# Thesis (In-Progress

Caden Keese

6th May 2025

# Abstract

# Contents

# Chapter 1

# Introduction

# Chapter 2

# Background

### 2.0.1 Quadrature Sampling (IQ Sampling)

To represent a signal digitally, it is necessary to decompose that signal into discrete values that can be captured and stored. A standard sampling method is Quadrature or IQ sampling. This method works because any sinusoidal wave can be created via the equation: $x(t) = I\cos(2\pi ft) + Q\sin(2\pi ft)$, where $I$ and $Q$ are the amplitudes, $f$ is the frequency, and $t$ is time. This sampling method is especially helpful with phase shift encoded data as signals recorded with this method can be plotted in Cartesian space in a way that shows how close the data is to the ideal phase and also the amplitude. T <Insert Diagram Here>

### 2.0.2 Backscatter Transmission

In wireless devices, data is transmitted by encoding it in a baseband signal centered around zero, which is then shifted up to a specific frequency by combining it with a carrier wave.

<Insert Diagram Here>

In traditional wireless devices, this carrier is internal and is responsible for a significant amount of the power draw required to transmit data [TODO CITATION (see notes)]. Backscatter is a wireless transmission method in which the transmitter modulates an external carrier wave to send data. The separation of carrier and transmitter enables this method to be used in situations that require low power, as the carrier can be power and located apart from both the transmitter and receiver.

<Insert Diagram Here>

### 2.0.3 IEEE 802.15.4 O-QPSK

The IEEE 802.15.4 standard defines a common physical layer (PHY) and medium access control (MAC) layer for low-power, low-data-rate wireless embedded systems. It is the basis for popular protocols like ZigBee and Thread. 802.15.4 defines multiple physical layer specifications with different frequency ranges and modulation schemes. the most common being 2.45GHz - O-QPSK option. The 802.15.4 packet structure has four necessary components: the preamble sequence (0x000000), the start of frame delimiter (0xA7), the payload frame length, and the payload.

The preamble sequence '0x000000' is useful for matching the start of the packet with non-standard receivers (TODO: link to USRP parsing impl).

To transmit each packet, every 2 bits of data are mapped to a 16-element chip sequence, where each chip corresponds to one of four signal phases, each separated

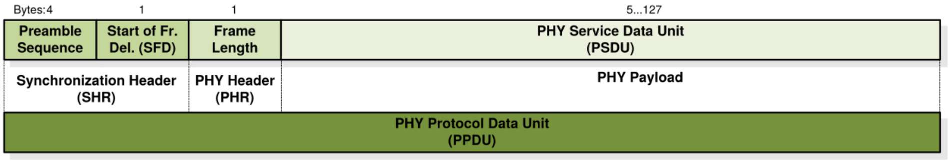

Figure 2.1: IEEE 802.15.4 Physical Protocol Data Unit (PPDU)

by 90 degrees. For the 802.15.4, the chip sequences correspond to a half-sine in the I and Q channels, where the Q signal is offset by half a wave. The Offset guarantees no transitions through the center, and the half-sine creates a signal with a constant amplitude. Figure 2.2 shows the difference in the constellations of Half Sine O-QPSK, O-QPSK, and QPSK visually.

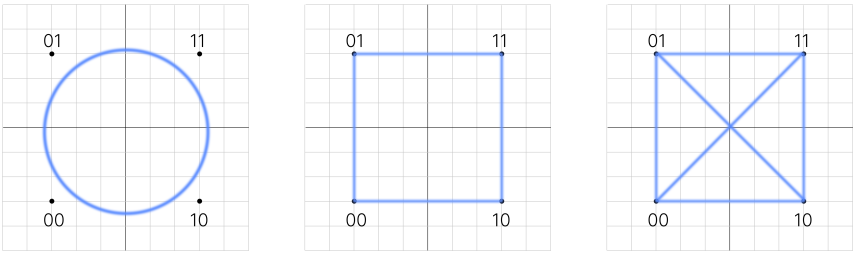

Figure 2.2: O-QPSK half-sine, O-QPSK, and QPSK Ideal Constellations

TODO: Copy over info about backscatter platform from notes
TODO: Explain the basics of classification

# Chapter 3

# Design

The EBP (TODO: better name) Fingerprinting System (EBPFS) comprises a constantly transmitting carrier device, an EBP, an IQ sampling receiver, a feature extraction pipeline, and a simple machine learning classifier trained on extracted features.

### 3.0.1 EBP Firmware design

The firmware to generate

# Chapter 4

# Implementation

5 antennas 5 picos 5 backscatter tag

pico / pio implementation

Packet identification

Filters

Half Sine Filter

# Chapter 5

# Evaluation

TODO

## Chapter 6

# Conclusions

TODO

# Bibliography