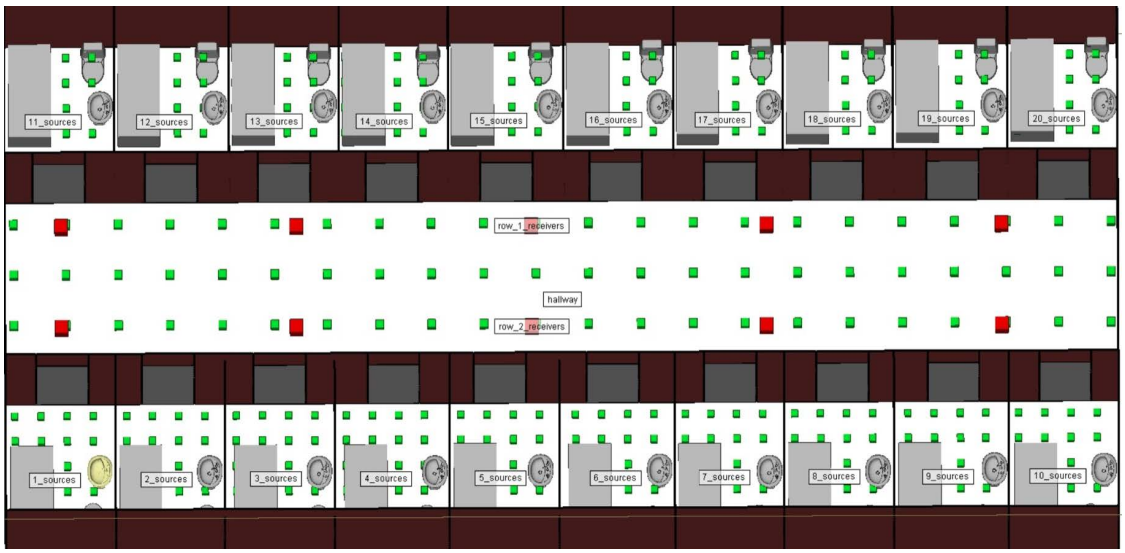


Figure 3.10: 3D model of a prison environment created in Wireless Insite [36] [57]

This detailed methodology provided the foundation for an efficient contraband cellphone detection system. Its ultimate goal is to spot and pinpoint illegal cellphones hidden within the prison, significantly enhancing security measures and putting a stop to unauthorized communications.

3.3.3.3 Device Fingerprinting

An MLP served as the validation tool for the dataset in device fingerprinting. MLPs represent standard neural networks and function as a baseline for potential future models trained on this dataset. The construction of this MLP took place on Google Colab using Python 3.6.9 with the scikit-learn framework. This particular MLP focused on a single location (0.1) of frames, resulting in a dataset containing 3000 frames from various devices.

To prepare the dataset, the frames were initially trimmed to the first 1500 samples. Subsequently, the absolute values of these samples were computed and standardized within a range from 0 to 1. The network architecture designed for the MLP consists of four layers, each of which comprises 515 neurons and Rectified Linear Unit (ReLU) activation functions. These layers feed into the output layer. A 5-fold cross-validation was implemented, along with an L2 penalty term of 0.0001. With a batch size of 200, the MLP employed the Adam (adaptive moment estimation) method for training, utilizing a learning rate of 0.001. The training and testing dataset split involved allocating 80% to training and 20% to testing. This methodology was instrumental in fine-tuning and evaluating the MLP's performance in the context of device fingerprinting.

3.3.3.4 Location Fingerprinting

For location fingerprinting, a 1D CNN was employed. CNNs leverage spatial correlations in data and are more memory-efficient compared to standard **DNNs!**s. The construction of the CNN

for this task was carried out using TensorFlow on Google Colab, utilizing Python 3.6.9. The network optimization was achieved using the Adam method for training, with a learning rate of 0.0001. The batch sizes were set to 64, and the data was divided into training, validation, and testing sets at a distribution of 60%, 20%, and 20%, respectively.

The data preprocessing involved using the absolute values of the first 1500 complex samples to reduce the network's size. The frames were then passed through a conv1D layer with 25 filters of size 20, followed by a max pooling layer of size 2. Subsequently, they were directed to a Batch Normalization layer to mitigate overfitting. Afterward, they were passed through another conv1D layer with 40 filters of size 13 and another max pooling layer of size 2. Finally, the frames underwent processing through a conv1D layer with 56 filters of size 7, followed by another max pooling layer of size 2. Following this, a dropout layer of 0.5 was applied, and then the data was flattened.

The flattened data was then directed to three fully-connected layers with sizes 64, 32, 24, and 12, before going through another dropout layer of 0.7. The final step was connecting the data to the output layer, which consists of two nodes representing the x and y coordinates of the device.

A second experiment was conducted for second real-world data collected from the setup shown in Figure 3.8. The datasets have been neatly organized and stored in Hierarchical Data Format 5 (HDF5) files. At the lowest level, these datasets comprise arrays of IQ samples and CSI values, forming the STF and Long Training Field (LTF) of each frame. To keep things well-arranged, these values have been structured based on the locations where they were collected and the specific phones used for collection. In the HDF5 file, each phone is labeled as RX-label, systematically

assigned numbers 0 through 7. Furthermore, the datasets are organized by the SDR label that gathered them, pinpointing the transmitter and location using labels within the dataset.

In terms of prepping the data for the neural network, IQ samples and CSI frames have been furnished as input variables, while location numbers serve as labels or output variables. The raw IQ signals and CSI frames have been combined into a cohesive dataset. To facilitate effective training and testing, the data has been divided into two portions, with approximately two-thirds reserved for training and one-third for testing. A validation dataset wasn't employed due to settings not being fine-tuned during the experiment. Sklearn's train-test split function, employing the stratify option, ensures each class is evenly represented in both training and testing sets. Additionally, the random state option is set to maintain consistent data splits across experiments.

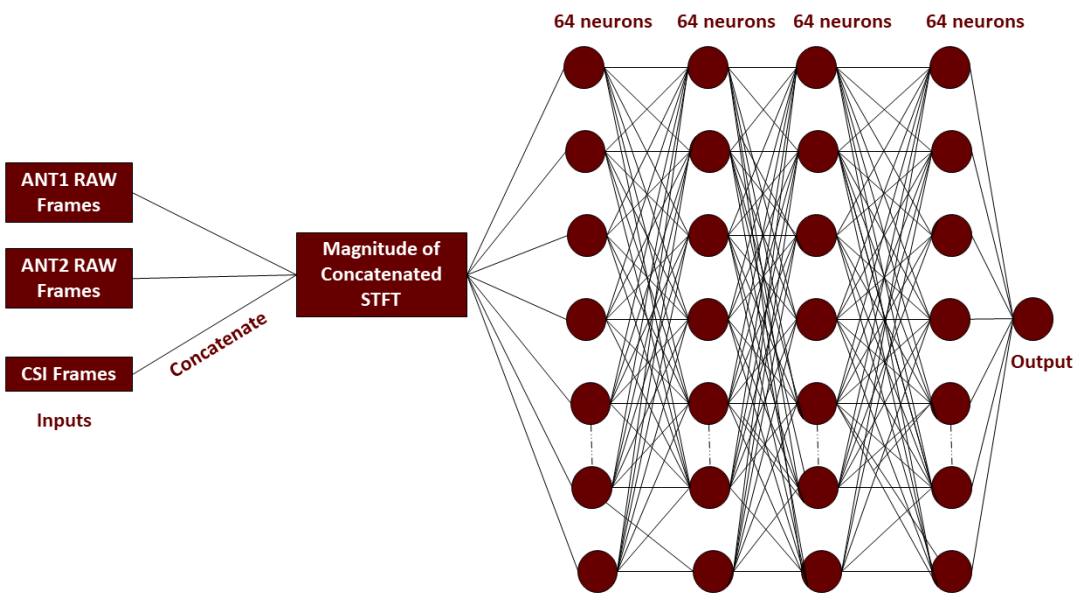


Figure 3.11: MLP network architecture for the second experiment shown in Figure 3.8 [31]

.

To enhance accuracy and latency in calculations, the concatenated samples in the training and testing data have been transformed into STFT, a complex-valued signal. Magnitudes of these complex-valued STFT signals have been used as input for the neural network. The classification task is executed using an MLP model with four layers, each containing 64 neurons as shown in Figure 3.11. To prevent over-fitting, the regularization parameter, represented by alpha, is set to 1e-4. The maximum iteration value is set to 1,000 to allow for an adequate number of iterations to converge.

In analyzing the data, a 200-sample Hanning window was applied to perform the STFT. Experimentation with various window sizes was conducted, and the best results were achieved using this particular window length. A binary classifier was utilized for classifying eight different locations in a multi-class classification setup, employing a one vs. all approach. This approach generated eight separate binary classifier models.

3.4 Human Activity Recognition with Wi-Fi

This section explains the methodology used to collect the dataset (section 3.4.2), pre-process (section 3.4.4) the collected dataset, and finally train a CNN model (section 3.4.5.1) for classification. Various popular deep learning methods are explored in section 3.4.5 that can be used for future work as suggested in 5.2. The following sections explain the various data acquisition methods as well as publicly available datasets to perform experiments for human activity recognition using Wi-Fi.

3.4.1 Purpose and Research Objective

This section is an effort to act as a guide to researchers who are looking to explore CSI data collection and Human Activity Recognition using Wi-Fi signals. This section presents the various data acquisition methods that are readily available, provides ideas on how to implement one or the other techniques, and talks about the possible hardship while doing so. Along with the data acquisition methods, we will also present the public datasets that are available. In addition to that, this section also compares the different preprocessing techniques and deep learning methods that were explored before.

3.4.2 Data Acquisition Techniques

To proceed with the study of human activity recognition using Wi-Fi signals, one can perform in-house data collection or download publicly available datasets. It is unfortunate that the manufacturers of the Wi-Fi chips have not made CSI accessible for researchers. However, studies [42] and [26] reduce the effort and provide CSI easily. Atheros CSI and 802.11 Linux CSI tool have been quite popular, and it provides CSI for Qualcomm Atheros NIC and Intel 5300 Wi-Fi Card

correspondingly. These tools have been used for many prior types of research. However, Nexmon [64] is gaining popularity currently because of its support in various Wi-Fi chips, unlike Atheros and 802.11 Linux CSI tool.

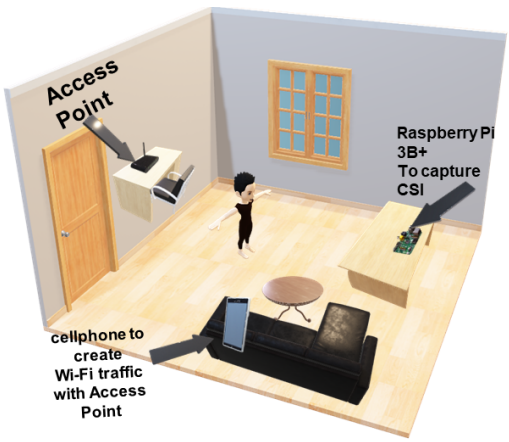
There are various data acquisition techniques that are available to collect CSI data from Wi-Fi. For all of these techniques, there is another way to collect CSI using the SDR-based method. This method, however, requires a deep understanding of Wi-Fi protocol. The next subsection explains these techniques individually in detail. Our data collection setup in different environments is shown in the Figure 3.12.

The different devices can be placed in different places for the purpose of data collection or in real-world settings. Those combinations are shown in Table 3.2:

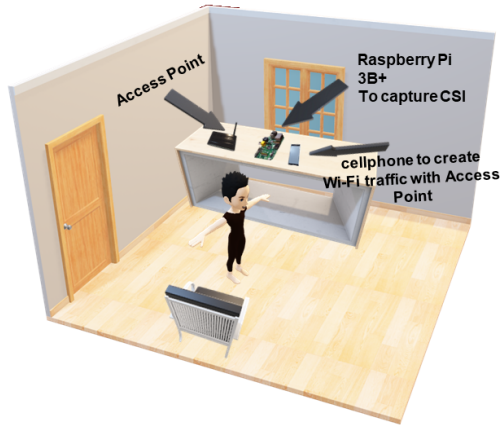
Table 3.2: Combination of Devices Locations

Same Location	Different Location
Tx, Rx, Sniffer	-
Tx, Rx	Sniffer
Rx, Sniffer	Tx
Tx, Sniffer	Rx
	Tx, Rx, Sniffer

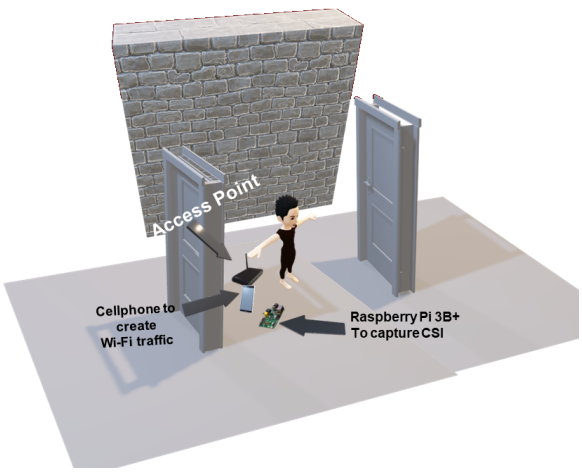
The various methods of data acquisition methods are shown in Figure 3.13. Five different data acquisition scenarios mentioned before are readily available to set up in the compatible hardware to collect CSI from Wi-Fi for HAR. Each of them has pros and cons which are explained below.



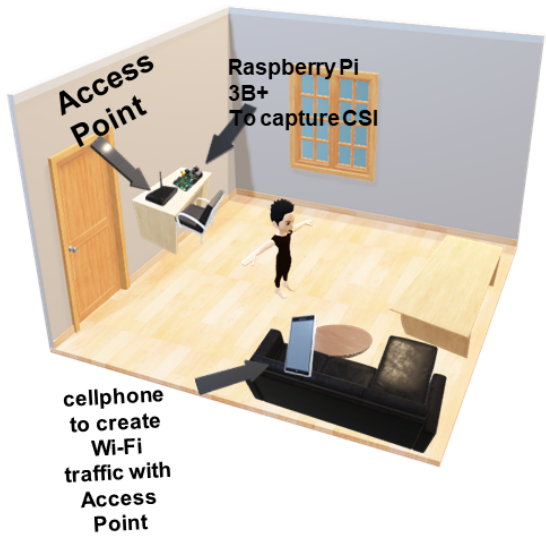
(a) Data collection setup in an apartment.



(b) Data collection setup in a lab.



(c) Data collection setup in a hallway.



(d) Configuration of different devices in different locations. This is an example of a combination from Table 3.2 where the router and Raspberry Pi are in one location and the transmitter(cellphone) is in a different location.

Figure 3.12: Data collection setup in various environments.

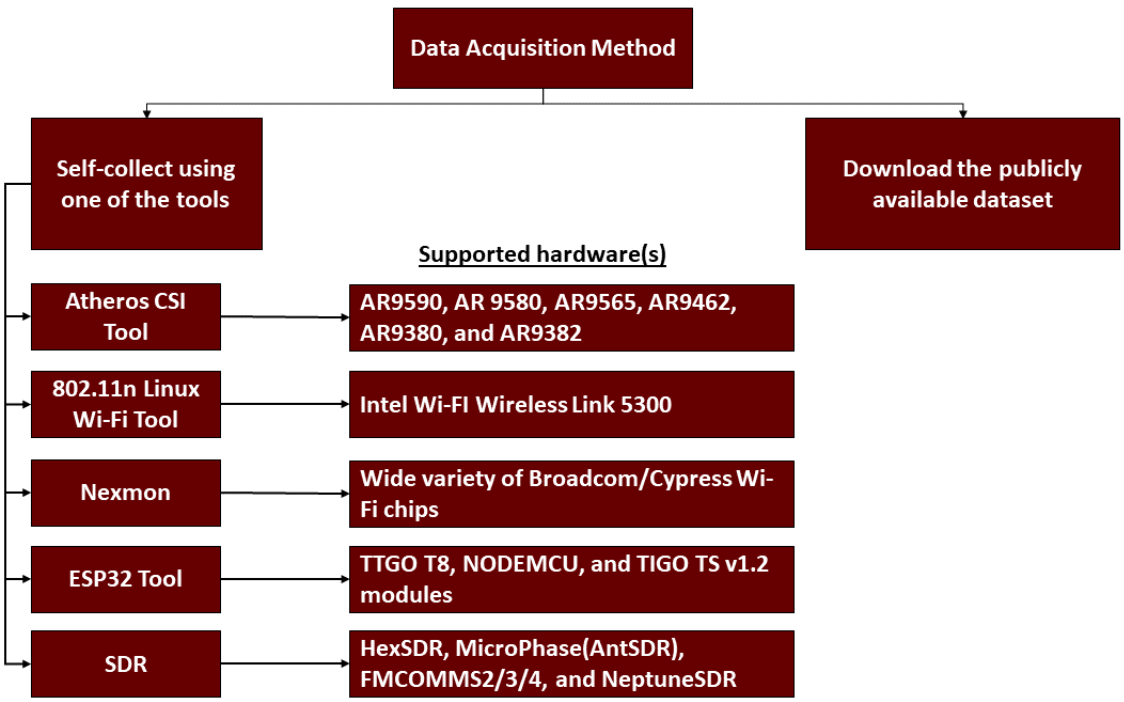


Figure 3.13: Data acquisition techniques overview.

3.4.2.1 Atheros CSI Tool

Atheros CSI Tool [42] is a software tool that was developed to extract and analyze the CSI from Qualcomm Atheros Wi-Fi Chipset. At the time of this writing, only AR9590, AR 9580, AR9565, AR9462, AR9380, and AR9382 have been verified by the developer and other organizations. This tool uses 10 bits to give the value of the real part and another 10 bits to give the imaginary part of the CSI with the real and imaginary parts ranging from -512 to 512. The final data is structured in a matrix format. Ath9k Linux driver is used to build this tool which is also capable of providing the received packet payload, time stamp, RSSI of each antenna, the data rate, etc. This tool works for Linux-based systems such as Ubuntu [46], OpenWRT [55], and Linino [75].

3.4.2.2 Linux 802.11n CSI Tool

Linux 802.11n CSI Tool [26] is another popular tool that is used for collecting CSI data from Intel Wi-Fi Wireless Link 5300 for 802.11n MIMO radios. It consists of custom-modified firmware with open-source Linux wireless drivers. This tool is capable of reporting CSI Wi-Fi with 30 subcarriers spread evenly among the 56 and 114 subcarriers for the 20MHz and 40MHz channels. The developers also provided Matlab utilities to parse the standardized CSI format. Installation instruction is located here [12].

3.4.2.3 Nexmon

Nexmon [64] is the new C-based firmware patch that works for several Broadcom/Cypress Wi-Fi chips. This tool is gaining a lot of popularity in the present days due to its support for BCM43455c0 which is found in Raspberry Pi 3B+/4B. Raspberry Pi is a single-board embedded system with a very low cost. Hence, it is an excellent choice to flash this firmware to collect CSI

data. This method allows one to extract channel state information of 802.11a/g/n/ac up to 80MHz bandwidth Wi-Fi channel. At the time of this writing, the GitHub for Nexmon supports kernel version 5.10.92. However, the current kernel version is 5.15 which is not supported. So, in addition to the steps mentioned in the creator's repository, we had to perform a hold on the kernel update to compile the firmware successfully.

To understand the Wi-Fi firmware and the modification, it is important to know the underlying architecture of the Wi-Fi hardware itself. Figure 3.14 shows the BCM43455 Wi-Fi architecture.

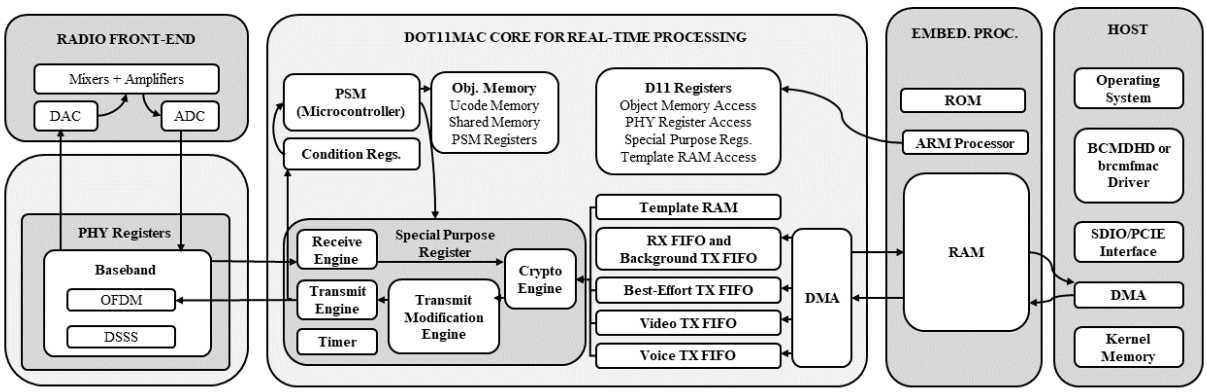


Figure 3.14: Raspberry Pi 3B+ BCM43455 Wi-Fi Diagram [63] [9]

Figure 3.15 illustrates the portion of Nexmon workflow. To understand the complete workflow, it is recommended to go through Figure 2 in [63]. The author's work summarizes that they start by analyzing the firmware in IDA to extract address and structure information. Using this information, they successfully extracted binary blobs for replacement (templateram), modification (flashpatches), and compression (ucode). Then they require the latter to attain space for firmware patches. Before compression, it is possible to modify the ucode to change the chip's real-time

behavior. To modify the ARM firmware, patches were written in C, which was then linked against the firmware functions and the result was merged into a new firmware.

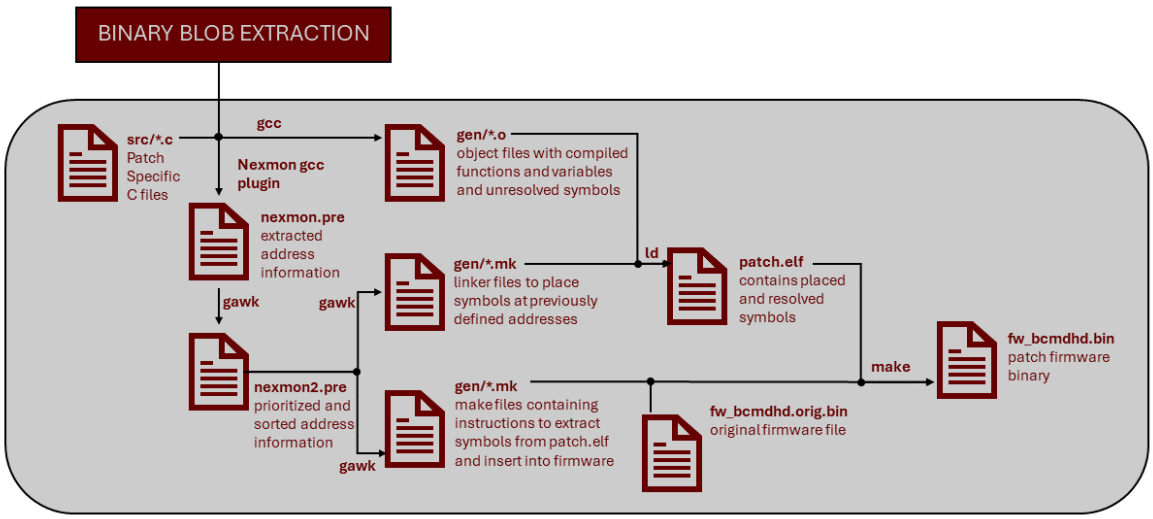


Figure 3.15: Raspberry Pi 3B+ BCM43455 Wi-Fi Diagram [63]

Wi-Fi CSI data is collected using 2.5 GHz Wi-Fi with 80 MHz bandwidth which provides 256 subcarriers. Subcarrier indices 90 - 120 are used to generate spectrograms for each index. For HAR using Wi-Fi, Nexmon flashed into Raspberry Pi 3B+ to collect dataset.

3.4.2.4 SDR-based Method

Open-sdr has created an open-source tool named OpenWi-Fi [54] that is capable of running 802.11a/g/n Wi-Fi with 20MHz bandwidth. This tool supports various SDRs such as HexSDR, MicroPhase(AntSDR), FMCOMMS2/3/4, and NeptuneSDR.

3.4.2.5 ESP32 CSI Tool

The ESP32 CSI Tool [72] supports TTGO T8, NODEMCU, and TIGO TS v1.2 modules that enable researchers to receive CSI for Wi-Fi and transmit the obtained CSI data through USB serial in real-time to a computer or smartphone.

After data acquisition whether in-house collection or publicly available dataset, the data is pre-processed before feeding it to the deep learning methods. A typical process of the flow is shown in Figure 3.16.

3.4.3 Publicly Available Dataset

Researchers and practitioners in this field have created various publicly available datasets to facilitate experimentation and benchmarking. Table 3.3 is a compiled list of datasets that can be utilized for activities such as indoor localization, presence detection, and joint activity recognition. These datasets are valuable resources for evaluating algorithms and techniques in WiFi-based human activity recognition. The following table provides details and direct links to these datasets.

Table 3.3: Publicly Available Datasets for WiFi-based Activity Recognition

Dataset	GitHub
A Survey of Human Activity Recognition Using WiFi CSI	[94]
Deep Learning and Its Applications to WiFi Human Sensing: A Benchmark and A Tutorial	[89]
AutoFi: Towards Automatic WiFi Human Sensing via Geometric Self-Supervised Learning	[90]
Joint Activity Recognition and Indoor Localization With WiFi Fingerprints	[79]
Harvesting Ambient RF for Presence Detection Through Deep Learning	[91]
OPERAnet: A Multimodal Activity Recognition Dataset Acquired from Radio Frequency and Vision-based Sensors	[37]
WiAR: A Public Dataset for WiFi-based Activity Recognition	[25]

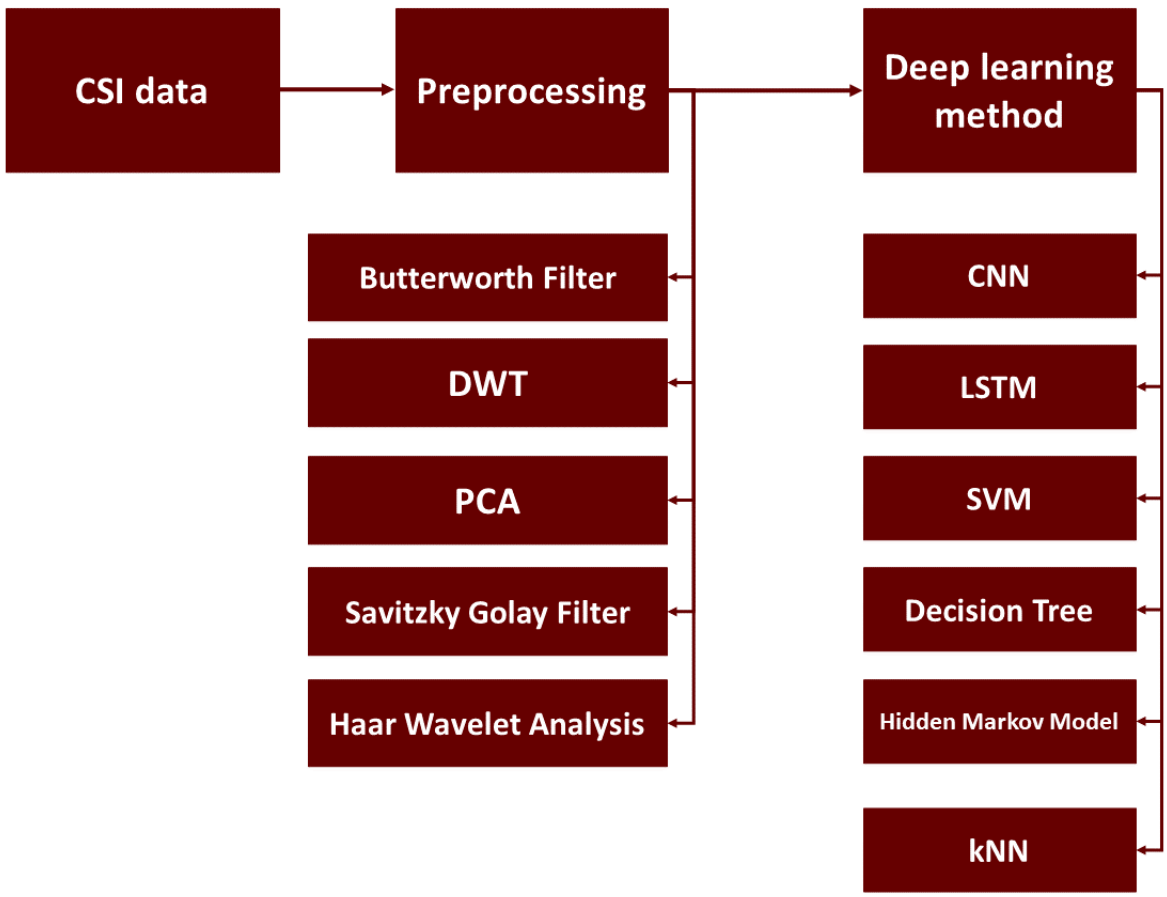


Figure 3.16: Typical flow of HAR.

3.4.4 Preprocessing Techniques

While many previous works have used simple techniques like using amplitude only from the CSI [84, 88], conjugate multiplication [73], FFT [73], removal of carrier frequency offset [67], packet Detection delay [67], gaussian smoothing [32, 96, 23], time stretching [96], frequency shifting [96], random phase shift removal [47], etc. Some of these techniques that have been explored in the literature that proved preprocessing helps to increase the accuracy of detection are described below.

3.4.4.1 Butterworth Filtering

Lots of researchers [43, 32, 85] have used the Butterworth Filtering method to filter noise in experiments related to Human Activity Recognition. It is a low-pass Infinite Impulse Response (IIR) filter that can improve the accuracy of activity recognition algorithms. The filter works by allowing the frequencies relevant to human activities to pass through with minimal distortion while blocking out irrelevant frequencies. It can be particularly beneficial for the dataset that contains noise and interference (significant sources of error) for Human activity recognition.

3.4.4.2 Discrete Wavelet Transform (DWT)

DWT is a mathematical model that can decompose a signal into its constituent frequency sub-bands. As the name suggests, DWT breaks down the signals into a series of wavelets with different frequencies and scales [10, 99, 43, 82, 93, 81]. Unlike the Fourier Transform, the DWT uses wavelet basis to represent specific features of the signal at different scales. It works by passing the signal through a series of high-pass and low-pass filters which results in a set of low-frequency and high-frequency components. This is an iterative process as shown in Figure 3.17. Various

researchers have used this method to preprocess the dataset before applying machine learning methods for HAR.

3.4.4.3 Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is another popular method in this domain to process the data before feeding it to machine learning techniques [73, 96, 53, 93, 80, 10, 82, 93, 81]. Past papers have used PCA in their dataset which resulted in better results. It is a statistical technique that is used to reduce the dimensions of a dataset without losing the most important variables(features) that contribute to the variation in the data. The principal components are ordered in descending order of the variance meaning the first principal component has the most variation in the data and so on. Since there are many subcarriers in the OFDM symbol (Wi-Fi data), it has been shown that PCA helps in removing some of those subcarriers with a lower variance that does not contribute to activity recognition. This results in improving the accuracy and lowering training time.

3.4.4.4 Savitzky Golay Filter

Savitzky Golay Filter is another digital signal processing technique that helps to smoothen noisy data [76]. This filter at first fits a polynomial to a small window of data points and then estimates the value of the polynomial at the center of the window. It uses the least-squares method to estimate the coefficient of the polynomial. The window size and polynomial degree are chosen such that they provide data that is smooth without losing too much of fine details. A larger window size includes more data points which can provide better smoothing at the expense of a potential loss of fine details.

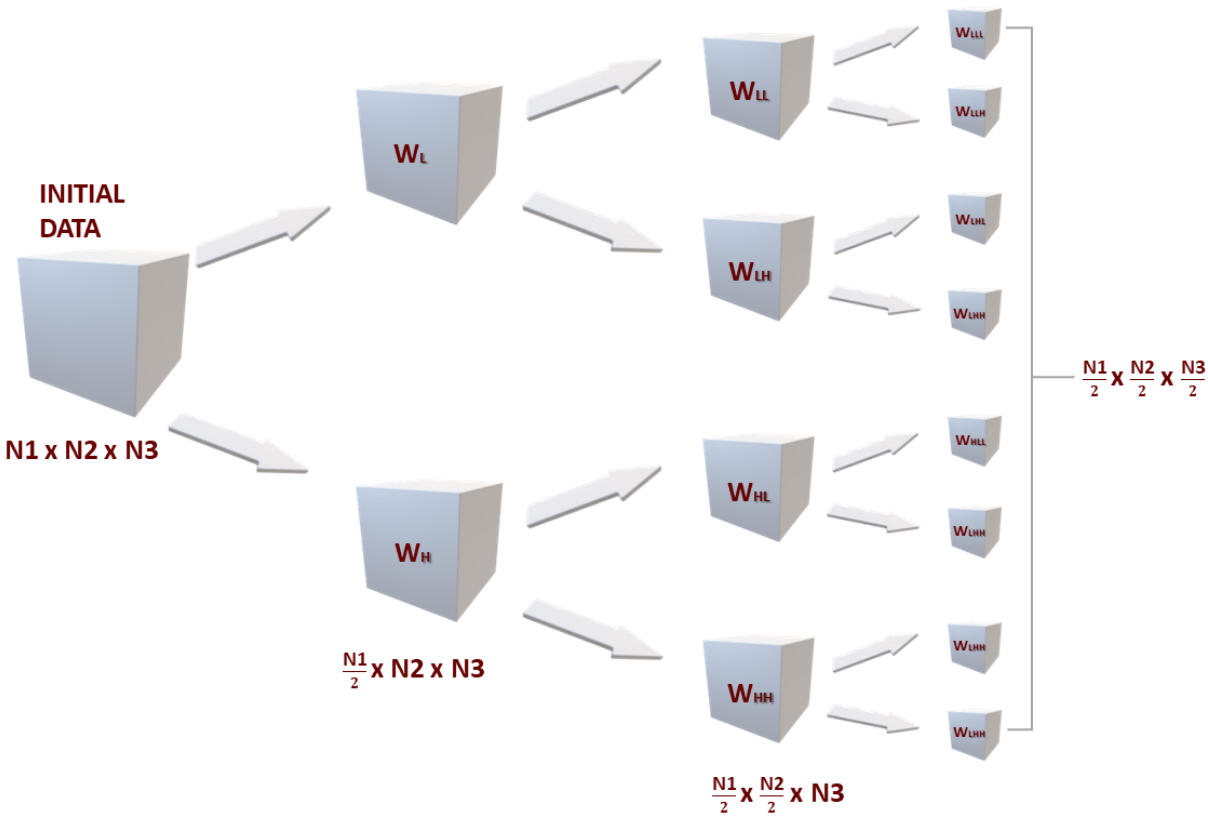


Figure 3.17: The figure depicts 3-D separable DWT procedure by applying 1-D DWT for each dimension and splitting the data into chunks to obtain wavelets for different sub-bands [50]

3.4.4.5 Hampel Filter

The Hampel filter is used to remove outliers from the time series dataset [99, 39]. The filter uses window size to calculate the Median Absolute Deviation (MAD) for each data point in the window. MAD is a measure of the variation of the data within the said window. The difference between the data point and the median of the window is then calculated. If the difference is greater than a certain threshold(3x median), then it is considered an outlier and is replaced by the median of the window. Previous works have shown this filter has helped in smoothing the activity recognition dataset.

3.4.4.6 Haar Wavelet Analysis

Haar Wavelet Analysis is a special type of DWT with its function known as the Haar wavelet function [10]. It is a step function that decomposes a signal into a series of wavelets where each wavelet is scaled and shifted version of the Haar wavelet function. These wavelets capture different frequencies and characteristics of the signal by dividing the signal into smaller and smaller sub-signals at different levels of resolution. At each subsequent level, the approximation from the previous level is further decomposed into a new approximation and detail. This is an iterative process that terminates when the condition of the desired level of decomposition is met. Many previous papers have applied this method to process their dataset.

3.4.5 Classification and Regression Models for HAR

The prior research has used CNN, Recurrent Neural Network (RNN), K-Nearest Neighbor (kNN), and Long-Short Term Memory (LSTM) models to classify the activities with great accuracy. These methods are explained below:

3.4.5.1 Convolutional Neural Network (CNN)

A CNN or ConvNet is a specialized type of artificial neural network designed primarily for processing and analyzing visual data, such as images and videos [35, 44, 97, 14, 41]. CNNs are widely used in computer vision tasks, including image recognition, object detection, image segmentation, and more. The above-mentioned papers have utilized a CNN-based network to train their model to classify the type of activity performed. The key feature of CNNs is their ability to automatically learn hierarchical patterns and representations directly from the raw pixel data, making them highly effective for visual tasks. So, generating a spectrogram from the CSI data resulted in better results. CNN comprises of following:

- **Convolutional Layers:** These layers apply convolutional operations to the input image using small filters or kernels. A convolutional operation involves moving the filter across the input image, computing element-wise multiplications, and summing up the results to produce a feature map. Each filter captures different patterns, such as edges, textures, or shapes. Multiple filters are typically used to extract diverse features.
- **Activation Function:** After each convolutional operation, an activation function, often ReLU, is applied element-wise to introduce non-linearity into the model. ReLU sets all negative values to zero and keeps the positive values unchanged.
- **Pooling Layers:** Pooling layers downsample the spatial dimensions of the feature maps, reducing the computational load and making the network more robust to small variations in the input. Max-pooling is a commonly used technique where the maximum value within a small region (pooling window) is taken as the representative value for that region.
- **Fully Connected Layers:** After several convolutional and pooling layers, the network typically ends with one or more fully connected layers, which act as classifiers or regression layers to make predictions based on the high-level features learned by the previous layers.

Figure 3.18 shows the CNN model used for this study and 3.19 shows the elaborated model.

3.4.5.2 Long-Short Term Memory (LSTM)

LSTMs were designed to address the vanishing and exploding gradient problems that occur in traditional RNNs when dealing with long sequences of data [44, 83, 62, 33, 65].

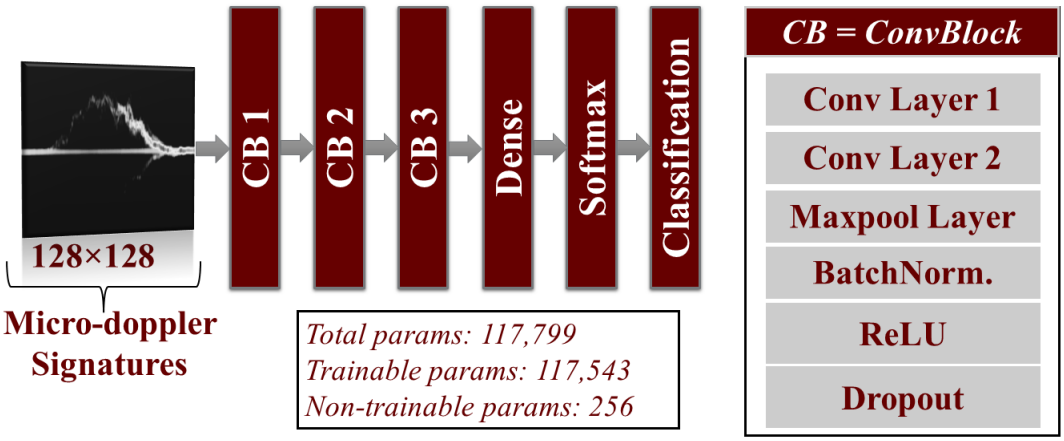


Figure 3.18: The CNN architecture for classification

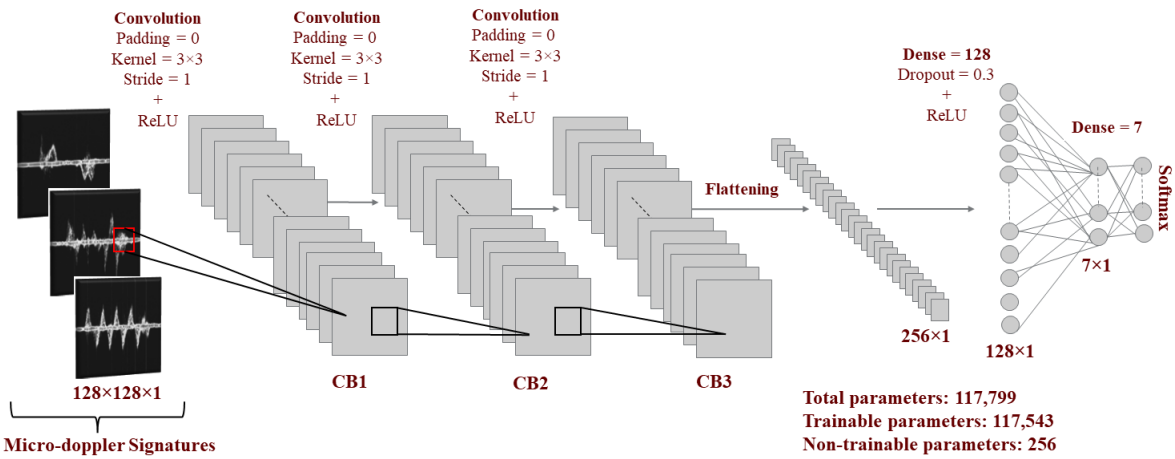


Figure 3.19: The elaborated CNN architecture for classification

In sequential data, such as our time-series data in human activity recognition problems, the order of elements matters, and traditional feedforward neural networks cannot efficiently handle such data due to their fixed-size inputs. RNNs were introduced to handle sequential data by maintaining a hidden state that evolves with each element in the sequence, allowing them to capture temporal dependencies.

Standard RNNs struggle to retain and propagate information over long sequences, making them less effective when dealing with tasks that require long-term dependencies. This is where LSTMs come into play. The LSTM architecture includes additional components called "gates" that help regulate the flow of information and selectively update the hidden state. Looking at the previous research, this model has shown great results in the Human Activity Recognition problem using CSI data.

3.4.5.3 Support Vector Machine (SVM)

An Support Vector Machine (SVM) is a supervised machine learning algorithm that has shown to be a good choice for classification and regression tasks [77, 65, 52, 40, 11, 41, 3]. SVMs are particularly effective for binary classification problems but can also be extended to handle multiclass classification like human activity recognition.

The main idea behind SVM is to find the optimal hyperplane that best separates the data points of different classes in a high-dimensional feature space. The hyperplane is chosen such that it maximizes the margin, which is the distance between the hyperplane and the closest data points (support vectors) of each class. The intuition is that a larger margin leads to better generalization and robustness of the model on unseen data.

In the case of linearly separable data, the optimal hyperplane is the one that maximizes the margin between the two classes. If the data is not linearly separable, SVM can still find a hyperplane by introducing a soft margin to allow some misclassifications. The trade-off between maximizing the margin and minimizing the classification error is controlled by a hyperparameter called the "regularization parameter" (often denoted as C).

For nonlinearly separable data like Wi-Fi CSI, SVM can use a kernel trick to map the data into a higher-dimensional feature space, where the classes might become linearly separable. Commonly used kernels include the polynomial kernel and the Radial Basis Function (RBF) kernel (also known as the Gaussian kernel). The choice of the appropriate kernel function is critical to the performance of SVM with Wi-Fi CSI data. The selection of the kernel function and its hyperparameters should be based on the specific characteristics of the data and the classification task at hand. Common kernel functions used with SVM for Wi-Fi CSI data include the polynomial kernel and the RBF kernel.

3.4.5.4 Decision Tree

A Decision Tree is a popular supervised machine learning algorithm used for both classification and regression tasks [44, 52]. It is a tree-like model where each internal node represents a decision based on a feature, and each leaf node represents the outcome or predicted value. Decision Trees are capable of handling both linearly and non-linearly separable data. Wi-Fi CSI data can be used with Decision Trees for classification tasks.

3.4.5.5 Hidden Markov Model (HMM)

A Hidden Markov Model (HMM) is a statistical model used to model sequential data, where the underlying system is assumed to be a Markov process with hidden states [14, 86, 92, 83]. It is a type of probabilistic graphical model that finds applications in various fields, including speech recognition, natural language processing, bioinformatics, and more. HMM has also been used over the past with Wi-Fi CSI data to model and analyze the changes in the wireless channel over time. The changes in the radio channel due to the movement of objects or people in the environment in Wi-Fi CSI data can be used to understand and predict the underlying patterns and states of the channel using HMM.

3.4.5.6 K-Nearest Neighbor (kNN)

Another popular model that made this list is kNN [4, 24, 95]. It is a simple and intuitive supervised machine learning algorithm used for classification and regression tasks. It is a type of instance-based learning algorithm, meaning that it memorizes the training data points and makes predictions based on the proximity (i.e., distance) of new data points to the training examples. It can be used with Wi-Fi CSI data for classification tasks, such as activity recognition or localization in wireless environments. kNN is a suitable choice for Wi-Fi CSI data because it can handle non-linear relationships and does not assume any specific data distribution.

3.4.6 Radar vs. Wi-Fi-based HAR

Radar is an active sensor, it is highly used in HAR. Wi-Fi on the other hand is passive and is readily available. This section presents the methodology used to compare the two of the most popular RF sensors and shows how they perform. A dataset of 7 activities, fall, lie down, pick up,

run, sit down, stand up, and walk, is developed for this study. The activities are chosen in such a way that they are distinct from one another. Figure 3.20 depicts each gesture made by a participant.

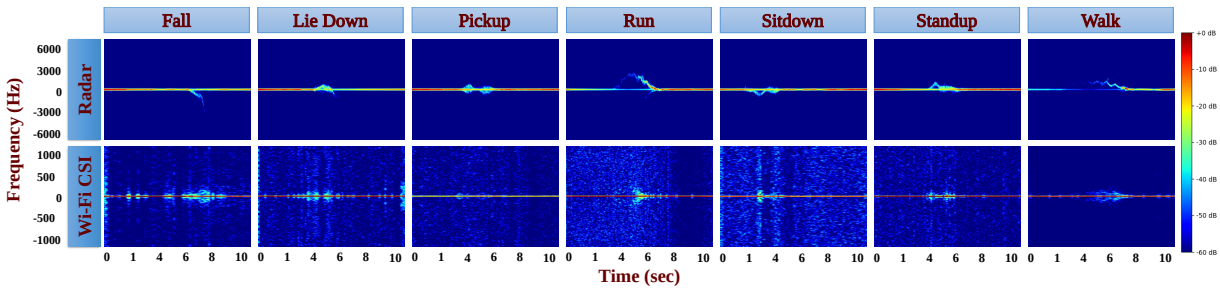


Figure 3.20: Spectrogram of 7 activities for Radar and Wi-Fi CSI data

In total, 700 samples were collected, encompassing 7 distinct gestures. Each gesture was represented by 100 individual samples, which were collected from 5 different subjects. In other words, each subject provided 20 samples for each class the first 16 samples (80%) were used for training and the last 4 samples (20%) were used for testing.

To perform the data collection, three different sensors, INRAS Radarbook2 Radar, Raspberry Pi 3B+, and Camera, are used in the data collection to capture both kinematic movement and visual data. The Raspberry Pi 3B+ is used for Wi-Fi CSI data collection by using Nexmon as explained in section 3.4.2.3. The Azure Kinect Camera is used as a reference for each data collected from Radar and Raspberry Pi as shown in Figure 3.21.

The INRAS Radarbook2 functions as a Frequency-Modulated Continuous Wave (FMCW) radar system, with an operating frequency range spanning from 76GHz to 80GHz. This system emits chirp signals directed towards the radar's field of view. Initially, these transmitted signals bounce off the target, specifically in our case, humans. Consequently, the radar receives a signal

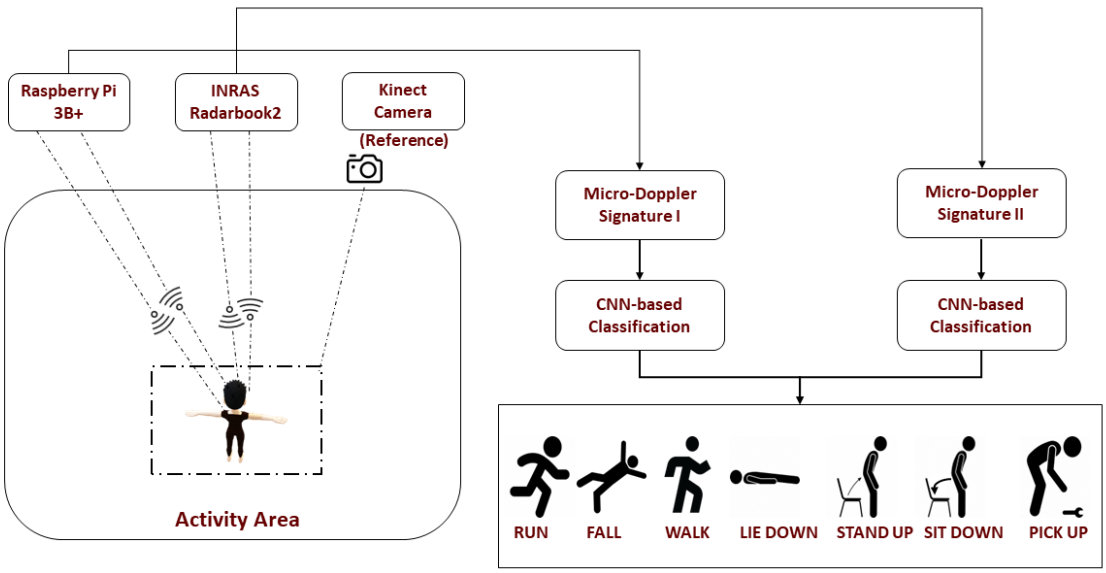


Figure 3.21: Radar vs. Wi-Fi comparison data collection testbed

that has undergone frequency shifts and time delays, relative to the initially transmitted signal. The kinematic characteristics of each human target movement give rise to a dynamic sequence of micro-motions, such as vibrations and rotations, as outlined in Chen et al.'s work [6]. Each unique gesture generates its own distinct patterns, which can be analyzed effectively through time-frequency analysis techniques. The μ-D spectrogram is then calculated from the square modulus of the STFT of the continuous-time input signal $x[k]$ and may be described in terms of the window function, $h[k]$.

$$\text{STFT}[x[k]]_{m,\omega} = X[m,\omega] = \sum_{k=-\infty}^{\infty} x[k]h[k-m]e^{-j\omega k} \tag{3.2}$$

$$\text{Spectrogram}[x[k]]_{m,\omega} = |X[m,\omega]|^2 \tag{3.3}$$

Figure 3.22 illustrates the process of creating a μ-D spectrogram from 2D raw radar data. Figure 3.20 presents examples of μ-D signatures for various activities, represented through color-scaled images. Positive Doppler frequencies are visualized above the horizontal axis, while negative Doppler frequencies are depicted below the horizontal axis, with the frequency scale starting from 0 Hz.

Figure 3.22: Block diagram of radar signal processing for μ-D signature generation

The INRAS Radarbook2 is used for radar data collection. The radar operates from 76 to 80GHz, with two TX and 16 RX. Since the radar is used only for collecting the movements of the targets, only 1 TX-RX pair has been used for the experiment. The device can be initialized with different parameters depending on the situation. Table 3.4 shows the parameters set for the INRAS Radarbook2 radar for the experiment.

Table 3.4: AWR2243 Radar Parameters [29]

Parameter	Value
Number of ADC Samples	256
Number of TX Channels	1
Number of RX Channels	1
Starting Frequency	76GHz
Frequency Slope	53.33MHz/µs
Bandwidth	4GHz
Pulse Repetition Interval (PRI)	83.33 μs
Sampling Rate	3.41GHz
RX Gain	40 dB
Periodicity	100 ms
Number of Chirp Loops per Frame	1200
Number of Frames	100
Total Time	10 sec

CHAPTER IV

RESULTS

In this chapter, the research findings are presented, offering insights drawn from data analysis. This section presents the final product, relationships, and trends identified in the research, enhancing our understanding of the subject matter and carrying practical implications. This chapter shall provide ideas for future work that can be derived which will be explained in detail in section 5.2.

4.1 Spectrum Scanning System

After a full sweep of the frequency band from 100MHz to 3GHz with an increment of 50MHz bandwidth, the designed system can plot the whole band as shown in figure 4.1.

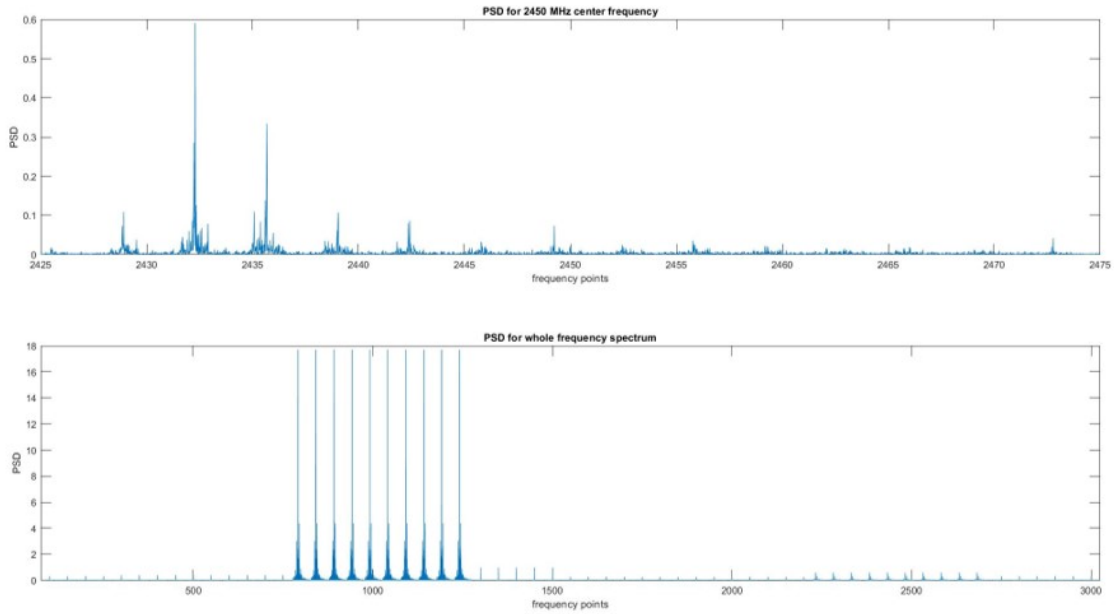


Figure 4.1: Spectrum scanning system result after scanning from 100MHz to 3GHz frequency band. The top figure is zoomed into 2.5 GHz center frequency to observe the peaks observed in the bottom figure. This scan was performed in Simrall Hall at Mississippi State University and the high power is seen for the college Wi-Fi on the 4th floor.

4.2 Contraband Cellphone Detection

This section presents the results of device fingerprinting and location fingerprinting for contraband cellphone detection. The performance of classification algorithms for accurate room location estimation is presented in this section. All the algorithms were implemented in Python 3.7 and executed on a desktop computer with a 3.80 GHz AMD Ryzen Threadripper 24-Core processor and 256.0 GB of RAM. The operating system used was Windows 10 Pro.

4.2.1 Device Fingerprinting

The MLP (Multi-Layer Perceptron) used for device fingerprinting ran for 59 training epochs before it stopped early due to a lack of improvement in the validation score by 0.001. This training

process took a total of 3.4 minutes. It was observed that misclassifications were distributed quite evenly among the various devices. The only significant exceptions were observed between two iPhone SE devices, which is not surprising since they are of the same make and model. In summary, the algorithm performed well on the dataset, achieving an accuracy of 90.23%. This result establishes a strong baseline for future research in this field.

4.2.2 Location Fingerprinting

The CNN was trained for 25 epochs and took approximately 7.1 minutes to complete. Notably, the final Root Mean Square Error (RMSE), or Euclidean distance, for the test set was 1.08 meters. This result is quite promising, especially considering that the spacing between the data points should enable users to distinguish the location within the room where the phone's signal was emitted.

It's important to note that this work serves as a preliminary exploration, and there is room for improvement. Incorporating additional features such as CSI or RSSI could potentially enhance the accuracy and precision of the model.

4.2.3 Effect of DoA on Classification Accuracy

The impact of DoA on classification accuracy was assessed. Initially, only IQ numbers were used to train and test the neural network. The SDR employed in this study had four antennas, each providing one complex value (one real and one imaginary number). This resulted in eight features from the four antennas used to train the neural network. Subsequently, the signal's DoA was added as an additional feature to evaluate its effect on localization accuracy. The performance

of a customized neural network, a basic CNN, Decision Tree (DT), and SVM was compared. The classification results are summarized in Table 4.1.

Table 4.1: Classification Accuracy with and without DoA

Classifier Name	Only IQ Samples	Both DoA and IQ Samples
MLP	0.70	0.89
CNN1D	0.62	0.63
DT	0.58	0.85
SVM	0.86	0.88

The accuracy without DoA is 0.70, 0.62, 0.58, and 0.86 for MLP, CNN1D, DT, and SVM, respectively. When DoA was added, the accuracy increased to 0.89, 0.63, 0.85, and 0.88, respectively. This suggests that DoA significantly improved localization accuracy for all classifiers, with the MLP network achieving the highest accuracy.

4.2.4 Binary Classification vs Multi-class Classification

Multi-class classification was initially used to analyze data keeping both IQ samples and signal DoA. However, as individual location accuracy varied, binary classification was employed for each location, and the averages were compared. Table 4.2 provides the binary classification results from the MLP classifier.

The individual accuracy for each location ranged from 0.85 to 0.99, while the overall accuracy in multi-class classification was 0.89. The average classification result for binary classification was 0.91, which is higher than the previous result. Binary classification improved accuracy for individual locations, enhancing the performance. For example, location 4 increased from 82

Table 4.2: Classification Accuracy with Binary Classification Method

Location Number	Accuracy
0	0.99
1	0.93
2	0.92
3	0.85
4	0.88
5	0.89
Average	**0.91**

4.2.5 Detecting Unknown Locations

The classifier's ability to detect unknown locations without prior training was analyzed. Data was divided into training and testing parts, ensuring that they did not share any location points. The MLP network was used for this analysis, considering both IQ samples and adding DoA as features. Table 4.3 presents the results.

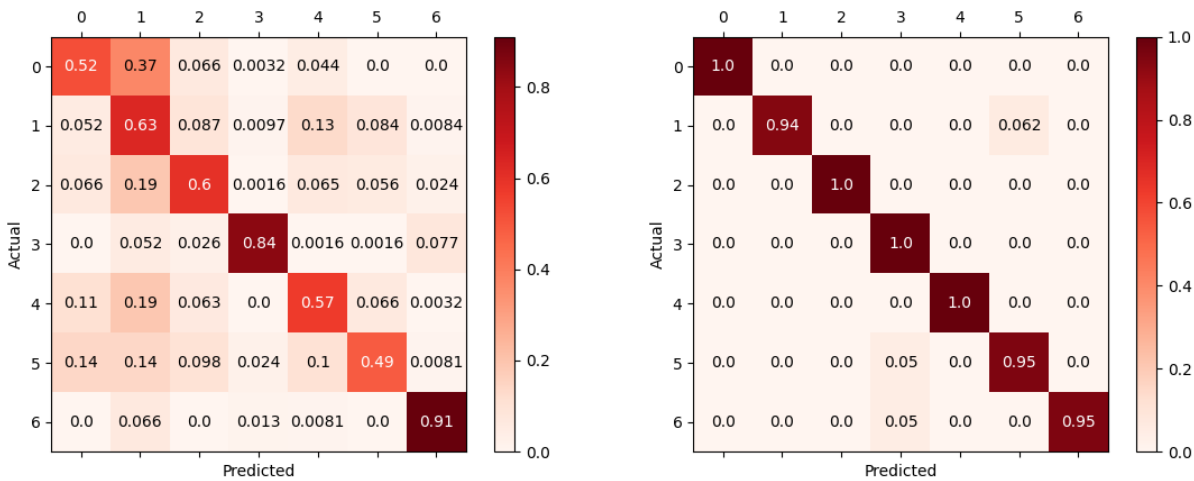
Table 4.3: Performance of Detecting Unknown Locations

Samples used for Training	Classification Accuracy
Only IQ Samples	0.49
Both DoA and IQ Samples	0.38

The accuracy was lower than the previous classification result, which is reasonable. Notably, when trained with IQ samples only, the accuracy was better, achieving 0.49, compared to 0.38 after adding DoA. While the accuracy was not exceptionally high, the classifier was able to identify some locations without training data. The accuracy depends on the number of samples used for training and the accuracy of those samples' labels.

4.3 Human activity recognition

For the classification of radar and Wi-Fi μ-D spectrograms, a 2D CNN structure has been designed. As depicted in Fig. 3.18, this CNN architecture is composed of three Convolution Block (CB), with each block featuring two convolution layers. The convolution layers of the first two CBs are equipped with 32 filters, while the last CB employs 64 filters for its two convolution layers. Each convolution layer utilizes a 3×3 kernel size and a 1×1 stride. Following the two convolution layers in each block, there is a sequence of operations: a 3×3 max-pooling, batch normalization, ReLU activation, and dropout with a rate of 0.3. Subsequently, the tensor is flattened and fed into a dense layer with a size of 128. Then a dropout operation with a rate of 0.3 and ReLU activation are applied. Finally, the network concludes with a softmax classifier.



(a) Confusion matrix for Wi-Fi-based activity classification

(b) Confusion matrix for radar-based activity classification

Figure 4.2: Confusion matrix for Wi-Fi and Radar-based activities

Table 4.4: Performance Comparison

Network	Testing Accuracy	Precision	Recall	F1 Score
Wi-Fi	65.09	67.91	65.09	65.72
Radar	97.78	97.99	97.68	97.78

For performance evaluation, the dataset was divided into 80% for training and 20% for testing as mentioned in 3.4.6. Spectrogram images derived from radar and Wi-Fi data were saved as 128x128 grayscale PNG images. The comparison results between radar-based and Wi-Fi-based signatures are presented in Table 4.4. It's evident from the table that radar exhibits higher efficiency in human activity classification. Radar achieves a classification accuracy of 97.78%, while Wi-Fi achieves only 65.09%. This indicates that radar outperforms Wi-Fi-based activity classification by a significant margin of 32.7%.

Despite the dataset's challenging nature, given the variability in performed gestures among individuals, the confusion matrix depicted in Fig. 4.2b illustrates how accurately the 2D CNN distinguished between different classes for radar-based spectrograms. Conversely, the confusion matrix in Fig. 4.2a shows the performance of Wi-Fi-based human activity classification. While Wi-Fi lags significantly behind radar in terms of accuracy, the results suggest that there is substantial potential for Wi-Fi in this domain. This can be explained because Radar operates at 76-80GHz whereas Wi-Fi is at 5GHz. Doppler shifts for higher frequencies are much higher thus easily detecting activities. Further advancements in this field could open up new opportunities across various applications for Wi-Fi.

CHAPTER V

CONCLUSIONS

5.1 Conclusions

In this thesis, three distinct studies have been discussed: the Spectrum Scanning System, Contraband Cellphone Detection System, and Human Activity Recognition using Wi-Fi. All of these studies used Software Defined Radios to collect data. These studies have made substantial impacts on various research. This section concludes the document with conclusion by looking at the accomplishments and implications of each project.

The Spectrum Scanning System realized through the innovation of SDR, has ushered in intriguing possibilities in passive microwave remote sensing. The project has demonstrated the capability to pinpoint and leverage occupied spectrums, often referred to as "signals of opportunity," in order to enrich remote sensing. By employing SDR, this system functions as an active spectrum analyzer, continuously scrutinizing the electromagnetic spectrum. It isn't solely engaged in acquiring communication data; instead, it identifies valuable information with scientific and environmental implications. This technology permits the gathering of data from diverse sources, including television and radio broadcasts, satellite communications, and even cellphone signals. Such data holds immense value for passive microwave remote sensing, offering advantages to domains like meteorology, environmental surveillance, disaster management, and soil moisture calculation for

agriculture. The evolution and expansion of this system are anticipated to yield further efficiency in passive microwave remote sensing.

The Contraband Cellphone Detection System project can significantly enhance security in correctional facilities. Advanced technology was harnessed to craft a system proficient in identifying concealed cellphones within prisons. While this task may seem straightforward, it is a transformative achievement. It not only serves as a deterrent for illicit activities within correctional facilities but also safeguards the well-being of inmates and the dedicated personnel working in these environments. This isn't solely about technology; it marks a substantial step toward ensuring justice, security, and harmony in our communities.

Looking into the device fingerprinting and location fingerprinting, in summary, this work outlines a guide to create personalized datasets for Wi-Fi and LTE devices, crucial for device/location fingerprinting. This approach entails the utilization of multiple cost-effective receivers and open-source software to facilitate data collection. Diverse data features are collated, encompassing raw IQ samples, CSI, and RSSI / Reference Signal Received Power (RSRP). Furthermore, this work furnishes two datasets following the same methodology, focusing on both Wi-Fi and LTE signals. These datasets encompass a multitude of signals emitted by various devices located within a densely populated room, thereby introducing added complexity to the datasets and the challenges they seek to address. Additionally, this work provides fundamental Machine Learning (ML) algorithms as a benchmark for each dataset, demonstrating performance levels akin to state-of-the-art algorithms, thus substantiating their credibility. These datasets and baseline algorithms can be invaluable for researchers aiming to evaluate the efficacy of their own fingerprinting algorithms.

In the study, room-level location classification was conducted using both raw IQ samples and Signal DoA data. The dataset was meticulously collected within the laboratory setup, involving an X300 SDR, two cellphones, and six distinct locations. The analysis encompassed three key phases: initially, the accuracy of classification using solely IQ samples was compared with that using only DoA data, with the combination of IQ samples and DoA yielding the best results. Notably, the MLP network tailored for this purpose outperformed other classifiers like the CNN1D, DT, and SVM. Following this, a binary classification approach for individual locations was adopted, proving superior to the multi-class classification. Lastly, a mechanism was implemented to enable the classifier to detect unknown locations by withholding specific location information during training. Overall, the experiments yielded highly satisfactory accuracy results, underscoring the effectiveness of the approach.

Wi-Fi-based HAR is a technology that uses Wi-Fi signals to detect and classify human activities. It relies on capturing CSI data from Wi-Fi packets to analyze changes in signal patterns caused by different activities. However, this method faces several limitations and challenges. Handling the large volume of Wi-Fi packets and network traffic poses computational and processing challenges. Additionally, the trained model's inability to generalize across different environments, such as from a lab to a hallway or apartment setup, presents a significant issue. Varying geometry in different spaces can affect Wi-Fi signals differently, impacting the system's accuracy. Privacy and security concerns arise due to Wi-Fi signals' ability to penetrate walls and capture sensitive information inadvertently. Interference from other devices and neighboring Wi-Fi networks can also degrade the quality of data. Furthermore, distinguishing between similar activities and optimizing power consumption are ongoing challenges. Despite these limitations, Wi-Fi-based HAR shows promise

in various applications, and ongoing research aims to address these issues and improve its accuracy and applicability in real-world settings.

Finally, looking into Wi-Fi-based HAR, it is a technology with great potential for various applications, but it comes with significant limitations and challenges. The reliance on large volumes of Wi-Fi packets and handling network traffic poses computational complexities. Moreover, the inability of trained models to generalize across different environments and the impact of varying geometry on Wi-Fi signals reduce the system's overall effectiveness. Despite these obstacles, ongoing research and technological advancements hold the key to overcoming these limitations and improving the accuracy and reliability of Wi-Fi-based HAR systems. By addressing these challenges, future work can unlock the full potential of Wi-Fi-based HAR in smart homes, healthcare, and other domains, bringing us closer to a more connected and intelligent future.

5.2 Future Work

In terms of spectrum scanning, there is room for significant advancement through a range of research directions. The cyclostationary method, for instance, can be further explored and fine-tuned to enhance its efficiency, especially in complex and noisy environments. Future work can be towards refining algorithms and signal processing techniques to better detect cyclostationary signals. Similarly, for the matched filter, there's potential in investigating more advanced design and implementation techniques, tailoring filters to specific signal types or modulations. This targeted approach can significantly improve the detection accuracy.

The energy detection method, too, can benefit from further sophistication. Researchers can explore advanced energy detection algorithms and thresholding techniques to increase sensitivity

and reduce false positives in signal detection. Moreover, integrating these methods into a hybrid system can prove promising, creating a dynamic spectrum scanning system that selects the most suitable method based on the general scenario.

A significant emphasis could be placed in the anechoic chamber to conduct experiments to establish ground truth for capturing known signals. By utilizing the controlled conditions within the chamber, researchers can characterize and validate the behavior of signals across different frequencies, power levels, and environmental factors.

These experiments would involve precisely generating and emitting known signals within the anechoic chamber while simultaneously employing the spectrum scanning system to capture and analyze them. By comparing the system's measurements with the ground truth established through experimental setups, researchers can refine and calibrate the system's algorithms for signal detection, classification, and characterization.

For the contraband cellphone detection system, expanding the dataset is a key future step. Incorporating data from a broader range of devices, models, and locations can strengthen the system's adaptability and robustness. It's also crucial to analyze the positioning of SDRs and its impact on localization accuracy. This can lead to optimized SDR placement strategies, accounting for factors such as signal propagation and interference. Additionally, adding signals such as Time of Arrival (ToA) data can provide insights into the trajectory of detected devices, offering valuable information.

In the domain of human activity recognition through Wi-Fi signals, there are several avenues for future work. One crucial aspect is the refinement of preprocessing techniques. One can continue to explore and combine various methods to enhance data quality. This may involve experimenting

with new techniques or fine-tuning existing ones to effectively filter, denoise, and prepare the Wi-Fi signal data as mentioned in section 3.4.4.

A primary focus shall involve the systematic collection of datasets that incorporate the presence of wheelchairs and other metallic objects such as crutches. This data collection effort aims to elucidate how Wi-Fi signatures of human activities are affected by the proximity of such metallic surfaces in Nursing homes. Conducting experiments in controlled environments will enable researchers to analyze variations in Wi-Fi signal patterns induced by interactions with metallic objects, thus refining the accuracy and robustness of HAR systems.

In addition to investigating the influence of metallic objects, future research endeavors could explore the variability of Wi-Fi signatures across diverse environmental settings. This exploration entails collecting datasets in various indoor and outdoor environments, thereby providing insights into how environmental factors such as building structures, furniture layouts, and external interferences affect Wi-Fi signal propagation and activity recognition. By comprehensively studying Wi-Fi signatures in different contexts, researchers can improve the generalizability and adaptability of HAR systems for real-world applications.

Experimenting with the range of machine learning models for human activity recognition is another crucial step. Beyond the familiar models, such as LSTM, kNN, SVM, and decision trees, new models should be tested to assess their performance and suitability for different scenarios and applications. Furthermore, feature engineering techniques can be applied to extract more informative features from Wi-Fi signal data. Dimensionality reduction, PCA, and wavelet transforms can be explored to identify relevant patterns.

Lastly, an important step for development is the adaptation of these systems for real-time applications, accomplished through the creation of a real-time notification system using a single board PC. This goal involves the optimization of algorithms and models to ensure low-latency and resource-efficient deployment. Such enhancements enable the system to recognize human activities in real-time, offering potentially life-saving applications, particularly in environments like nursing homes.

REFERENCES

[1] F. Alemuda and F. J. Lin, "Gesture-Based Control in a Smart Home Environment," *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jun 2017.

[2] Amped Wireless, "Wireless Standard,", `https://ampedwireless.com/learningcenter/tutorials#wifi-standard`, 2021, Accessed on November 8, 2023.

[3] S. Arshad, C. Feng, Y. Liu, Y. Hu, R. Yu, S. Zhou, and H. Li, "Wi-chase: A WiFi based human activity recognition system for sensorless environments," *2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Macau, China, June 2017, pp. 1–6, IEEE.

[4] S. A. Arshad, C. Feng, Y. Liu, Y. Hu, R. Yu, S. Zhou, and H. Li, "Wi-chase: A WiFi based human activity recognition system for sensorless environments," *2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2017, pp. 1–6.

[5] S. Banerjee and V. Brik, "Wireless Device Fingerprinting," *Encyclopedia of Cryptography and Security*, Springer, Boston, MA, 2011.

[6] V. C. Chen, D. Tahmoush, and W. J. Miceli, *Radar micro-Doppler signatures*, Institution of Engineering and Technology, 2014.

[7] CNX Software, "802.11ax WiFi Aims to Deliver Higher Throughput up to 10 Gbps in High-Density Scenarios,", `https://www.cnx-software.com/2016/05/27/802-11ax-wifi-aims-to-deliver-higher-throughput-up-to-10-gbps-in-hi-/gh-density-scenarios/`, 2016, Accessed on November 8, 2023.

[8] T. Q. Company, "Qt Documentation,", `https://doc.qt.io/`, 2023, Accessed on October 18, 2023.

[9] C. S. Corporation, *CYW43455 Single-Chip 5G WiFi IEEE 802.11n/ac MAC/Baseband/Radio with Integrated Bluetooth 5.0*, Mar. 2019.

[10] N. Damodaran, E. Haruni, M. Kokhkharova, and J. Schäfer, "Device free human activity and fall recognition using WiFi channel state information (CSI)," *CCF Transactions on Pervasive Computing and Interaction*, vol. 2, 2020, pp. 1–17.

[11] N. Damodaran and J. Schafer, "Device Free Human Activity Recognition using WiFi Channel State Information," *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Leicester, United Kingdom, Aug. 2019, pp. 1069–1074, IEEE.

[12] D. Dhalperi, "Linux 802.11n CSI Tool Installation Instructions," 2023, Accessed on October 18, 2023.

[13] M. Dillinger, K. Madani, and N. Alonistioti, *Software Defined Radio: Architectures, Systems and Functions*, wiley series in software radio, June 2003.

[14] P. Fard Moshiri, R. Shahbazian, M. Nabati, and S. A. Ghorashi, "A CSI-Based Human Activity Recognition Using Deep Learning," *Sensors*, vol. 21, no. 21, Oct. 2021, p. 7225.

[15] A. S. Fayez, "Designing a Software Defined Radio to Run on a Heterogeneous Processor," 2011.

[16] A. for Healthcare Research and Quality, "Falls Dashboard,", `https://www.ahrq.gov/npsd/data/dashboard/falls.html`, 2023, Accessed on October 18, 2023.

[17] P. S. Foundation, "Python Documentation,", `https://www.python.org/doc/`, 2023, Accessed on October 18, 2023.

[18] J. L. Garrison, J. R. Piepmeier, and R. Shah, "Signals of Opportunity: Enabling New Science Outside of Protected Bands," *2018 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, 2018, pp. 501–504.

[19] R. Globalnet, "SDR for Prototyping Satellite Ground Stations,", `https://www.rfglobalnet.com/doc/sdr-for-prototyping-satellite-ground-stations-0001`, 2022, Accessed on October 18, 2023.

[20] GNU Radio Development Team, "GNU Radio: Free and Open-Source Software Radio,", `https://www.gnuradio.org/`, 2021, Accessed on October 18, 2023.

[21] E. Grayver, *Implementing Software Defined Radio*, 1 edition, Springer, New York, NY, 2012.

[22] Great Scott Gadgets, "HackRF,", `https://greatscottgadgets.com/hackrf/`, 2009-2023, Accessed on October 18, 2023.

[23] Y. Gu, F. Ren, and J. Li, "PAWS: Passive Human Activity Recognition Based on WiFi Ambient Signals," *IEEE Internet of Things Journal*, vol. 3, no. 5, 2016, pp. 796–805.

[24] Y. Gu, F. Ren, and J. Li, "PAWS: Passive Human Activity Recognition Based on WiFi Ambient Signals," *IEEE Internet of Things Journal*, vol. 3, no. 5, Oct. 2016, pp. 796–805.

[25] L. Guo, L. Wang, J. Liu, , and W. Zhou, "WiAR: A Public Dataset for WiFi-based Activity Recognition," 2023.

[26] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "802.11n CSI Linux Tool,", https://dhalperi.github.io/linux-80211n-csitool/, 2011, Accessed on October 18, 2023.

[27] F. Han and X. Zhang, "An ESPRIT-like algorithm for coherent DOA estimation," *IEEE Antennas and Wireless Propagation Letters*, vol. 4, 2005, pp. 443–446.

[28] N. Instruments, "National Instruments Corporation,", https://www.ni.com/, 2023, Accessed on October 18, 2023.

[29] T. Instruments, "TI AWR2243,", https://www.ti.com/product/AWR2243, Accessed on November 8, 2023.

[30] F. Islam, J. Farmer, A. Dahal, B. Tang, J. Ball, and M. Young, "Wifi fingerprinting based room level classification: combining short term Fourier transform and imbalanced learning method," *Signal Processing, Sensor/Information Fusion, and Target Recognition XXXI*. June 2022, vol. 12122, pp. 269–277, SPIE.

[31] F. Islam, J. Farmer, A. Dahal, B. Tang, J. E. Ball, and M. Young, "Wi-Fi Fingerprinting-Based Room-Level Classification: Combining Short Term Fourier Transform and Imbalanced Learning Method," *Proceedings Volume 12122, Signal Processing, Sensor/Information Fusion, and Target Recognition XXXI*, 2022, p. 121220Y.

[32] M. S. Islam, M. K. A. Jannat, M. N. Hossain, W.-S. Kim, S.-W. Lee, and S.-H. Yang, "STC-NLSTMNet: An Improved Human Activity Recognition Method Using Convolutional Neural Network with NLSTM from WiFi CSI," *Sensors (Basel, Switzerland)*, vol. 23, 2022.

[33] M. S. Islam, M. K. A. Jannat, M. N. Hossain, W.-S. Kim, S.-W. Lee, and S.-H. Yang, "STC-NLSTMNet: An Improved Human Activity Recognition Method Using Convolutional Neural Network with NLSTM from WiFi CSI," *Sensors*, vol. 23, no. 1, Dec. 2022, p. 356.

[34] Keysight Technologies, "OFDM Basic Principles Overview,", https://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems/wlan-ofdm/Content/ofdm_basicprinciplesoverview.htm, 2023, Accessed on October 18, 2023.

[35] P. H. Kindt, C. Turetta, F. Demrozi, A. Masrur, G. Pravadelli, and S. Chakraborty, "WiFiEye – Seeing over WiFi Made Accessible," 2022.

[36] S. Kodipaka, A. Dahal, L. Smith, N. Smith, B. Tang, J. E. Ball, and M. Young, "Adversarial indoor signal detection," *Proc. SPIE 11756, Signal Processing, Sensor/Information Fusion, and Target Recognition XXX*, 2021, p. 1175615.

[37] R. Kou, "OPERAnet: A Multimodal Activity Recognition Dataset Acquired from Radio Frequency and Vision-based Sensors," 2023.

[38] E. Lagunas, M. Najar, and M. Navarro, "UWB joint TOA and DOA estimation," *2009 IEEE International Conference on Ultra-Wideband*. 2009, pp. 839–843, IEEE.

[39] H. Li, X. He, X. Chen, Y. Fang, and Q. Fang, "Wi-Motion: A Robust Human Activity Recognition Using WiFi Signals," *IEEE Access*, vol. 7, 2018, pp. 153287–153299.

[40] H. Li, X. He, X. Chen, Y. Fang, and Q. Fang, "Wi-Motion: A Robust Human Activity Recognition Using WiFi Signals," *IEEE Access*, vol. 7, 2019, pp. 153287–153299.

[41] H. Li, K. Ota, M. Dong, and M. Guo, "Learning Human Activities through Wi-Fi Channel State Information with Multiple Access Points," *IEEE Communications Magazine*, vol. 56, no. 5, May 2018, pp. 124–129.

[42] Y. X. M. Li, "Atheros-CSI,", `https://wands.sg/research/wifi/AtherosCSI/`, 2015, Accessed on October 18, 2023.

[43] G. Lin, W. Jiang, S. Xu, and X. Zhou, "Human Activity Recognition Using Smartphones With WiFi Signals," *IEEE Transactions on Human-Machine Systems*, vol. PP, January 2022, pp. 1–12.

[44] G. Lin, W. Jiang, S. Xu, X. Zhou, X. Guo, Y. Zhu, and X. He, "Human Activity Recognition Using Smartphones With WiFi Signals," *IEEE Transactions on Human-Machine Systems*, vol. 53, no. 1, Feb. 2023, pp. 142–153.

[45] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 6, 2007, pp. 1067–1080.

[46] C. Ltd., "Ubuntu,", `https://www.ubuntu.com/`, 2023, Accessed on October 18, 2023.

[47] Y. Ma, G. Zhou, S. Wang, H. Zhao, and W. Jung, "SignFi: Sign Language Recognition Using WiFi," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, 2018, pp. 23:1–23:21.

[48] J. Machado Fernández, "Software Defined Radio: Basic Principles and Applications," *Revista Facultad de Ingenier'ia*, vol. 24, 01 2015, pp. 79–96.

[49] MathWorks, "WLAN PPDU Structure,", `https://www.mathworks.com/help/wlan/gs/wlan-ppdu-structure.html`, 2016, Accessed on November 8, 2023.

[50] Y. Mei, T. Jiang, X. Ding, Y. Zhong, S. Zhang, and Y. Liu, "WiWave: WiFi-based Human Activity Recognition Using the Wavelet Integrated CNN," *2021 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, 2021, pp. 100–105.

[51] B. Mitchell, "History of Wireless Standard 802.11a,", https://www.lifewire.com/history-of-wireless-standard-802-11a-816554, 2020, Accessed on October 18, 2023.

[52] M. Muaaz, A. Chelli, and M. Patzold, "WiHAR: From Wi-Fi Channel State Information to Unobtrusive Human Activity Recognition," *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, Antwerp, Belgium, May 2020, pp. 1–7, IEEE.

[53] M. Muaaz, A. Chelli, and M. Pätzold, "WiHAR: From Wi-Fi Channel State Information to Unobtrusive Human Activity Recognition," *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–7.

[54] openwifi, "Opensdr-Openwifi,", https://github.com/open-sdr/openwifi, 2022, Accessed on October 18, 2023.

[55] O. Project, "OpenWRT,", https://openwrt.org/, 2023, Accessed on October 18, 2023.

[56] proxicast, "ANT-120-008 3-6 dBi Omni-Directional 4G/5G/CBRS Terminal Antenna,", https://www.proxicast.com/shopping/index.php?dispatch=attachments.getfile&attachment_id=203, 2022, Accessed on November 8, 2023.

[57] Remcom, "Wireless em Propagation Software - Wireless Insite,", https://www.remcom.com/wireless-insite-em-propagation-software/, 2021, Accessed on October 18, 2023.

[58] E. Research, "UHD - USRP Hardware Driver,", https://www.ettus.com/sdr-software/uhd-usrp-hardware-driver/, 2023, Accessed on October 18, 2023.

[59] RTL-SDR Blog, "RTL-SDR,", https://www.rtl-sdr.com/, 2023, Accessed on October 18, 2023.

[60] K. Sabanci, E. Yigit, D. Ustun, A. Toktas, and M. F. Aslan, "Wifi based indoor localization: application and comparison of machine learning algorithms," *2018 XXIIIrd International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED)*. 2018, pp. 246–251, IEEE.

[61] K. Sabanci, E. Yigit, D. Ustun, A. Toktas, and M. F. Aslan, "Wifi based indoor localization: application and comparison of machine learning algorithms," *2018 XXIIIrd International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED)*. 2018, pp. 246–251, IEEE.

[62] H. Salehinejad and S. Valaee, "LiteHAR: Lightweight Human Activity Recognition from WIFI Signals with Random Convolution Kernels," *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Singapore, Singapore, May 2022, pp. 4068–4072, IEEE.

[63] M. Schulz, D. Wegemer, and M. Hollick, "Nexmon," *WiNTECH17*, Oct. 2017.

[64] M. Schulz, D. Wegemer, and M. Hollick, "seemoo-lab/nexmon,", `https://github.com/seemoo-lab/nexmon`, 2017, Accessed on October 18, 2023.

[65] J. Schäfer, B. R. Barrsiwal, M. Kokhkharova, H. Adil, and J. Liebehenschel, "Human Activity Recognition Using CSI Information with Nexmon," *Applied Sciences*, vol. 11, no. 19, Sept. 2021, p. 8860.

[66] S. Shang and L. Wang, "Overview of WiFi fingerprinting-based indoor positioning," *IET Communications*, vol. 16, no. 7, 2022, pp. 725–733.

[67] F. Shi, W. Li, A. Amiri, S. Vishwakarma, C. Tang, P. V. Brennan, and K. Chetty, "Pi-NIC: Indoor Sensing Using Synchronized Off-The-Shelf Wireless Network Interface Cards and Raspberry Pis," *2022 2nd IEEE International Symposium on Joint Communications & Sensing (JC&S)*, 2022, pp. 1–6.

[68] L. Smith, "Machine learning for wireless signal learning,", 2021.

[69] L. Smith, N. Smith, S. Kodipaka, A. Dahal, B. Tang, J. E. Ball, and M. Young, "Effect of the short time Fourier transform on the classification of complex-valued mobile signals," *Proc. SPIE 11756, Signal Processing, Sensor/Information Fusion, and Target Recognition XXX*, May 21 2021, p. 117560Y.

[70] N. Smith, L. Smith, S. Kodipaka, A. Dahal, B. Tang, J. E. Ball, and M. Young, "Real-time location fingerprinting for mobile devices in an indoor prison setting," *Proc. SPIE 11756, Signal Processing, Sensor/Information Fusion, and Target Recognition XXX*, April 12 2021, p. 1175612.

[71] N. G. Smith, "Radio Frequency Dataset Collection System Development for Location and Device Fingerprinting,", 2021.

[72] Steven M. Hernandez, "ESP32-CSI-Tool,", `https://github.com/StevenMHernandez/ESP32-CSI-Tool`, 2019, Accessed on October 18, 2023.

[73] Y. Sugimoto, H. Rizk, A. Uchiyama, and H. Yamaguchi, "Towards Environment-Independent Activity Recognition Using Wi-Fi CSI with an Encoder-Decoder Network," *Proceedings of the 8th Workshop on Body-Centric Computing Systems*, New York, NY, USA, 2023, BodySys '23, p. 13–18, Association for Computing Machinery.

[74] H. Tang, "DOA estimation based on MUSIC algorithm," 2014.

[75] L. Team, "Linino,", https://www.linino.org/, 2023, Accessed on October 18, 2023.

[76] C. Tian, Y. Tian, X. Wang, Y. H. Kho, Z. Zhong, W. Li, and B. Xiao, "Human Activity Recognition With Commercial WiFi Signals," *IEEE Access*, vol. 10, 2022, Received 13 October 2022, accepted 13 November 2022, date of publication 18 November 2022, date of current version 23 November 2022.

[77] C. Tian, Y. Tian, X. Wang, Y. H. Kho, Z. Zhong, W. Li, and B. Xiao, "Human Activity Recognition With Commercial WiFi Signals," *IEEE Access*, vol. 10, 2022, pp. 121580–121589.

[78] R. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*, Artech House, Inc., Norwood, MA, 2000.

[79] F. Wang, J. Feng, Y. Zhao, X. Zhang, S. Zhang, and J. Han, "Joint Activity Recognition and Indoor Localization With WiFi Fingerprints," 2023.

[80] F. Wang, W. Gong, and J. Liu, "On Spatial Diversity in WiFi-Based Human Activity Recognition: A Deep Learning-Based Approach," *IEEE Internet of Things Journal*, vol. 6, 2019, pp. 2035–2047.

[81] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and Modeling of WiFi Signal Based Human Activity Recognition," *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, 2015.

[82] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Device-Free Human Activity Recognition Using Commercial WiFi Devices," *IEEE Journal on Selected Areas in Communications*, vol. 35, 2017, pp. 1118–1131.

[83] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Device-Free Human Activity Recognition Using Commercial WiFi Devices," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 5, May 2017, pp. 1118–1131.

[84] S. K. Yadav, S. Sai, A. Gundewar, H. Rathore, K. Tiwari, H. M. Pandey, and M. Mathur, "CSITime: Privacy-Preserving Human Activity Recognition Using WiFi Channel State Information," *Neural Netw.*, vol. 146, no. C, feb 2022, p. 11–21.

[85] H. Yan, Y. Zhang, Y. Wang, and K. Xu, "WiAct: A Passive WiFi-Based Human Activity Recognition System," *IEEE Sensors Journal*, vol. 20, 2020, pp. 296–305.

[86] H. Yan, Y. Zhang, Y. Wang, and K. Xu, "WiAct: A Passive WiFi-Based Human Activity Recognition System," *IEEE Sensors Journal*, vol. 20, no. 1, Jan. 2020, pp. 296–305.

[87] J. Yan, C. Ma, B. Kang, X. Wu, and H. Liu, "Extreme learning machine and adaboost-based localization using CSI and RSSI," *IEEE Communications Letters*, vol. 25, no. 6, 2021, pp. 1906–1910.

[88] J. Yang, X. Chen, D. Wang, H. Zou, C. X. Lu, S. Sun, and L. Xie, "Deep Learning and Its Applications to WiFi Human Sensing: A Benchmark and A Tutorial," *ArXiv*, vol. abs/2207.07859, 2022.

[89] J. Yang, X. Chen, D. Wang, H. Zou, C. X. Lu, S. Sun, and L. Xie, "Deep Learning and Its Applications to WiFi Human Sensing: A Benchmark and A Tutorial," 2023.

[90] J. Yang, X. Chen, H. Zou, D. Wang, and L. Xie, "AutoFi: Towards Automatic WiFi Human Sensing via Geometric Self-Supervised Learning," 2023.

[91] Y. J. Yang Liu, Tiexing Wang and B. Chen, "Harvesting Ambient RF for Presence Detection Through Deep Learning," 2023.

[92] S. Yousefi, H. Narui, S. Dayal, S. Ermon, and S. Valaee, "A Survey of Human Activity Recognition Using WiFi CSI,", Aug. 2017, arXiv:1708.07129 [cs].

[93] S. Yousefi, H. Narui, S. Dayal, S. Ermon, and S. Valaee, "A Survey on Behaviour Recognition Using WiFi Channel State Information," 2017.

[94] S. Yousefi, H. Narui, S. Dayal, S. Ermon, and S. Valaee, "A Survey of Human Activity Recognition Using WiFi CSI," 2023.

[95] Yu Gu, Lianghu Quan, and Fuji Ren, "WiFi-assisted human activity recognition," *2014 IEEE Asia Pacific Conference on Wireless and Mobile*, Bali, Indonesia, Aug. 2014, pp. 60–65, IEEE.

[96] J. Zhang, F. Wu, B. Wei, Q. Zhang, H. Huang, S. W. Shah, and J. Cheng, "Data Augmentation and Dense-LSTM for Human Activity Recognition Using WiFi Signal," *IEEE Internet of Things Journal*, vol. 8, 2021, pp. 4628–4641.

[97] J. Zhang, F. Wu, B. Wei, Q. Zhang, H. Huang, S. W. Shah, and J. Cheng, "Data Augmentation and Dense-LSTM for Human Activity Recognition Using WiFi Signal," *IEEE Internet of Things Journal*, vol. 8, no. 6, Mar. 2021, pp. 4628–4641.

[98] Q. Zhang, H. Abeida, M. Xue, W. Rowe, and J. Li, "Fast implementation of sparse iterative covariance-based estimation for source localization," *The Journal of the Acoustical Society of America*, vol. 131, no. 2, 2012, pp. 1249–1259.

[99] A. Zhuravchak, O. Kapshii, and E. Pournaras, "Human Activity Recognition based on Wi-Fi CSI Data - A Deep Neural Network Approach," *Procedia Computer Science*, vol. 198, 2022, pp. 59–66, This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0).