Ministry of Higher Education and Scientific Research
Saad Dahleb University – Algeria
Institute of Aeronautics & Space Studies

Department of Air Navigation
CNS/ATM

Academic Master's Degree Thesis

Passive geo-location of an immobile RF transmitter using RTL-SDR receiver in outdoor environment

Presented by: Kaiouche Amine

Major Professor: Dr. Rahmouni Mohamed

2020 – 2021

ملخص البحث

يركز البحث على استخدام جهاز استقبال RTL-SDR لتحديد الموقع الجغرافي لمرسل الذبذبات RF الغير متحرك ؛ يتطلب إجراء قياسات لشدة المجال التباعد الجغرافي وبرمجيات مناسبة؛
بالنسبة لمجموعات البيانات الملتقطة ، توفر الأطروحة ثلاث تقنيات تستند إلى معادلة إرسال فريس من اجل التنبؤ بمكان المرسل الغير متعاون في بيئة خارجية.
الهدف هو الحصول على تقدير تقريبي مناسب باستخدام تقنية غير مكلفة وبعض التحليلات العددية.

Research Summary

The research focuses on using an RTL-SDR receiver to geo-locate an immobile RF transmitter; the procedure requires geo-spaced field strength measurements and appropriate software.
For diverse gathered datasets, the thesis provides three techniques based on the Friis transmission equation to predict uncooperative transmitter position in outdoor environment.
The objective is to get a decent approximation utilizing inexpensive technology and numerical analysis.

Résumé de la Recherche

La recherche se concentre sur l'utilisation d'un récepteur RTL-SDR pour géo localiser un émetteur RF immobile
La procédure nécessite des mesures d'intensité sur le champ de propagation géo-espacé et un logiciel approprié
Pour divers ensembles de données recueillies, la thèse propose trois techniques basées sur l'équation de transmission de Friis pour prédire la position de l'émetteur non coopératif dans l'environnement extérieur.
L'objectif est d'obtenir une approximation décente en utilisant une technologie peu coûteuse et l'analyse numérique.

Data processing software: Matlab2015b

***Keywords**: Outdoor geolocation, radio-frequency transmitter, Received field strength, RF emitter, Approximation of signal source location, Low-cost RF geolocation*

Acknowledgements

I would thank God for giving me the courage and the patience to complete my studies, and to finalize this project successfully. Then, I will thank my parents, especially my mother "Kerdjadj Lynda", and my grandfather "Kerdjadj Slimane", for believing in me, and supporting me throughout my studies. I would not have been successful without them.

I would also like to thank my major professor, Dr.Rahmouni Mohamed, for trusting in my project concept and providing support through this experience. I'd also like to express my gratitude to all my professors during my academic years.

This project is dedicated to my Mother & to the memory of my Grandfather Slimane

---

Table of Contents

List of Abbreviations

ADC: Analog-to-Digital Converter
ATIS: Automatic Terminal Information Service
AOA: Angle-of-Arrival
AGC: Automatic Gain Control
AM: Amplitude Modulation
BNC: Bayonet-Neill-Concelman
CSV: Comma Separated Values
DSP: Digital Signal Processing
DC: Direct Current
DVOR: Doppler VHF Omni-directional Range
FFT: Fast Fourier Transform
FM: Frequency Modulation
GSM: Global System for Mobile Communications
GPS: Global positioning system
HD: High Definition
HF: High Frequency
IF: Intermediate Frequency
ICAO: International Civil Aviation Organization
I/Q: In-phase and Quadrature
IR: Infrared radiation
LNA: Low-Noise Amplifier
LSB: Lower Side Band
LF: low frequency
LOS: Line-Of-Sight
MF: Medium frequency
NOTAM: Notice to Air-Men
NLOS: Non-Line-Of-Sight
OTG: USB On-The-Go
PPM: Parts Per Million
RF: Radio Frequency
RTL: Register Transfer Level
RX: Receiver
RSS: Received Signal Strength
SDR: Software Defined Radio
SHF: Super High Frequency
SNR: Signal-to-Noise Ratio

TOA: Time-of- Arrival
TDOA: Time-Difference-of-Arrival
TV: Television
TX: Transmitter
UHF: Ultra-High Frequency
USB: Universal Serial Bus
UAV: Unmanned Aerial Vehicle
VHF: Very High Frequency
VLF: Very Low Frequency
VHDL: Verilog Hardware Description Language

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Overview

In electronics and telecommunications a radio transmitter or just transmitter is an electronic device which produces radio waves with an antenna. The transmitter itself generates a radio frequency alternating current, which is applied to the antenna. When excited by this alternating current, the antenna radiates radio waves.

Geolocation of radio frequency transmitter is becoming a necessity rather than a choice, it has a direct relationship with safety and surveillance.

The main purposes of geolocation are to find physical position of a device for locating unauthorized transmitter, perform radio tags tracking, and find people with radio emitters who transmit radio-frequency signal on private radio bands or in prohibited area. It can also find jammers position after doing signal processing procedure. Furthermore, identify and distinguish between legitimate radio emission and illegitimate one.

Radio frequencies are regulated and monitored by authorities to protect sensitive data and installations. Private companies and specialized organisations use sophisticated and expensive hardware as well as software implementation that's comes with to achieve an efficient surveillance level for different radio bands.

There are many mathematics axioms that support geolocation process, and give an interesting position estimation of RF transmitter, without using expensive hardware Some approaches handle adoption of Friis transmission equation in free space environment and have shown interesting results in other researches Even though, radio frequencies are affected by environment and the mechanism of electromagnetic propagation in real space like multipath distortion, distance power loss, wave's reflections.

The thesis focuses on received signal strength to determine the position of radio frequency transmitters with a known centred frequency.

Position estimation presents only longitude and latitude coordinates, elevation estimation needs additional equipment's and other approaches for a correct evaluation.
To achieve measurements task, only one RTL-SDR dongle (28MHZ-1700MHZ) is available, simulation with random data on MATLAB is required for algorithms adjustments. In addition to adapt some published algorithms from other researches to our measurements. VHF band is privileged for data collection to consider attenuation certainly in small area. Two transmitters are selected, DVOR station and ATIS broadcast transmitter of (Houari Boumediene airport) to collect real data using RSS approach. Moreover, transmitter's coverage area are carefully inspected before starting the experience to avoid ambiguity. The signals are noisy and affected by ground obstacles, which creates many variations in received power from selected stations. Aeronautical transmitter in general are made for air reception purposes. But it is possible to receive RF signals on ground scale when the receiver position's is near to the transmitter, and the any broadcast from stations could be easily recognizable when listening to radio diffusion for each station
This introduction serves as a presentation of the basic ideas and concepts that have fuelled this research

1.2 Problem definition

Detect radio frequency transmitter could be a huge challenge because of encountered ground obstacles, topography and the proprieties of electromagnetic waves propagation in real space, especially if the hardware used is inadequate.

Geolocation with a higher accuracy is needed to provide location-related services in communications, the development of an efficient method to do so is not easy, the progress of technology in radio field and the large access to electronics components by public may be a disadvantage sometimes when used to design local transmitters that interfere with official allowed radio frequency band on a precise frequency

Transmitting data in unauthorized area could be a national security concern, people who broadcast randomly and choose any frequency they want without permission, should be detected and tracked to comply with local regulations, the presence of jammers occupy allocated frequency band and interferes with data transmission on different channels may shutdown authorized services in that area, and prevented them from operating ….etc.
As we can see there is a lot of embarrassing situations noted when radio frequencies are not regulated and correctly monitored.

1.3 Objective

The basic purpose of the thesis is to develop and adapt some already published algorithms to our local area, test capability of algorithms proposed and compare between results after data processing. Associate mathematical computations to a real world experience. Finding an acceptable position estimation of immobile transmitter without using expensive hardware, opens the doors for other researches that determines locations of mobile transmitters Avoid any kind of cooperation with transmitter station, aid to geolocate a hostile transmitter with only a known active centered frequency Determine the impact of loss coefficient for different propagation models inside the area of interest. Comparing results between methods for different datasets. Deduce methods performance in outdoor environments corresponding to data collected.

1.4 Literature overview

1.4.1 Definition of electromagnetic propagation

The use of electromagnetic waves for transmitting information is attractive, in part, because direct physical connections such as wires or cables are not required. This advantage gave rise to the terms "wireless telegraphy" and "wireless telephony" that were commonly used for radio in the early part of the past century and have returned to popular usage with the widespread development of "wireless" systems for personal communications in recent decades.

Electromagnetic waves are utilized in many engineering systems: long-range point-to-point communications, cellular communications, radio and television broadcasting, radar, global navigation satellite systems, and so on. The same considerations make electromagnetic energy useful in "sensors", systems that obtain information about regions from which transmitted energy is reflected. Electromagnetic sensors can be used for detecting hidden objects and people aircraft control, anti-collision detection and warning systems, for measuring electron concentrations in the Earth’s upper atmosphere and in planetary atmospheres in general, the wave state of the sea, the moisture content of the lower atmosphere, soils, and vegetation, and in many other applications

In most cases, it is possible to divide the complete system, at least conceptually, into three parts. The first is the transmitter, which generates the electromagnetic wave in an appropriate frequency range and launches it toward the receiver, the second is the region sensed between transmitter and receiver. The last is the receiver, which captures some fraction of the energy that has been transmitted or scattered from the medium being sensed for extracting the desired information.

Propagation is the intervening process whereby the information bearing wave, or signal, is conveyed from one location to another. In communications, propagation is the link between the transmitter and the receiver, while for sensors, propagation occurs between the transmitter and the target to be sensed and between the target and the receiver.

1.4.2 Propagation mechanisms of radio waves

A radio wave propagates without encountering any obstacle in free space. The surface of the wave is the set of all points reached at a certain time after the moment of emission of the wave. The attenuation in free space comes from the scattering of energy that occurs when the wave propagates away from the transmitter.
In real space, the excess attenuation compared to free-space attenuation is defined as the difference between the path loss and free-space attenuation like atmospheric absorption, building penetration loss, vegetation attenuation, attenuation due to diffraction…etc.).
Reflexion occurs when a propagating wave impinges upon a surface with large dimensions compared to the wavelength. Generally radio waves are reflected at different surfaces in this case, a distinction is commonly drawn between specular reflections, occurring in the presence of a perfectly plane, homogeneous surface, and the broadcast.

1.4.2.1 Direct propagation

The simplest mechanism is perhaps direct propagation, involving the travel of the signal directly from the transmitter to the receiver quite unaffected by the intervening medium. It assumes the form of a spherical wave emanating from the transmitter. Since the receiver is often sufficiently far away from the transmitter, this wave can be approximated as a plane wave at the receiver location. Direct propagation may seem to be a highly idealized situation, but it has important applications. For frequencies in the UHF and higher frequency bands, the ionosphere has little influence, essentially because the electrons responsible for its conductivity at lower frequencies are unable to follow the rapid variations at such high frequencies. Also, at higher frequencies it is possible to build very directive antennas, so that the signal beam may be kept isolated from ground effects except maybe at the end point of its intended path, if this is very close to the ground

Under these conditions, the signal propagation is mostly unaffected by ground or sky effects. Since most radars and satellite communications systems operate in this way, and because a narrow beam is also advantageous for separating a particular radar target from its surroundings, direct propagation is the dominant mechanism, and sometimes the only one to be considered, for many microwave radar and satellite communications calculations. The frequency spectrum for direct propagation is not open ended at the higher frequency end, however, because then a band of frequencies in the upper SHF range and above is reached in which atmospheric constituents are able to absorb energy efficiently. In this range, the direct propagation assumption must be modified to account for this absorption by the inclusion of an additional attenuation term.
As frequency is increased even further, the wavelength decreases until it becomes of the order of magnitude of atmospheric dust and water droplet particles.
As a result, these particles can scatter or absorb the signal quite strongly, which requires further modification of the propagation model.
In short, direct propagation is the appropriate mechanism to consider only when all other mechanisms are inoperative, a situation most frequently encountered in the atmosphere at UHF and SHF with systems utilizing highly directive antennas and when the transmitter and receiver are in direct line of sight with respect to one another at elevation angles that preclude ground effects. The effect of gravity causes the atmosphere to be generally more dense and moist at lower altitudes than at higher ones. Though the effect is small, it causes a significant bending of the propagated signal path under many conditions. For example, in the design of microwave links that are sometimes used for long-distance telephone voice and data communications, care must be taken that the link will perform adequately for a variety of atmospheric conditions that may cause the beam to bend upward or downward. This bending is known as tropospheric refraction. The atmospheric effects that cause tropospheric refraction also cause time delays as signals propagate through the atmosphere; such time delays have a significant impact on systems used for global navigation such as the GPS.

1.4.2.2 Ducting

The bending effect of tropospheric refraction may be strong enough to cause signals to follow closely along the curvature of the Earth, so that they are in effect guided along the Earth. Such behavior is called ducting. Ducts are most frequently observed at VHF and UHF; they also exist at higher frequencies but the more directive antennas employed at these frequencies are less likely to couple efficiently into a duct. Ducting is much more common at some localities than others since it is closely related to meteorological phenomena. In most areas of the world, it is a source of potential interference rather than a means of reliable communication.

1.4.2.3 Earth reflections

When antennas used are not very directional, or if they are located near the ground, signals may travel from the transmitter to the receiver by reflection from the ground In this case, both the directly propagated signal and the ground reflected signal must be considered in evaluating the propagation performance of a system A typical case is ground-to-air or air-to-air communication at UHF The size limitation of aircraft antennas makes it impossible to use highly directive antennas in this frequency regime, so it is not possible to keep signals from reaching the ground. The ground reflected signals can be added to or subtracted from the directly propagated signal constructive or destructive interference, respectively, so both terms must be considered.

1.4.2.4 Terrain diffraction

All the mechanisms considered thus far can be described using the concept of rays that is energy traveling along straight or nearly straight paths. Therefore, these propagation mechanisms would allow no signal transmission when the transmitter and receiver are not within the line of sight.
However, such transmission is still possible, and the reason becomes apparent when diffraction is taken into account. Diffraction by the Earth's curvature itself is important, but even more pronounced is the effect of sharper obstacles, such as mountains. These obstacles scatter energy out of the incident beam.

1.4.2.5 Multipath environments

In many cases, it is possible for transmitted signals to reach a receiver by multiple reflection or diffraction paths instead of a single reflection from the Earth's surface or single diffraction point from the terrain. When many time-delayed and distorted copies of a transmitted signal are received, the term "multipath environment" is used to describe the propagation mechanism Multipath is usually an important factor for ground-based point to point links, especially in urban environments, and must be considered, for example, in the design of wireless cellular communications and data networks. Because the consideration of multiple paths between the source and the receiver can become very complex. In recent years have seen extensive efforts in developing communications modulation and signal processing strategies to combat the impact of multipath fading effects.

1.4.2.6 Ground wave

When both the transmitting and receiving antennas operate near or on the ground, it is found that the direct and reflected waves cancel almost completely. In this case, however, one also finds that a wave can be excited that travels along the ground surface, one of several types of waves denoted as "surface waves " Since efficient transmitting antennas at MF and lower frequencies are necessarily large in size since the wavelength is long, they are generally positioned close to the

ground, and ground wave propagation becomes important at these lower frequencies. Ground wave propagation is the dominant mechanism for standard local radio broadcast transmissions; it is usually not an important mechanism at frequencies above the HF band.

1.4.2.7 Ionosphere reflections

In the MF and HF bands, electromagnetic signals can be well described in terms of rays that are reflected by the ionosphere and the ground, rays are bent rather than sharply reflected in the ionosphere, but the net effect is essentially the same. Signal transmission by this means can be very efficient, and great distances can be spanned with modest power and equipment. For this reason, "short-wave" bands, as these frequencies are often called popularly, are utilized for broadcasting, point-to-point communications, and amateur radio. Depending on the signal frequency, the reflection can occur in different layers of the ionosphere. In the VLF and LF parts of the spectrum, the ionosphere and the Earth may be considered, respectively, as the top and bottom of a waveguide that guides energy around the Earth This point of view is particularly useful at the lower end of these frequencies, because then the wavelength is pitching that the spacing of the "waveguide walls", that is, the Earth's surface and the effective ionospheric region, is on the order of a wavelength, and the mode description becomes relatively simple for calculation. It is not quite correct to distinguish between ionospheric reflection and waveguide modes as different physical mechanisms, in both cases, the signal is guided between the Earth and the ionosphere. However, if the wavelength is sufficiently long, it is more convenient to treat the problem in terms of waveguide modes. If the wavelength is very short compared to the Earth-ionosphere spacing, the ray picture becomes more convenient, and one treats the problem as a series of reflections. In between, in the LF region, computations by either technique become difficult. The distinction between ionospheric hops and waveguide modes is based more on the mathematical description employed than on the actual physical process itself

In addition to apparent reflections or guiding of signals, the ionosphere can also cause important effects on higher frequency systems up to about 3 GHz on Earth

to-space paths. Electromagnetic waves propagating through the ionosphere can experience time delays as in tropospheric propagation, polarization rotation, and scintillation effects. [1]

1.4.3 VHF waves characteristics

Radio waves in the VHF band propagate mainly by line-of-sight and ground-bounce paths; unlike in the HF band there is only some reflection at lower frequencies from the ionosphere in skywave propagation. They do not follow the contour of the Earth as ground waves and so are blocked by hills and mountains, although because they are weakly refracted by the atmosphere they can travel somewhat beyond the visual horizon out to about 160 km. They can penetrate building walls and be received indoors, although in urban areas reflections from buildings cause multipath propagation, which can interfere with television reception. Atmospheric radio noise and interference from electrical equipment is less of a problem in this and higher frequency bands than at lower frequencies. The VHF band is the first band at which efficient transmitting antennas are small enough that they can be mounted on vehicles and portable devices, so the band is used for two-way land mobile radio systems, such as walkie-talkies, and two way radio communication with aircraft (Air band) and ships (marine radio). Occasionally, when conditions are right, VHF waves can travel long distances by tropospheric ducting due to refraction by temperature gradients in the atmosphere.

- Frequencies range from 30 to 300 Mhz
- Wavelength (lambda) from 1 to 10 m
- Atmospheric influence like refraction and reflection due to irregularities of refractive index, ionospheric scatter and scintillations, Faraday rotation.
- Screening effects due to topography like mountains, diffraction inside valleys, ground and sea surfaces enhance multipath propagation.
- Radio diffusion could reach 160 km.
- Used in mobile communication, and aeronautical radio navigation beacons.

1.4.4 Geolocation

Geolocation is a process of determining the physical position of electronic device. Radio Frequency based localization utilizes properties of RF signals to determine the location of an RF device.

The localization process of a transmitter requires three or more stations to collect enough information for computing a good position estimation.

There is various localization methods, but each one comes with its own accuracy and cost. Some geolocation method are described below.

- Angle-of-Arrival (AoA)

The method use angle calculation which demands angle calculation of which direction of the signal is received from, and then perform triangulation for this node.

- Distance-based ranging

The method uses a known trilateration algorithms to determine the node's location.

- Time-of- Arrival (ToA)

The method calculates distance between the anchor node and the unknown node by determining how much time is required for signal to travel between them It requires high precision of time and synchronization to determine the time travel of the signal moving at the speed of light.

- Received Signal Strength (RSS)

The method is based on measurements to show the condition of received power in the anchor nodes and it is used in most of the wireless communication standard the received indicators demonstrates the size of electromagnetic wave energy in a media received by antenna in our sensor nodes.

- Time-Difference-of-Arrival (TDoA)

The method measures the difference of propagation time between two different signals in terms of their nature, such as using radio frequency or ultrasonic signal [3].

1.5 Received Signal Strength (RSS)

The method is the most economical to perform ranging-based localization, it does not need additional apparatus as said earlier. Every radio frequency chipset has RSS indicator. These indicators lacks the high accuracy of other range based methods due to signal deterioration caused by fading, so measurements in real space are considered as a non-ideal. To overcome this inferior accuracy problem, high number of indicators data readings is needed and taking into account that measures should be geographically separated, along with some data enhancement methods, to achieve comparable accuracy.

The received power of a radio frequency signal decreases conforming to some certain formula and by knowing the terms of this formula, we can deduce how far the signal has traveled from the transmitter to reach this certain received power at the receiver. Global Positioning System can be a solution for an accurate outdoor localization, simply with a smartphone.

In recent years, researchers are interested in improving the accuracy of localization with low cost technology that would last long in terms of weariness and battery life

The received signal strength method uses indicators pins found on many radio frequency receiving devices for locating an unknown transmitter. This pin allows the receiver to report the strength of the signal to whatever device is attached to it, and can in turn be used to help locate position of an RF emitters using Friis transmission equation. That can be exploited to retrieve distance from the transmitter if the transmitted power (P_t) and transmitter gain (G_t) are known .In practice this can be difficult as the transmitter power and gain are not always known quantities, fortunately there is some mathematical models that simplify the equation.

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2}$$

This equation can be solved to give a distance, d, for a single receiver from a given transmitter, where λ is the wavelength of the signal carrier. This range gives a radius of possible locations around the receiver on which the transmitter may be

located. Given multiple receiving antennas, the transmitter can be located on the intersection of all of these radii. This method is one of the simplest to implement because it does not require specialized hardware nor extensive calculation. Unfortunately, this method is also vulnerable to problems with multi-path fading and reflection from surfaces around the transmitter or receivers, and is especially inaccurate inside buildings [4].

1.6 Note on NLOS/ LOS

Due to the unknown propagation parameters, the challenge of RSS ranging in NLOS is exacerbated by the fact that obstructions between the transmitter and receiver can further complicate the distance–power relationship, making it difficult to estimate directly the distance accurately.

For example, let's consider a mobile station moving away from a base station in a typical direct LOS environment. The path loss model for this scenario is a typical LOS propagation model with path loss exponent around 1 or 2 and minimal shadowing variance However, as the mobile moves behind obstacles, the power suddenly fluctuates and severe attenuation perturbs the LOS distance–power relationship It then becomes very difficult to achieve accurate distance estimation in light of this problem. As a result, numerous research efforts have focused instead on an alternative RSS-based localization technique, namely fingerprinting-based localization.

In NLOS environments the path loss model will be significantly different when considering the type and number of obstructions separating the transmitter and receiver.

It is clear that, in practice, it is very difficult to have an accurate path loss model that can be used to estimate the distance accurately for all the environments.

VHF signals tend to bounce a lot and they are known as 'line of sight' frequencies. This means the receiving antenna must have a good unobstructed straight line between the transmitter and antenna. UHF signals are even more 'line of sight' [4]

1.7 Thesis Organization

The thesis present three geolocation methods related to RSS real world measurements and simulated data.

Chapter 2 presents hardware used and methodology, followed by real and simulation data utilized as input arguments. Chapter 3 demonstrates binary decision classification method based on designing a virtual grid probability, followed by its algorithm. A simulation for all datasets is practiced using a computer. Chapter 4 presents geometric circles method, it is based on circles multi-iterations idea, then, the algorithm that's goes with and final results.

In chapter 5, Newton Raphson iterative method described & adapted for transmitter position estimation with constant loss coefficient, equals to 2. Chapter 6 presents a comparison between various methods as well as a general conclusion of this study, its results and suggests future work.

Chapter 2

Methodology

2.1 RTL-SDR dongle

RTL-SDR is a low-cost software defined radio which is based on mass produced Digital HD TV USB receiver dongles with Realteck RTL2832U chip in them. It was discovered in 2012 by hardware hacker Eric Fry, Linux driver developer Antti Palosaari and Osmocom team who were developing their own SDR. The RTL2832U chip had a special mode, the chip allows transferring the raw I/Q samples to the host which enabled it to be used as a general wideband SDR.

In digital circuit design, RTL stand for **register transfer level**, it is a design abstraction that represents a synchronous digital circuit in terms of the flow of digital signals data between hardware registers, and the logical operations performed on those signals. Register-transfer-level abstraction is used in hardware description languages like Verilog and VHDL to create high-level circuit representations, from which lower-level representations and ultimately actual wiring can be derived. Design at the RTL level is typical practice in modern digital design.

SDR stand for **software defined radio**, it is a radio communication system where components that have been traditionally implemented in hardware for example mixers, filters, amplifiers, modulators detectors, etc. The components are instead implemented by means of software on a personal computer or embedded system. The system is equipped with a sound card, or other ADC converter, followed by some sort of RF front end (Rf Filter, Rf Amplifier, Mixer, Local Oscillator)

Large amounts of signal processing are handed over to the general-purpose processor, rather than being done in special-purpose hardware electronic circuits. Such a design produces a radio which can receive and transmit widely different radio protocols (sometimes referred to as waveforms) based entirely on the software used.

Figure 2 1: RTL SDR dongle with Chip RTL2832 used for real data collection

2.1.1 RTL-SDR dongle technical specifications

- 25-1760 MHz tunable range.
- 3.2 MHz max bandwidth (~2.8 MHz stable).
- 8-bit ADC giving a little under ~50 dBs of dynamic range.
- < 4.5dB noise figure LNA.
- 75 Ohm input impedance.

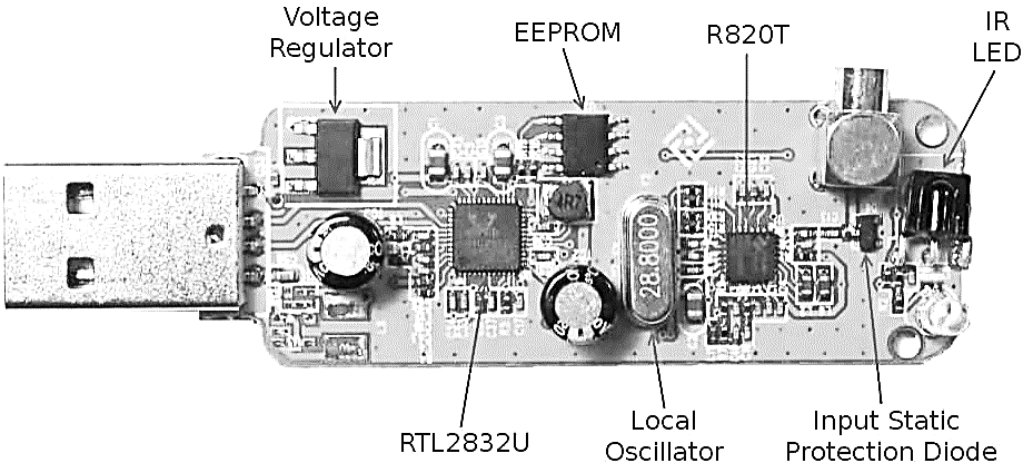


Figure 2.2: RTL SDR dongle with RTL2832 chip circuit board [5]

2.1.2 RTL-SDR ADC

ADC is an acronym for (Analogue to Digital Converter). It is a microchip that reads in an analogue signal and then digitizes it. The more bits an ADC has, the more accurate the digitization can be. For example an 8-bit ADC can scale the analogue input voltage range into values between $-V_{in} = -127\ mV$ and $V_{in} = +127mV$.

The disadvantage of using a low bit ADC is some small details in the analogue input, like weak signals may be lost during digitization, especially when there are strong and weak signals nearby.

The RTL-SDR dongle has an 8-bit ADC, which is clearly low, but just large enough for adequate performance for the data collection.

Dynamic range is the range between the largest and smallest possible values. The dynamic range of an ADC can be calculated approximately with: *(number of bits) * 6 dB*. This gives the RTL-SDR approximately

48 dB of dynamic range. However, the dynamic range may be improved slightly by using an oversampling method when using a computer compatible programs

2.1.3 RTL-SDR bandwidth

The bandwidth is the size of the real time frequency spectrum represented at any one time.

The maximum bandwidth of the RTL-SDR is 3.2 MHz, however the largest stable bandwidth is either 2.4 MHz or 2.8 MHz depending on the device used, and this is enough to realize the experience.

Most RTL-SDR compatible software let us choose the bandwidth which is sometimes referred to as sample rate as well. Although the sample rate and bandwidth are not the same thing, in the RTL-SDR setting the sample rate to 2 Msps (Mega Samples Per Second) will give 2 MHz of bandwidth; this is because the RTL-SDR uses I/Q sampling, where two ADCs are used, one for the minus part from the DC offset and one part for the positive part of the DC offset

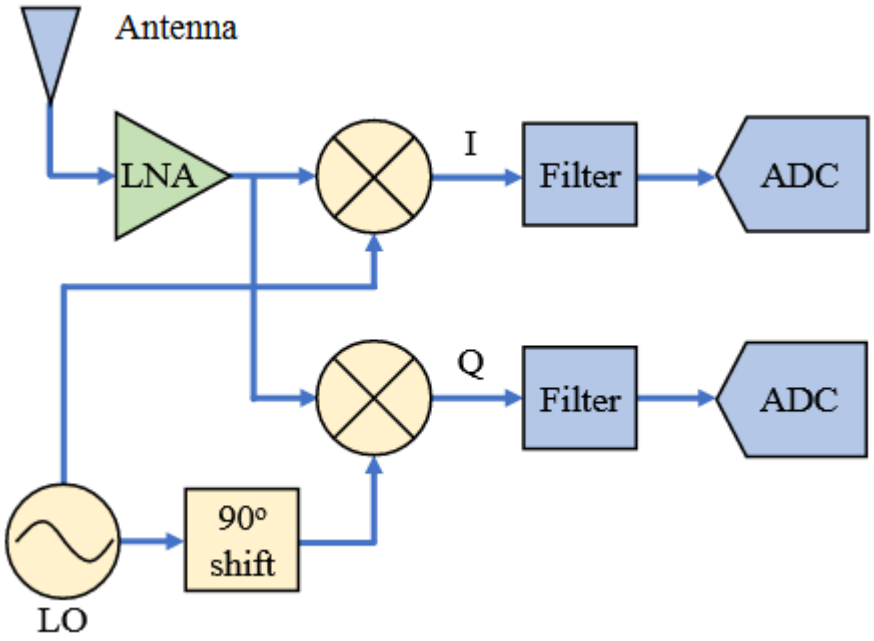


Figure 2.3: Q/I Direct conversion with zero IF

When the signal is received by the antenna, and transformed into IQ values, the dongle samples I and Q branches individually, using two analog-to-digital converters, and then combines the pairs and stores them as complex numbers. In other words, at each time step, it will samples one I value and one Q value and combines them in the form $I + jQ$ with one complex number per IQ sample There will always be a "sample rate", the rate at which sampling is performed
ADC requires analogue filtering on the input in order to prevent aliasing happening inside it.

Identifying the highest frequency component is needed especially for large bands, then doubling it, to make sure we sample at that rate or faster. The minimum rate in which we can sample is known as the Nyquist Rate. In other words, the Nyquist rate is the minimum rate at which a finite bandwidth signal needs to be sampled to retain all of its information. It is an extremely important piece of theory within DSP and SDR that serves as a bridge between continuous and discrete signals
Most receivers in general filter out everything above frequency sampling/2 right before the sampling is performed. If we attempt to receive a signal with too low

sample rate, that filter will chop off part of the signal. The SDRs go to great lengths to provide samples free of aliasing and other imperfections.
In digital signal processing, when reducing the bandwidth, the dynamic range increases. Bandwidth is related to the sample rate of the ADC. The dongles run at a high rate (for these measurements, 1.536 million 8-bit samples per second. That means they can receive a bandwidth of up to 1.536 MHz).
When we don't need that much bandwidth, we can decimate the data stream — throw away samples to reduce the rate. This reduces the processing workload, but it also has a notable result, each time decimating by four, we gain one bit that about 6 dB of dynamic range.
So, assuming we start with an 8 bit stream at 1.536 Msps, if we decimate by 8 to get 192 Ksps (and a 192 kHz RF bandwidth), we gain 2 bits, or 12 dB, of dynamic range.

2.1.4 Input impedance

RTL2832U dongles have an input impedance of 75 Ohms Most amateur and professional radio equipment runs on 50 Ohm cabling, connectors and adapters
Its look like this impedance mismatch will be a problem, however the signal loss due to the mismatch is minimal, equating to less than 0.2 dB.
In this research, the antenna used is directly connected to the dongle connector, to avoid additional signal loss by coaxial cable.

2.2 Software Defined Radio basic theory

A software defined radio simply works by receiving an analogue radio signal with an antenna and then using an ADC to digitize the signal. The digitized signal can then be worked on in digital signal processing software on a standard computer.
The total process is that the signal is received by an antenna, amplified with an internal LNA, mixed by the tuner, filtered to removed aliases, amplified again enough for the ADC to be able to read the signal and then digitized with the ADC
Once digitized the digital I/Q data is sent over USB into the computer where signal processing algorithms are used to demodulate and/or decode the signal

At any one time, SDR receives and processes samples of RF spectrum, for example 2 MHz worth of bandwidth, or more for more advanced SDR's. Within this sample of bandwidth there may be many signals. The software digital signal processing handles the tuning of individual signals within this element of bandwidth.
Briefly, the antenna receive entire analogue spectrum, then the SDR digitalizes a section of it that depends on SDR's bandwidth, after that the digitalized sample is delivered to a computer running DSP software that uses a digital IF filter algorithm to extract only the output signal that we want to study.

2.3 Configuration setup for data collection

2.3.1 Range

The dB level range shown on vertical axis in the radio frequency spectrum window is adjusted to maximum possible (figure 2.4), this so that the noise floor sits near the bottom of the RF spectrum window. This allows signals to be more visible in the FFT RF spectrum and waterfall displays The RTL-SDR has a dynamic range of approximately 50 dB
When using manual gain without any additional equipment added to the dongle
The maximum range in RF analyzer application is (-50dB).

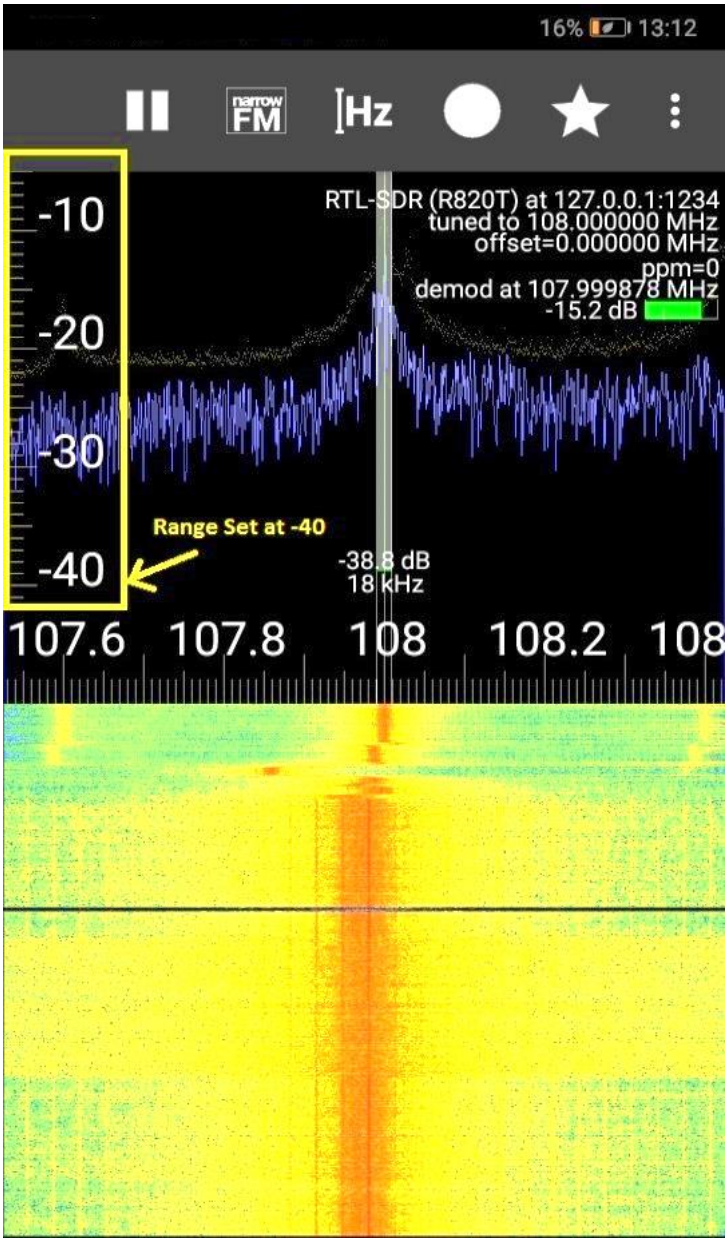


Figure 2.4: Range set illustration on RF analyzer

2.3.2 Offset

Adds an offset to the dB level range in the RF spectrum window. The offset is added to the top value on the dB level range in the RF spectrum. Usually there is no need to adjust this, it can mislead the amount of signal variation This setting will also affect the contrast in the waterfall and may help make weak signals easier to spot but in this research observing the variation of signal strength is mandatory for the experiment.

2.3.3 Frequency Correction (PPM)

Frequency stability is the specification used in many of the RF systems, RF oscillator, RF synthesizer, RF transceiver. In simple test set up it is measured using frequency counter. There are two types of frequency stability, short term and long term. Both are specified in terms of ppm. As it is mentioned in ppm often it is desired to convert the ppm to the Hz unit. ppm basically represents part of the whole number which will have units of the value 1/1000000.
The PPM formula represented below

$$Frequecny\ (Hz)\ = \frac{Frequency\ (PPM) * Rf\ carrier\ Frequecny\ (Hz)}{10^6}$$

The parameter allows as to correct the frequency offset that RTL-SDRs have from having low quality crystal oscillators.

2.3.4 Radio frequency Gain

There are three RF gain settings that can be found by clicking on (configure) button. RTL AGC turns on the RTL2832U chips internal automatic gain control AGC algorithm. Tuner AGC enables the RTL-SDR tuners AGC is disabled. The AGC's attempt to automatically optimize the SNR of the signals. Finally, the gain slider can be used to manually set the RF gain.

The manual gain control optimize the gain of a signal, however for casual browsing turning on Tuner AGC may suffice. RTL AGC is almost never used as it tends to just introduce a lot of unwanted noise and degrades reception quality, despite of that I have used manual value. So. RTL AGC is disabled.
When manually adjusting the RF gain, the aim is to get the highest signal-to-noise ratio as high as possible. This means that while the maximum signal strength should be significant, the noise floor should be kept as low as possible

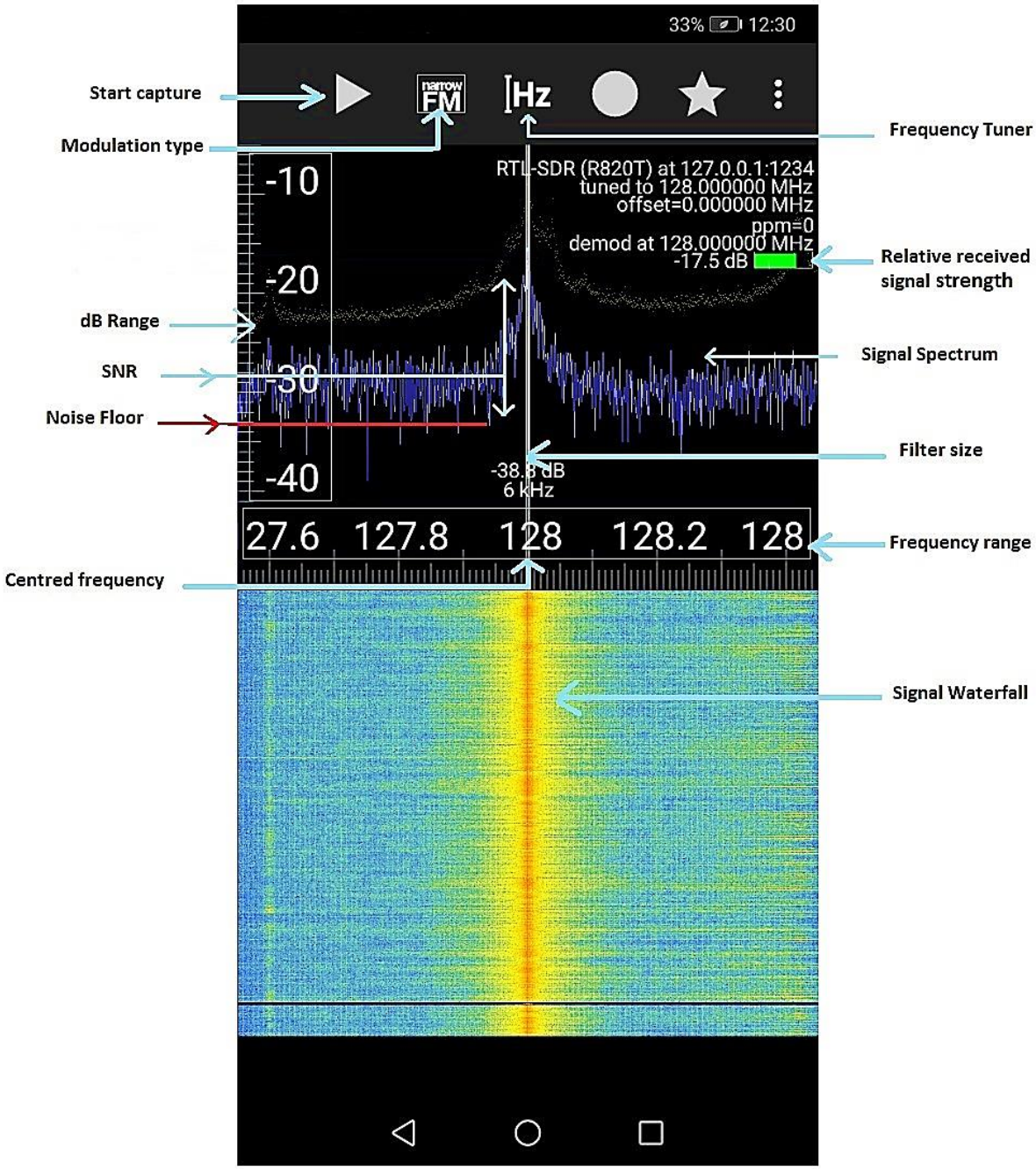


Figure 2.5: General illustration of RF analyzer android application

When increasing the gain, there will comes a point at which the noise floor begins to rise faster than the signal strength rises This is the reference point to stop increasing the gain

The signal peaks values are different from signal to noise values, the thesis focus on signal peaks values.

$$SNR\ value\ =\ Signal\ peak\ value\quad Noise\ floor\ value$$

In order to get a maximum reading of signal peak value, RF gain is set to a value that gives a maximum dynamic range, to observe clearly variation of signal strength when changing location and moving away from the transmitter in small area.

2.3.4 Low Noise Amplifier

The amplifier used in the dongle is while considered poor quality. However there are third party external LNAs that can be used to improve the signal quality. A poor amplifier inside RTL-SDR dongle with a noise figure of <4.5dB will introduce noise causing the signal to be degraded, especially when gain increased. The term noise figure is used to measure the amount of noise an amplifier will introduce into the signal. By using a high quality LNA with a noise figure <1dB this noise can be reduced. In this study, only integrated LNA that's comes with the dongle is used [5].

2.3.5 Antenna

The RTL-SDR packages come with a small single length antenna Some manufacturers provide a telescopic antenna instead, in this study I have used a monopole telescopic antenna which is much better that the single length whip. The extended length is 45 cm, can be used for portable radio scanner, VHF/UHF wireless system, digital TV.

Figure 2.6: Telescopic Antenna with BNC Connector, Max Length: 45cm

2.4 Data collection method

The RTL-SDR dongle is connected to a compatible android phone by OTG adapter from one side and to the telescopic antenna in the other side, antenna length is 45 cm during the experience. The phone attached to RTL-SDR dongle is fixed to a car phone holder support, the antenna position is approximately 90° to horizontal plan and positioned outside of the car from the window.

On phone side, SDR driver dedicated for RTL2832U chip by Martin Marinov is installed as well as RF Analyzer application by Dennis Mantz The application allows modifying different settings, displays signal spectrum and signal strength variation. The application has many features like browse the signal spectrum by scrolling horizontally, zoom in and out, both horizontally and vertically, automatic re-tune while scrolling and zooming, auto scale the vertical axis, jump directly to a frequency chosen, adjust the gain settings of the HackRF / RTL-SDR dongle, select a pre-recorded file as source instead of a real HackRF, change the FFT size, change FFT drawing mode: Line or Bars, waterfall color maps, peak hold, averaging, setting the frame rate either to a fixed value or to automatic control, activate logging and showing the log file, demodulate narrow FM, wide FM, AM,

LSB and USB with adjustable filters, adjust channel width, change the proportion of spectrum and waterfall, record the raw IQ samples to a file and select files as source, Select a fixed frequency shift [6].

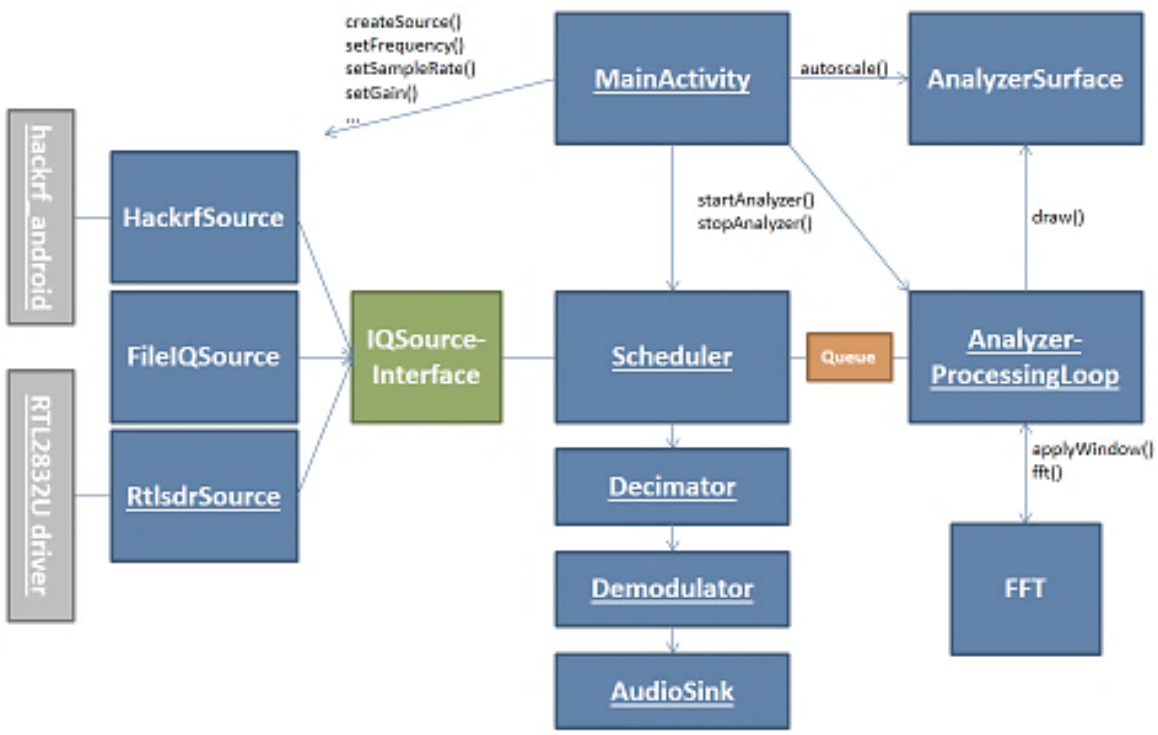


Figure 2.7: Rf Analyzer android application data collection scheme [6]

The signal strength values are unstable and fluctuate frequently. Then, for each three displayed values. I have selected only one value, the variation range is about 3 dB. The variation is caused by obstacles, metallic reflective surfaces and hardware heat inside dongle, in addition to the moving state of the car when collecting data which change environment conditions commonly

First transmitter frequency is set, after that, me and the professor started the experience by moving to different waypoints, assuming that the receiver is always inside transmitter's the coverage area.

Another android application operates on another phone for GPS tagging, the application named (GPS Logger) It is from (Basic Air Data) company, designed to collect different waypoints longitude, latitude and altitude information, then associates that data to the field strength measured by RF analyzer.

2.4.1 Dataset-A

First transmitter of interest is ATIS transmitter from Houari Boumediene airport. It is a continuous broadcast of recorded aeronautical information in airports and their immediate surroundings. ATIS broadcasts contain essential information, such as current weather information, active runways, available approaches, and any other information required by the pilots, such as important NOTAMs. Pilots usually listen to an available ATIS broadcast before contacting the local control unit, which reduces the controllers' workload and relieves frequency congestion
The data was collected on daytime between 10:30 AM and 12:00 AM on 03/06/21, the weather conditions was fine, the sky was partially covered and the temperature around Algiers city was 29°C.

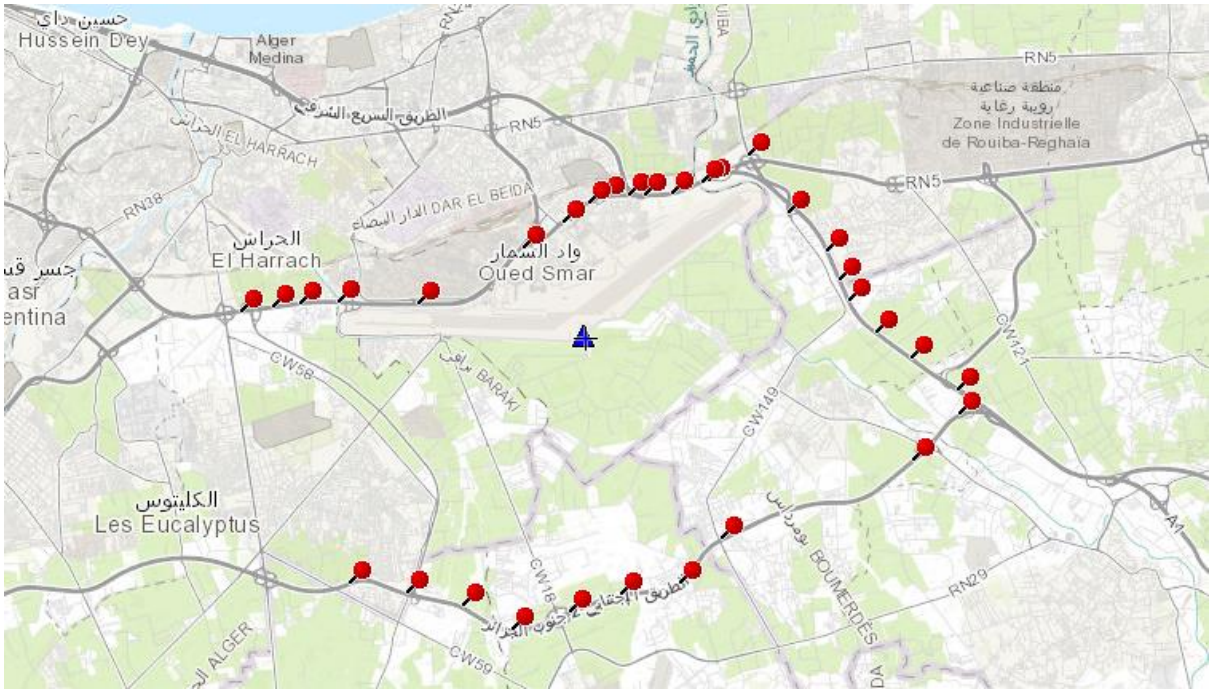


Figure 2 8: Map representing Tx and Rx positions dataset-A

Blue triangle illustrates the real position of the transmitter, red tags demonstrate various positions where data was collected.
Estimated position is compared to real position for each methods to calculate error in meter and comparing results for different methods in conclusion.

Transmitter: ATIS DAAG 128 52 MHZ

Real position: Latitude: 36 689811, Longitude: 3 216641 Elevation: 18m +H_{tx}

Rx data and waypoints:

Table 2.1: Dataset A

Number of observations	*Latitude*	*Longitude*	*Altitude (m)*	*Values(dB)*
1	*36.69412533*	*3.14291233*	*23.1*	*-27.3*
2	*36.69480500*	*3.14950067*	*24.4*	*-20.9*
3	*36 69544233*	*3 15561500*	*20 4*	*23 9*
4	*36.69567400*	*3.16367233*	*23.2*	*-19.5*
5	*36.69527833*	*3.18101000*	*24.3*	*-21.5*
6	*36.70496667*	*3.20356500*	*17.0*	*-24.3*
7	*36.71286833*	*3.21773333*	*17.6*	*-26.1*
8	*36 71407167*	*3 22622333*	*17 4*	*27 1*
9	*36.71440167*	*3.23544667*	*19.0*	*-25.9*
10	*36.71670500*	*3.24343167*	*22.4*	*-28.5*
11	*36.72103333*	*3.25200000*	*23.5*	*-31.1*
12	*36.71119333*	*3.26067167*	*30.7*	*-25.1*
13	*36 70453667*	*3 26894167*	*25 2*	*24.9*
14	*36.69945333*	*3.27162500*	*30.2*	*-28*
15	*36 69582833*	*3 27358500*	*27 7*	*31 9*
16	*36.69040333*	*3.27942333*	*28.3*	*-31.3*
17	*36.68594500*	*3.28704833*	*35.9*	*-30.6*
18	*36.68062000*	*3.29691167*	*39.0*	*26.8*
19	*36.67638500*	*3.29744333*	*47.7*	*-26.3*
20	*36 66850833*	*3 28746333*	*51 2*	*27 1*
21	*36.65489500*	*3.24628167*	*44.4*	*-29.6*
22	*36.64710667*	*3.23719167*	*36.8*	*-34.3*
23	*36.64527333*	*3.22444000*	*41.3*	*20.8*
24	*36.63918000*	*3.20126167*	*36.0*	*-29.9*
25	*36 64323500*	*3 19037333*	*30 4*	*30.3*
26	*36.64554833*	*3.17847667*	*31.3*	*-30.8*
27	*36.64729667*	*3.16627000*	*26.1*	*-29.1*

2.4.2 Dataset-B

Second transmitter is DVOR. It is a standard International Civil Aviation Organisation ground based radio navigational aid that provides bearing information to aircraft to define air traffic control routes for en-route, terminal and instrument approach/departure procedures. DVOR when collocated with DME provides both the angle and slant distance of aircraft with respect to ground station.

The data was collected near to DVOR transmitter on 03/06/21 that operates on 113.9 MHZ radio frequency. The weather conditions was good, the sky was partially covered and the temperature was 31°C.

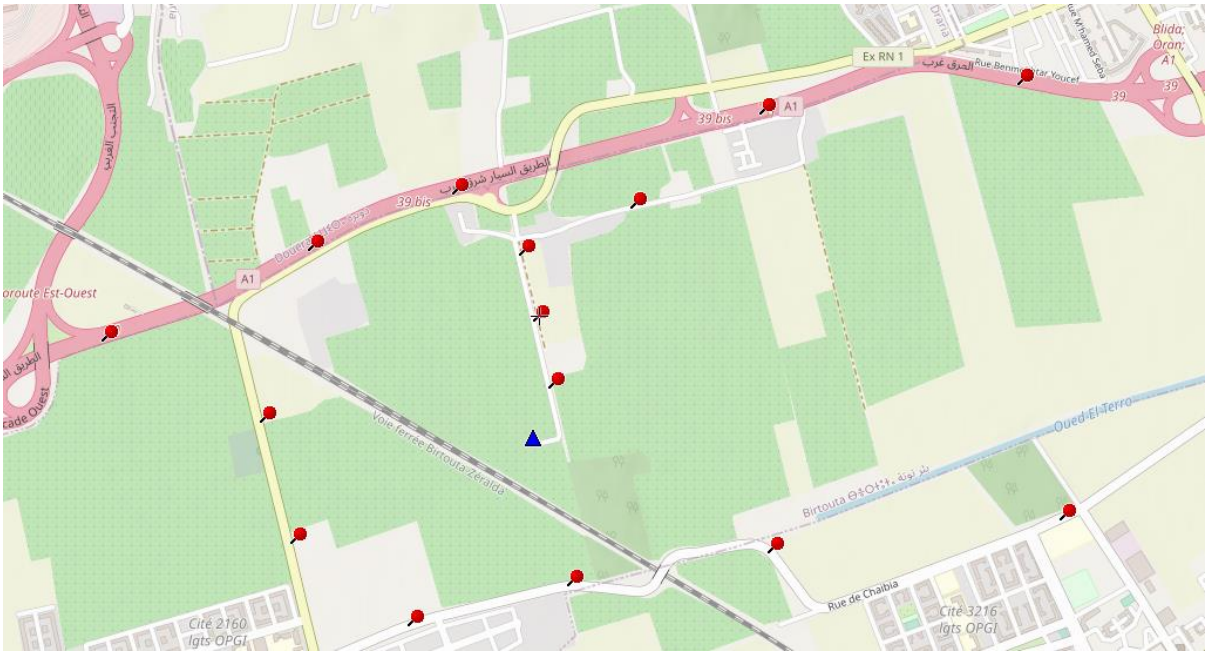


Figure 2.9: Map representing Tx and Rx positions - datasets-B

Transmitter: DVOR ALG: 113 9 MHZ

Real position: Latitude: 36 629898, Longitude: 2 972590 Elevation: 35m +H_{tx}

Rx data and waypoints:

Table 2.2 Dataset B

Number of observations	*Latitude*	*Longitude*	*Altitude (m)*	*Values (dB)*
1	*36 6313454*	*2 9731429*	*35 1*	*14 3*
2	*36 6332998*	*2 9725742*	*40 2*	*14 8*
3	*36.6352284*	*2.9720592*	*44.0*	*-15.5*
4	*36.6366059*	*2.9761362*	*44.2*	*-16.7*
5	*36.6393608*	*2.9808569*	*47.4*	*-20.1*
6	*36.6402216*	*2.9902983*	*43.2*	*-19.4*
7	*36.6370191*	*2.9696131*	*48.4*	*-18.0*
8	*36.6353661*	*2.9643345*	*49.2*	*-17.4*
9	*36 6327144*	*2 9567814*	*45 3*	*19 2*
10	*36.6303381*	*2.9625750*	*45.0*	*-15.4*
11	*36.6267907*	*2.9636908*	*37.8*	*-15.8*
12	*36.6243798*	*2.9679823*	*34.5*	*-15.4*
13	*36.6255508*	*2.9738188*	*31.2*	*-15.1*
14	*36 6265152*	*2 9811573*	*30 4*	*15 7*
15	*36.6274796*	*2.9918432*	*32.4*	*-18.4*

2.4.3 Dataset-C

Third transmitter is a simulation with random generated data with MATLAB software, there is no elevation variation, and loss coefficient is set to 2.2, for all dataset. Zone limits are: lon0 = 3.230; lon1 = 3.321; lat0 = 36.70; lat1 = 36.75.

Real position: Latitude: 36.735693, *Longitude:* 3.2576213 *Elevation: same for all waypoints*

Power reference = 1 mW/ 0 dbm

Rx data and waypoints:

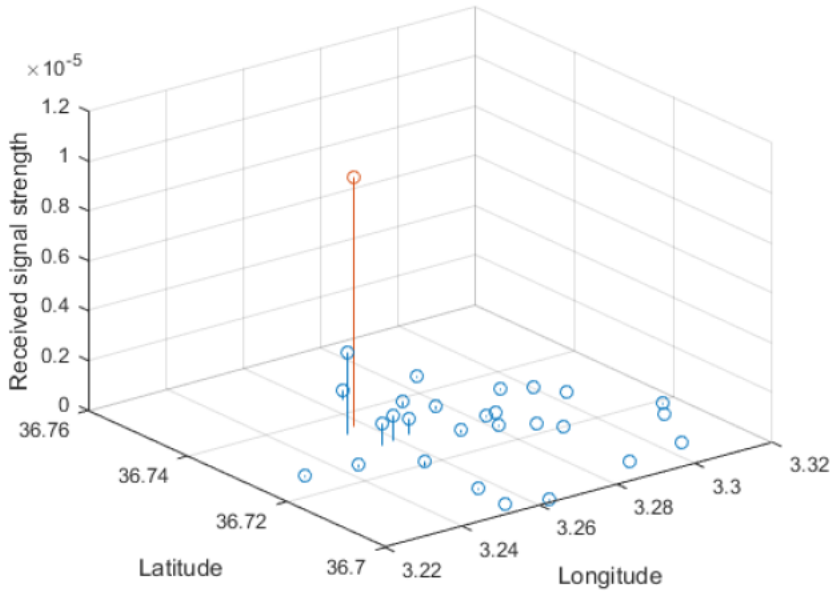


Figure 2.10: 3D Plan representing Tx and Rx positions and received power- datasets-C

Table 2.3 Dataset-C

Number of observations	*Latitude*	*Longitude*	*Values (dB)*
1	*36.72831494*	*3.255528324*	*-60.57976514*
2	*36 72845686*	*3 282497312*	*71 68179565*
3	*36.72531575*	*3.231750458*	*72.34935491*
4	*36.72870849*	*3.258680494*	*-59.83058484*
5	*36.73438694*	*3.277235197*	*-69.16401572*
6	*36 72868243*	*3 285317306*	*72 5739592*
7	*36.70533054*	*3.289770801*	*76.5581395*
8	*36.702792*	*3.254656477*	*-73.89828096*
9	*36.72490817*	*3.281089926*	*-71.6539335*
10	*36 71880235*	*3 315569311*	*79 39565506*
11	*36.74421908*	*3.284777973*	*72.54009541*
12	*36.73413573*	*3.253842418*	*-54.83993876*
13	*36.72925869*	*3.304393253*	*-77.15518833*
14	*36 70668454*	*3 30503389*	*78 64374621*
15	*36.73747723*	*3.272628825*	*66.76648967*
16	*36.72584829*	*3.27260369*	*-68.32385265*
17	*36.70072201*	*3.263269513*	*-74.53530374*
18	*36 72402574*	*3 243701707*	*68 44274931*
19	*36.71935527*	*3.255074565*	*67.5865222*
20	*36.74396857*	*3.265396861*	*-64.15920246*
21	*36.70868296*	*3.255257652*	*-72.09682917*
22	*36 71984699*	*3 291610739*	*75 05507377*
23	*36.7227466*	*3.288077232*	*73.91457159*
24	*36.73286181*	*3.300228046*	*-76.23913616*
25	*36.73479396*	*3.294272022*	*-74.84847541*
26	*36 72914889*	*3 263581173*	*61 88716809*
27	*36.71593496*	*3.31261845*	*79.10069256*

2.4.4 Dataset-D

Fourth transmitter is a simulation with random generated data with MATLAB software, there is no elevation variation, and loss coefficient is set to 3.3, for all area. Zone limits are: lon0 = 2.9108; lon1 = 3.0471; lat0 = 36.6529; lat1 = 36.7053.

Real position: lat: 36.690306, lon: 2.952171 *Elevation: same for all waypoints*
Power reference = 1 mW/ 0 dbm
Rx data and waypoints:

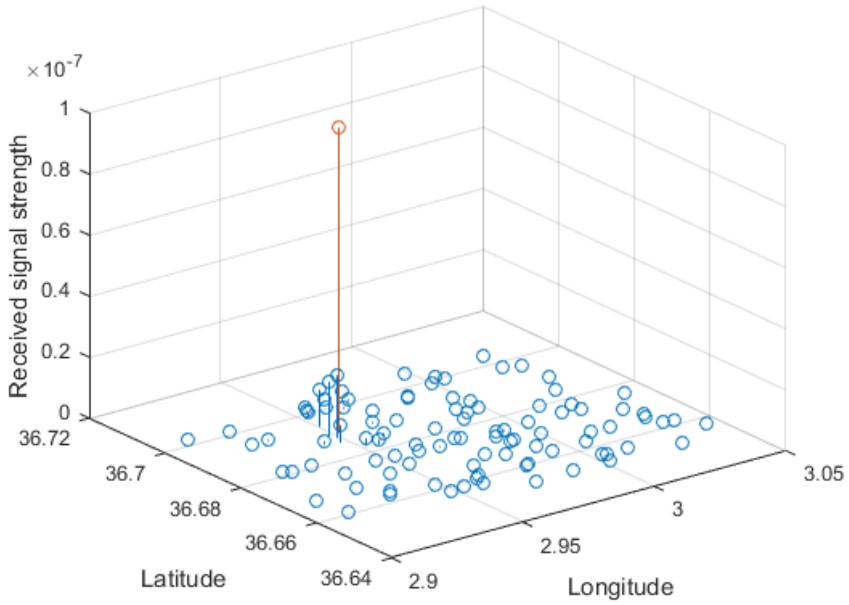


Figure 2.11: 3D Plan representing Tx and Rx positions with received power datasets D.

Table 2.4 Dataset-D

Number of observations	*Latitude*	*Longitude*	*Values(dB)*
1	*36.68842822*	*2.949036379*	*76.88446714*
2	*36.67063403*	*2.989430589*	*-108.738917*
3	*36.66094307*	*2.91342184*	*-110.6039288*
4	*36.67630932*	*2.953757707*	*-94.4641887*
5	*36.66052669*	*2.981548982*	*-108.6451101*
6	*36 6851345*	*2 993654382*	*108 6366223*
7	*36 68870031*	*3 000324836*	*110 4861012*
8	*36.68673653*	*2.947730525*	*-82.67088638*
9	*36.69633531*	*2.987322603*	*-106.5671357*
10	*36.6618545*	*3.038965903*	*-118.8196905*
11	*36.68755365*	*2.992846568*	*-108.3096949*
12	*36.67635581*	*2.946511226*	*-95.33039514*
13	*36 6749839*	*3 022226377*	*115 6676103*
14	*36.67797167*	*3.023185926*	*-115.7340683*
15	*36.70515915*	*2.974649548*	*-102.9129807*
16	*36.6535107*	*2.9746119*	*-109.0339283*
17	*36.6578601*	*2.960631149*	*-105.7633816*
18	*36.69441988*	*2.931322446*	*-99.82122484*
19	*36.68997355*	*2.948356739*	*-77.49254772*
20	*36 67805147*	*2 963817495*	*96 84129609*
21	*36.65803984*	*2.948630967*	*-105.3404932*
22	*36.65375774*	*3.0030807*	*-113.9118576*
23	*36.6918048*	*2.997788206*	*-109.780815*
24	*36.67572759*	*3.015987722*	*-114.4793854*
25	*36 66301484*	*3 007066775*	*113 6249451*
26	*36.68463501*	*2.961097954*	*90.72951516*
27	*36.66699177*	*3.034546097*	*117.975833*
28	*36.69685998*	*2.98798653*	*-106.8366055*
29	*36.6738234*	*2.988373405*	*-107.989259*
30	*36.6599287*	*2.979810721*	*-108.4057173*
31	*36.65376347*	*2.989059331*	*-111.4610618*
32	*36 70114123*	*3 004538795*	*111 8449338*
33	*36.6828546*	*2.988988317*	*107.2430169*
34	*36.69458195*	*2.925331057*	*-103.0268203*
35	*36.68168665*	*2.91841099*	*-106.2635678*
36	*36.67659719*	*2.978699661*	*-104.2532544*
37	*36.70040968*	*2.962055213*	*-94.50798784*
38	*36 6897445*	*3 031341213*	*116 9571412*
39	*36 65669459*	*3 003853989*	*113 6982157*
40	*36.6754842*	*2.990559187*	*108.4311172*
41	*36.68133161*	*2.929022062*	*-101.8482558*
42	*36.66581524*	*3.012962934*	*-114.4951162*
43	*36.66642642*	*2.98126243*	*-107.2684566*
44	*36.70275446*	*2.912768201*	*-108.4856279*
45	*36 66816426*	*2 976294178*	*105 4540502*
46	*36 66132365*	*2 963562476*	*104 799924*
47	*36.69660485*	*3.030658313*	*116.8857606*
48	*36.66437571*	*2.934469749*	*-104.906427*
49	*36.69028548*	*2.964902904*	*-93.14656275*

50	36 68924098	2 972807231	99 45609154
51	36 6704403	3 000381289	111 5158167
52	36.69946305	3.005648336	112.0332812
53	36.67046068	2.990259873	-108.9885035
54	36.6587763	2.954238706	-104.9896661
55	36.66881329	2.927775232	-105.3618343
56	36.68222682	2.977529435	-102.7534017
57	36 68233757	2 955872531	88 31427494
58	36 66520896	2 967236848	103 99356
59	36.67566036	2.961925653	-97.36310669
60	36.70085102	2.955139882	-91.18793373
61	36.67476803	2.932288726	-102.059559
62	36.66260219	3.035760523	-118.3434618
63	36.68763772	2.943010029	-89.38914778
64	36 65669499	3 013888273	115 4042045
65	36.66596243	3.02062741	-115.8381144
66	36.67521906	2.969074117	-100.6559727
67	36.66591385	3.034054384	-117.9496992
68	36.70115259	2.926429954	-103.3835607
69	36.66026801	2.961605965	-104.9431587
70	36.66225318	2.94849835	-103.5501549
71	36.65762273	3.044901589	119.7794646
72	36.69855973	2.966078935	-96.26314015
73	36.70101472	2.971210178	-100.1798396
74	36.69804702	3.025433801	-116.0187816
75	36.68437256	3.026236489	-116.1301115
76	36 68306632	2 952299325	85 79415634
77	36.67583976	3.003652136	111.8444938
78	36.69889444	2.952784449	88.05009865
79	36.69474667	2.971537563	-98.94517769
80	36.66276984	2.994086037	-111.0083447
81	36.68077745	2.921004442	-105.3929036
82	36.66296404	2.932380379	-105.8494445
83	36 70491086	2 998386712	110 5636946
84	36.67639654	3.041158483	118.637087
85	36.65646676	3.005560112	-114.023543
86	36.67479401	2.992827292	-109.1591343
87	36.69450058	2.951014111	-79.15760218
88	36.6676895	2.911432639	-110.050359
89	36 68544114	2 998588804	110 0716429
90	36 67027668	2 943164733	100 2497986
91	36.70376365	2.966249986	98.68493193
92	36.67197882	2.952821045	-97.90126468
93	36.70361283	3.026501328	-116.3404359
94	36.66627349	2.992733161	-110.2036359
95	36.68051936	3.014271341	-113.9525928
96	36 69892007	3 000286945	110 6741072
97	36 67686588	2 977160633	103 587862
98	36.70180102	2.956239074	92.58360364
99	36.67106368	3.032664673	-117.5348541
100	36.65310508	3.029259018	-117.9734083

2.5 Measurements in Decibels:

Decibel (dB) is a logarithmic unit that indicates ratio or gain, it is used to indicate level of acoustic waves and electronic signals.
The logarithmic scale can describe very big or very small numbers with shorter notation.
The dB level can be viewed as relative gain of one level vs. other level, or absolute logarithmic scale level for well-known reference levels.
Decibels (dB) are used to measure the intensity of a signal. The higher the dB value, the stronger the signal. Additional LNA helps to amplify the signal in receiver side, it can add 20 dB and enhance signal intensity, or the coaxial cable attenuates the signal by approximately 3 dB, depend on the quality and cable length. A 20 dB increase in signal means that the signal is increased by 100x. A 3 dB attenuation means that the signal is decreased by (2x).
The formula to convert decibels to ratio power is as follows, where (X) is the value in decibels [dB].

$$Ratio\ power\ \frac{P1}{P2} = 10^{\frac{X}{10}}$$

To convert to decibels from a power ratio or unit use the following.

$$Power\ (dB) = 10 * log10\ (Ratio\frac{P1}{P2})$$

Decibels is be measured with respect to a unit. It is useful to measure it with respect to power in watts (dBW) or milliwatts (dBm).
To get power in dBm :

$$Power\ (dBm) = 10 * log10\ (\frac{P(mW)}{1mW})$$

Coaxial cable and additional LNA are not used in this research, the range is adjusted in phone application to determine weak signal near ground noise about -50 dB and the stronger signal value is about -10 dB as an ideal value adapted to the hardware used [5].

I want to mention something important, the values obtained with the application RF analyzer are in dB which represents a mathematical relative quantity between two absolutes powers measurements in dBm (referenced to 1mW).
The selected configuration indicates only power variation in dB, when the values are close to 0 from negative scale, it means received signal is good and we are close to the transmitter location when situated in LOS environment. The signal strength values changes on dynamic range. When the distance between transmitter and receiver increases, it means we lost more signal power relatively to the initial power reference.

For example, if we have a measured signal strength (-100 dBm), then we can conclude that the signal strength is weak. It could be translated to real power value in Watt, and considered as a reference when we use Rf analyzer application. If measured signal strength is (-40 dBm) then we conclude that the signal is strong and the software takes that value as a reference.
Rf analyzer does not provide absolute received signal strength, we need additional steps to get that data The application gives only the difference between two measured powers in dBm. The vertical amplitude axis displayed on spectrum is in dB not in dBm, if we measure a known (0 dBm) reference signal, we can easily shift the chart and figure out the dBm of our signal power, with (0 dBm) signal amplitude happened to be (0 dB) as a maximum signal strength.
The correct way to measure real absolute received power is to calibrate the RTL-SDR dongle with a synthesized signal generator. We can use a known transmitter configuration to do calibration with a computer instead of a smartphone, also it is possible to use (rtl-kalibrate) to calibrate the dongle with a GSM transmitter tower, GNUradio script, and some dedicated software's for that purpose.
In the thesis, amplitude values in dB present well fluctuation of received signal strength, the main interest is to notice power strength variation and quantifying the power loss between different waypoints, therefore measuring absolute real received power from transmitter is not mandatory to locate the RF transmitter especially when dealing with an uncooperative emitter The power reference is selected to 1mW for all datasets

Antenna with good directivity towards the signal source will pick up more signal and less noise from other directions, a good antenna would catch more power. The amount of power received was sufficient to achieve the experience.

2.6 General notes

- Friss transmission equation is dedicated for free space environment, and the adaptation maid for simulated data is to take the distance powered by pre-selected loss coefficient, not the value 2.
- Guessing the right amount of power loss for every position need more steps and depends on area specifications.
- In real space environment, power loss is generally great than two in outdoor environments, trees, obstacles, topographic factor. The power loss coefficient could be greater than 4 due to shadowing and multipath effects. In this research all observation waypoints are approximately on the same level of elevation to avoid relief obstructions, see *Tables 2.1* and *Tables 2.2.*

- Cartesian mapping is implemented for all datasets The script change a pair of latitude and longitude points to a Cartesian point's pair on a plane support, where the Earth is represented as a flat surface in 2D with the x-axis and y-axis represent the origin at the intersection point of the Prime Meridian and Equator. The correction factor compensates for the distortion only at one given latitude, so the approximation is only good when close to that latitude.

$$x_0 = longitude * Correction\ factor$$

This approximation is enough when the distance between received observations waypoints are not in a large area. But let's consider that we have uncertainty $\pm\varepsilon$ ignored and added to final estimate for all observations. If the area of interest is big, uncertainty ε increases. Therefore, we could not ignore it.

- The area of interest is divided into small virtual bins and constitute 2D grid. The number of bins selected for method 1 and method 2 is 30, so the grid covers all the area of interest and has a different size of (30x30) blocks corresponding to each dataset. The number of bins has a direct effect on heatmap histograms and final position estimation. After a few attempts, 30X30 bins provide a reasonable estimate based on the dataset maximum size.

Chapter 3

Binary Decision Classification Method

Binary classification is the task of classifying the elements of a set into two groups on the basis of a classification rule. The variable of interest is dichotomous, it means only two possibilities are available, as an example, whether or not the area selected contain the transmitter. The method presented in this chapter is an association of binary classification theory with geometric disambiguation, where the goal is to adopt a model that can rank new objects such that those in one category are ranked in one side than those in the other side. Then, guessing an acceptable position estimation for the transmitter. Several iterations are needed to reduce maximum searching area. During simulation trials, the approach worked well when power loss coefficient is averaging a constant value for all the area [7].

3.1 Method description

The basic idea for this method is to draw a probability grid that has similar initial value for all the grid, then starts to multiply that values by pre-selected probability factor for the side that has strong received power strength, and divide that same factor on the side that has a weak received power strength. So, the probability grid will be updated for each iteration by choosing randomly pairs from initial collected data The algorithm selects pairs that have unequal received power strength and geo-spaced by more than 100 meters, which means if the distance between two measurements positions, waypoint (a) and waypoint (b) are equal or less than 100 meters, the algorithm will skips that pair and selects another pairs randomly that have larger distance.

A virtual line crosses midpoint of the segment distance *(a,b)* between the two receiver's positions. The geometric line is perpendicular. The midpoint is used in

geometrical part. It is equidistant from both endpoints, and it is the centroid both of the segment and of the endpoints. It bisects the segment.
First iteration gives us a general idea about the transmitter location, the real position is likely to be above the black line, the higher is received power, the closer we are to the transmitter location, especially in LOS situation. Thus, the side that has a higher received power strength for selected pair will be multiplied by that factor, and the other side is divided by the same factor.

The second iteration increases probability estimate, when updating grid probability, the area containing transmitter real position is reduced significantly, after multiple iterations, the final estimated position is deduced from intersections of all orthogonal segments that cross midpoints included in higher probability area guessed from the grid. Therefore, one bin will be selected *(figure 3.4)* and the center of that bin is considered as a final position estimate.
Testing the method using MATLAB, demonstrates an acceptable results, at least gives a correct approximations and reduce searching area [8, 9].

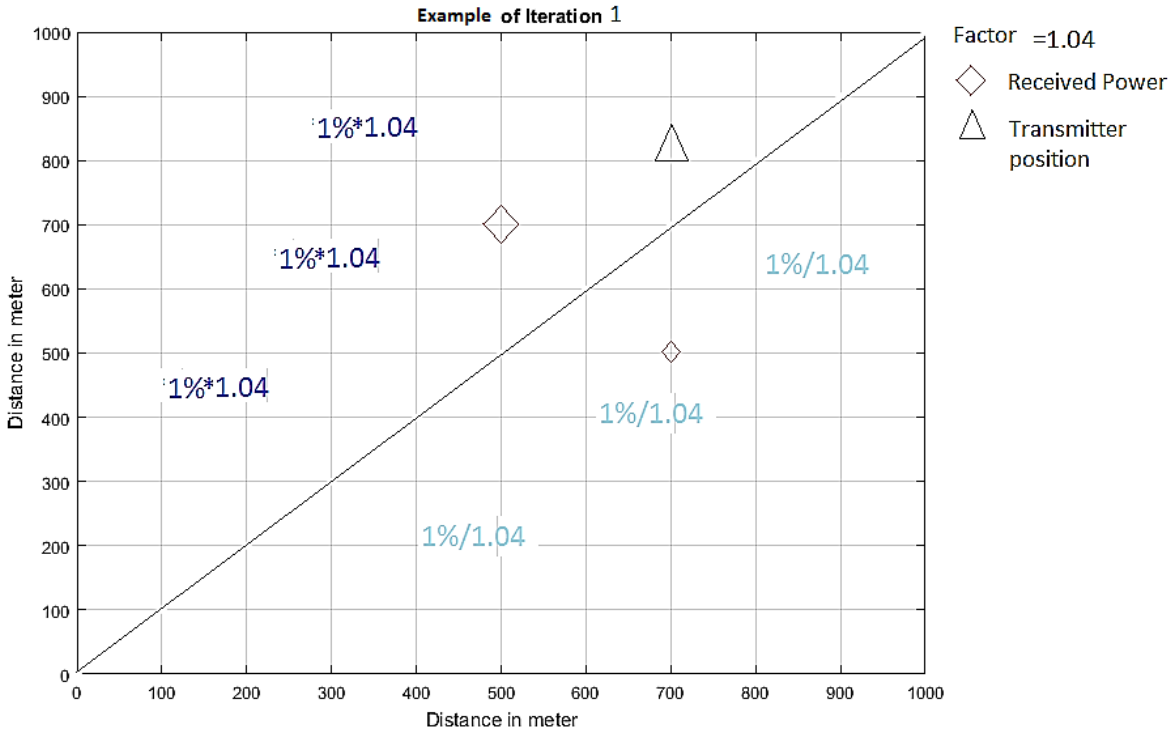


Figure 3.1: Example of iteration (1) for binary decision classification method

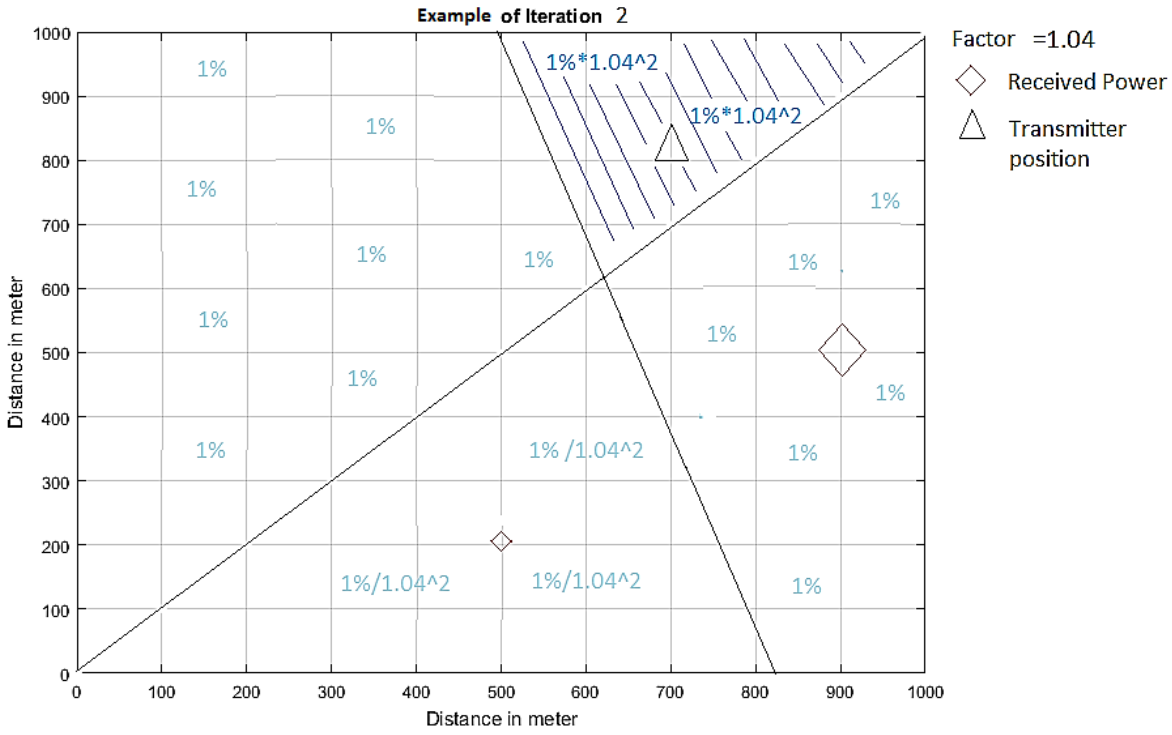


Figure 3.2: Example of iteration (2) for binary decision classification method

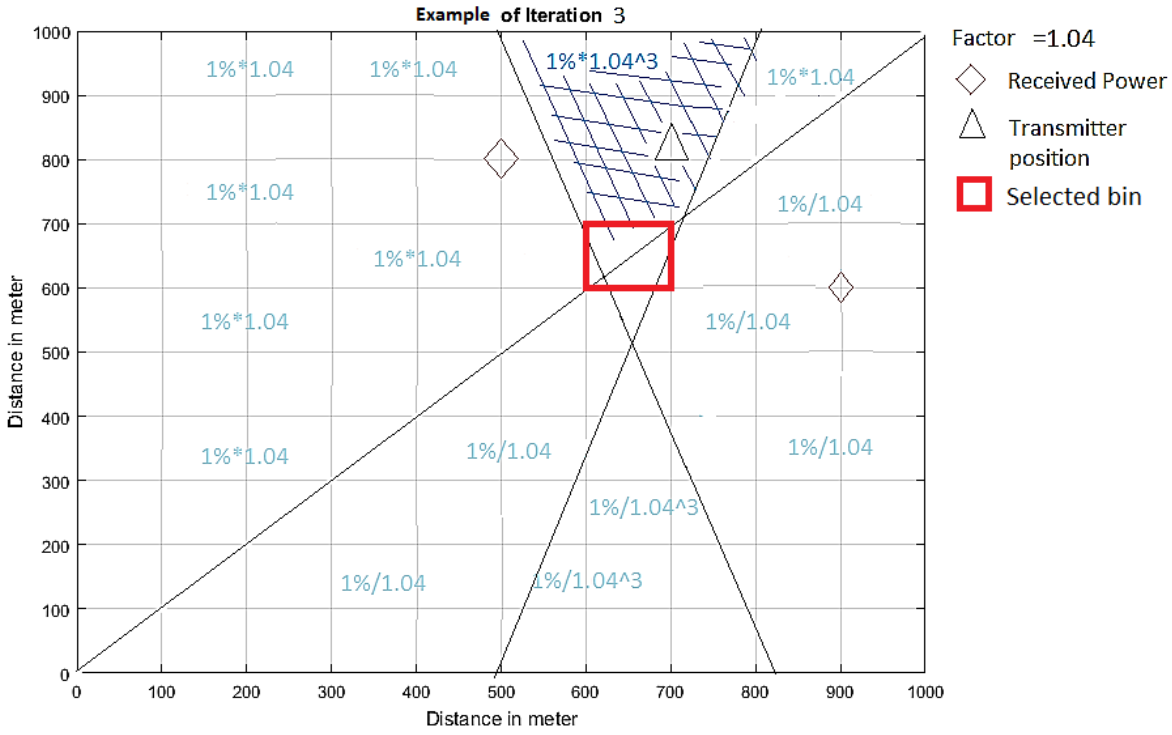


Figure 3.3: Example of iteration (3) for binary decision classification method

Probability grid modelized in (*figures 3 1, 3 2, 3 3)* above covers ($1km^2$). This is just an example to illustrate how the algorithm proceed for the first three iterations. Datasets input file contain longitude and latitude instead of distance in meters.
Black triangle represents the real position of RF transmitter that we are looking for, the two red diamonds show the measurement position and the amount of received power for that position. The larger the diamonds is, the higher power measurement is.
The black line divides the area into two regions for each iteration based on the midpoint of the two observations.

Probability factor must be strictly greater than 1. During the experience, the input factor is taken 1.04. I purposefully avoided to take a higher factor value to merely find the zone with a higher chance of containing the transmitter relatively to other zones inside the area of interest, so if a region has a 10% probability as an ultimate result, it would be considered for estimations.

3.3 Binary decision classification algorithm

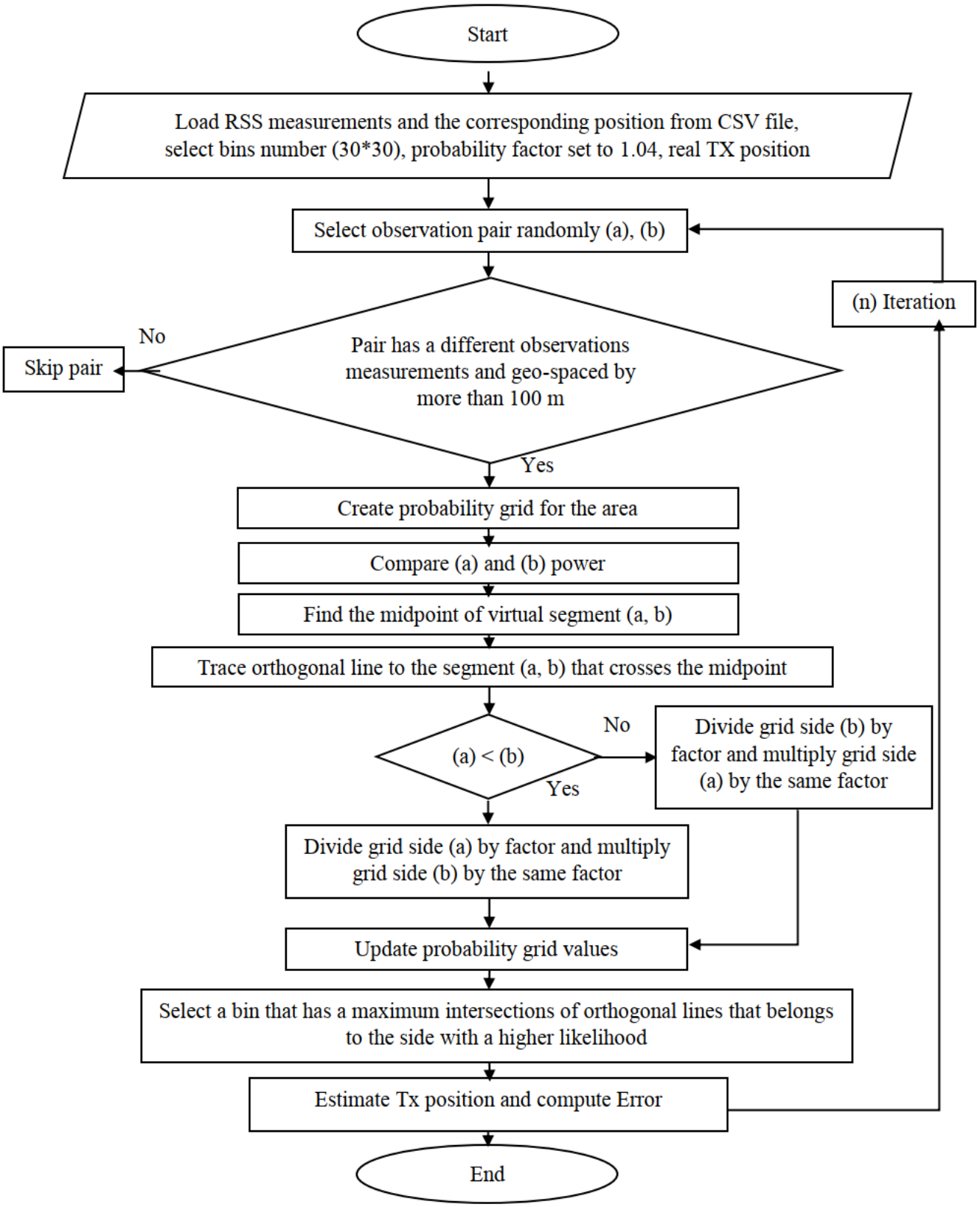


Figure 3.4: Binary decision classification method flowchart

3.4 Results

Table 3.1: Binary decision classification method efficiency

Dataset	*Searching area*	*Errors (meters)*
A (Number of pairs skipped: 0)	*164.139 km²*	*3798.55 (Average)*
B (Number of pairs skipped: 0)	*10.933 km²*	*186.47*
C (Number of pairs skipped: 0)	*45.049 km²*	*145.39*
D (Number of pairs skipped: 2)	*70.755 km²*	*102.12*

- **Dataset-A**

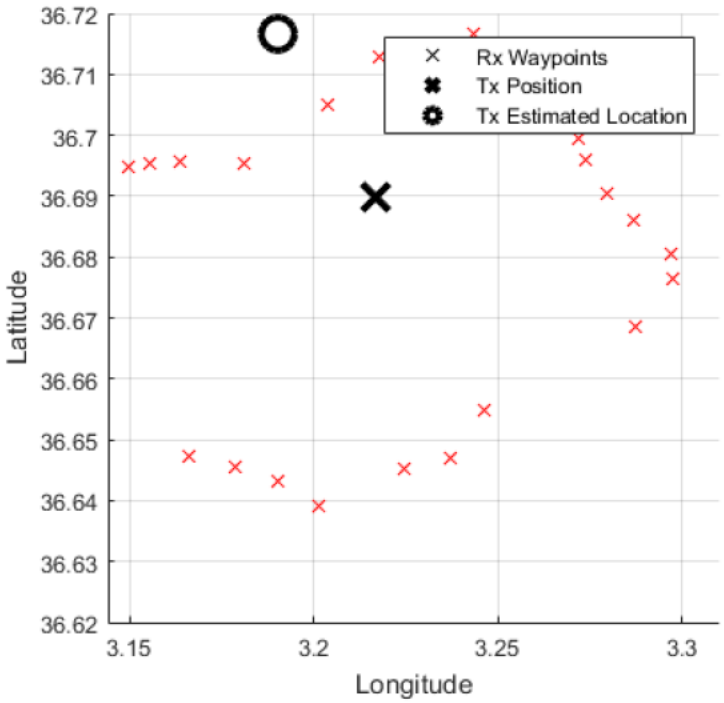


Figure 3.5: Diagram of Binary decision classification dataset-A

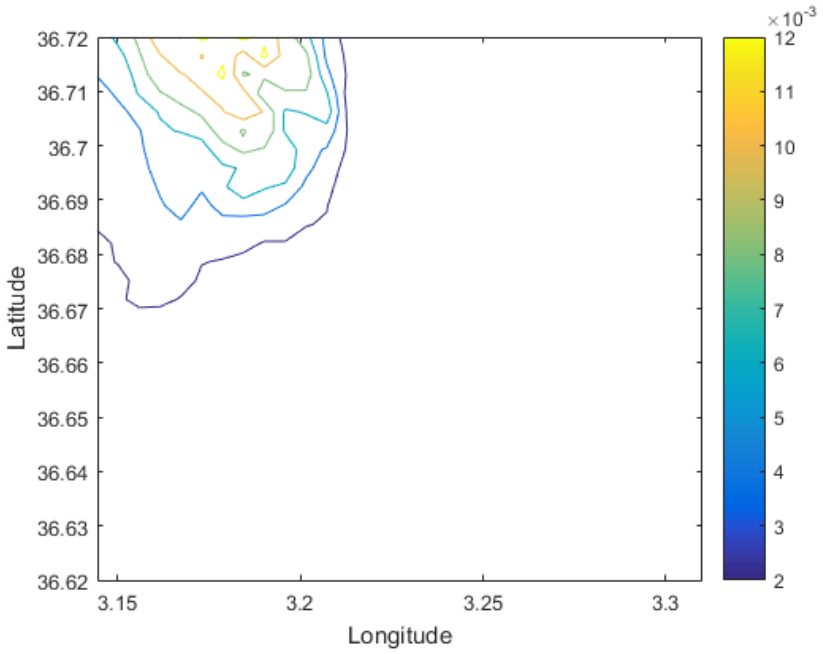


Figure 3.6: Contour map of Binary decision classification dataset A

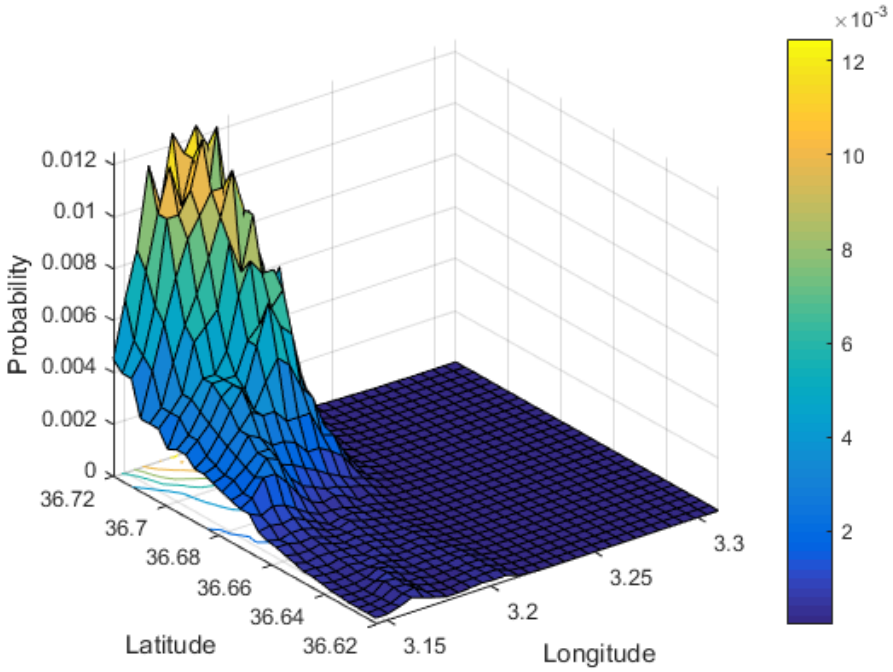


Figure 3.7: 3D Heatmap histogram of Binary decision classification –dataset A

Figure 3.6 and 3.7 above illustrates different colored contours, with yellow color being the area with the highest likelihood of having the transmitter.

The blue color denotes a low-probability location. The color code interpretation is the same for all datasets in this chapter.

- **Dataset –B**

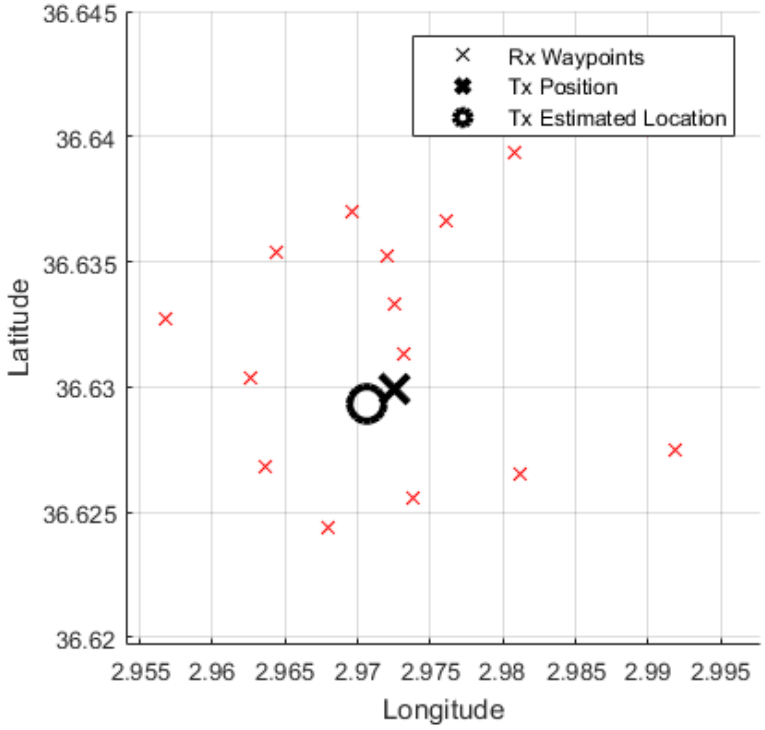


Figure 3.8 Diagram of Binary decision classification –dataset-B

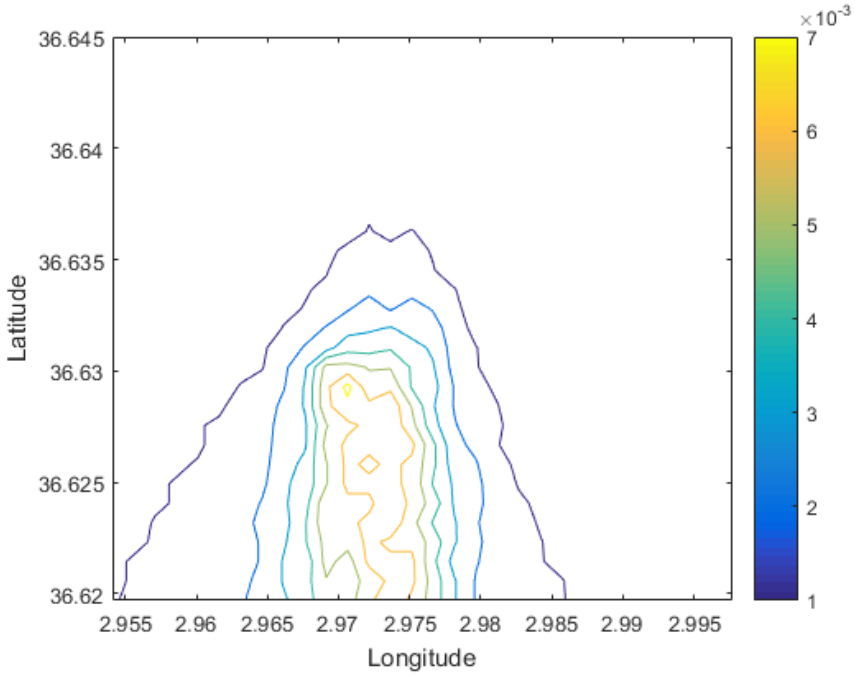


Figure 3 9: Contour map of Binary decision classification dataset B

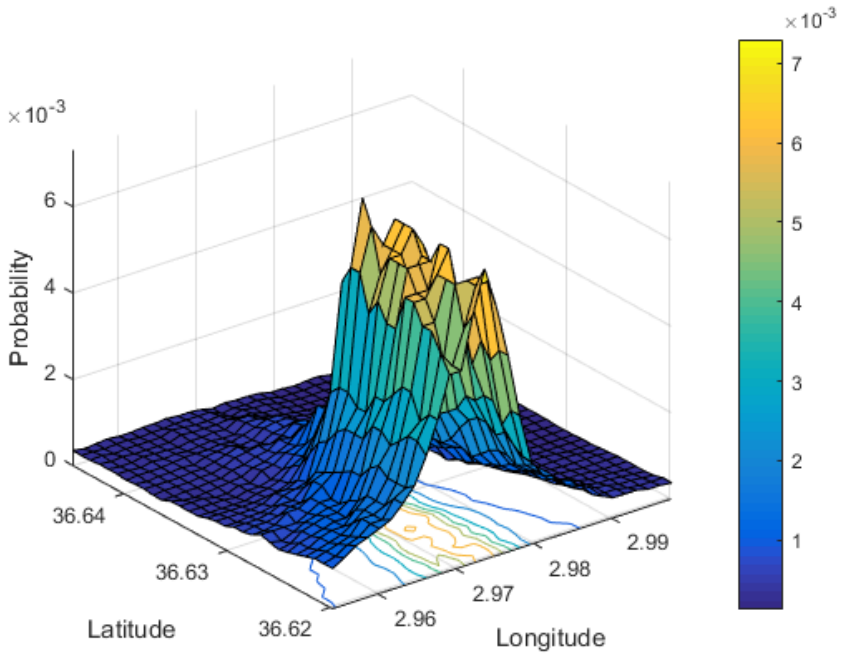


Figure 3 10: 3D Heatmap histogram of Binary decision classification –dataset B

- **Dataset-C**

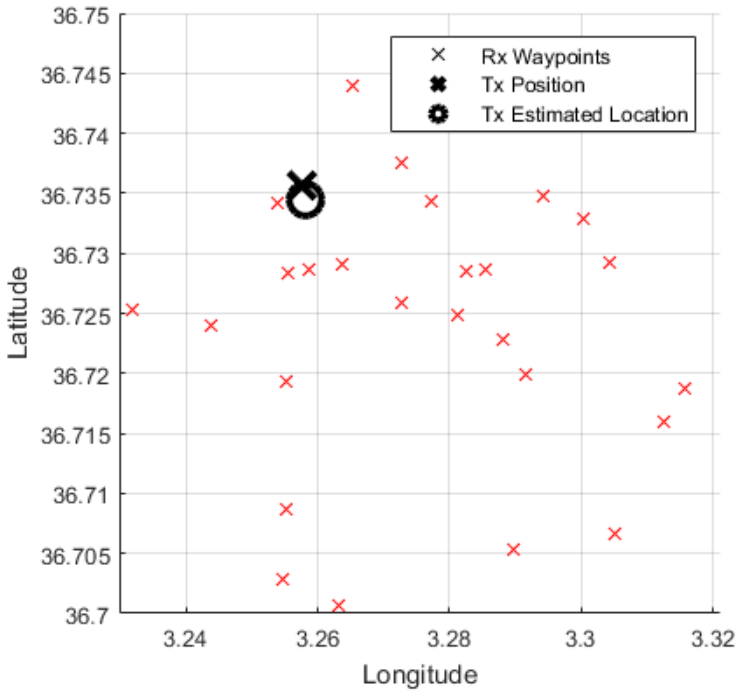


Figure 3 11: Diagram of Binary decision classification –dataset-C

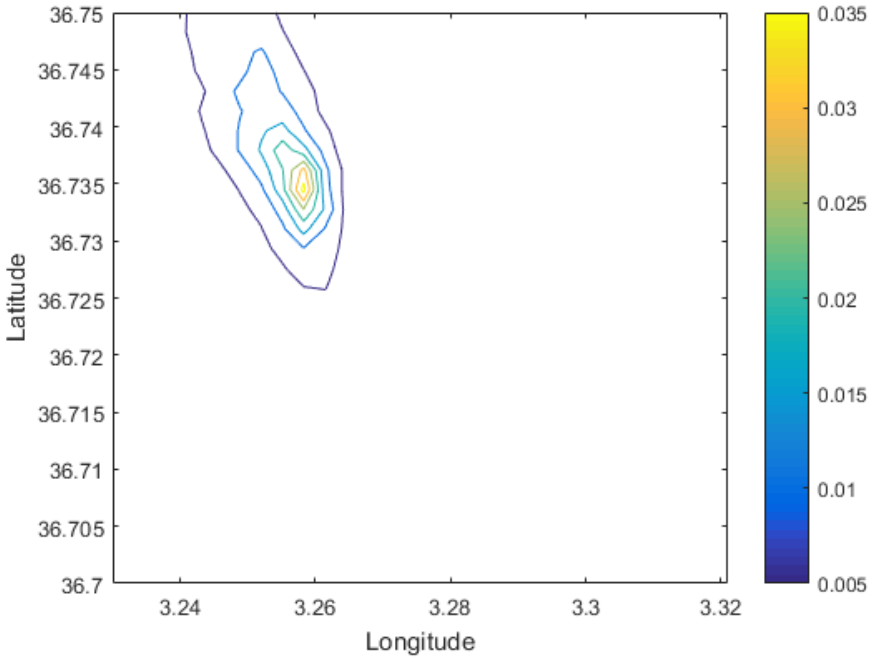


Figure 3 12: Contour map of Binary decision classification –dataset C

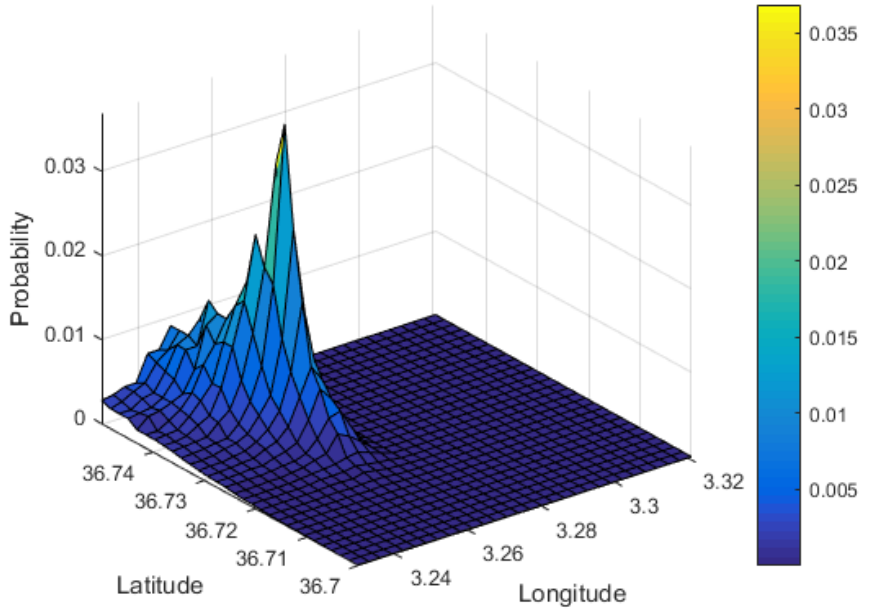


Figure 3.13 3D Heatmap histogram of Binary decision classification dataset C

- **Dataset-D**

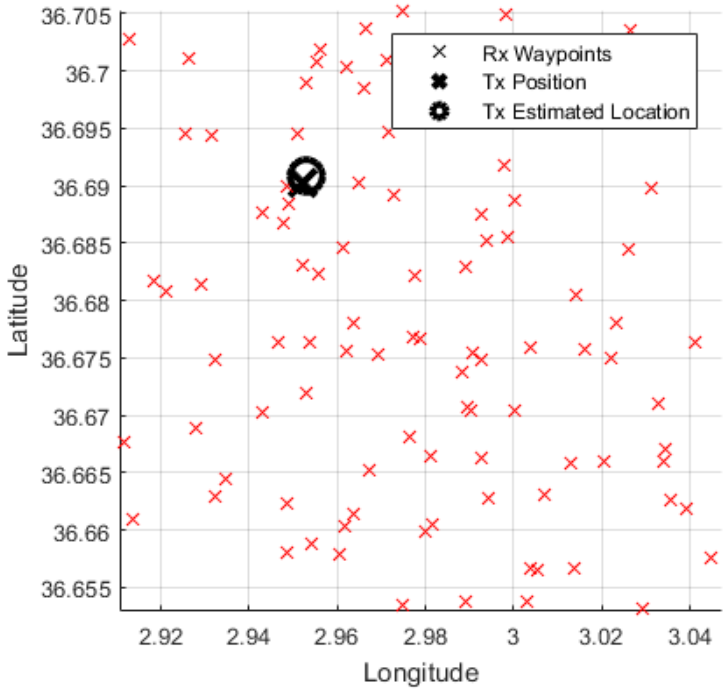


Figure 3.14: Diagram of Binary decision classification –dataset-D

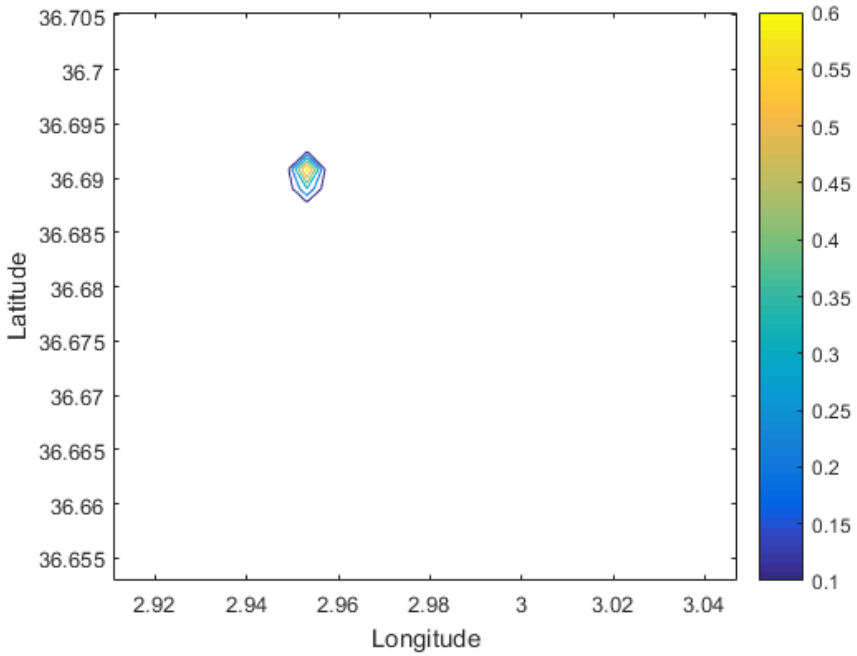


Figure 3.15: Contour map of Binary decision classification –dataset -D

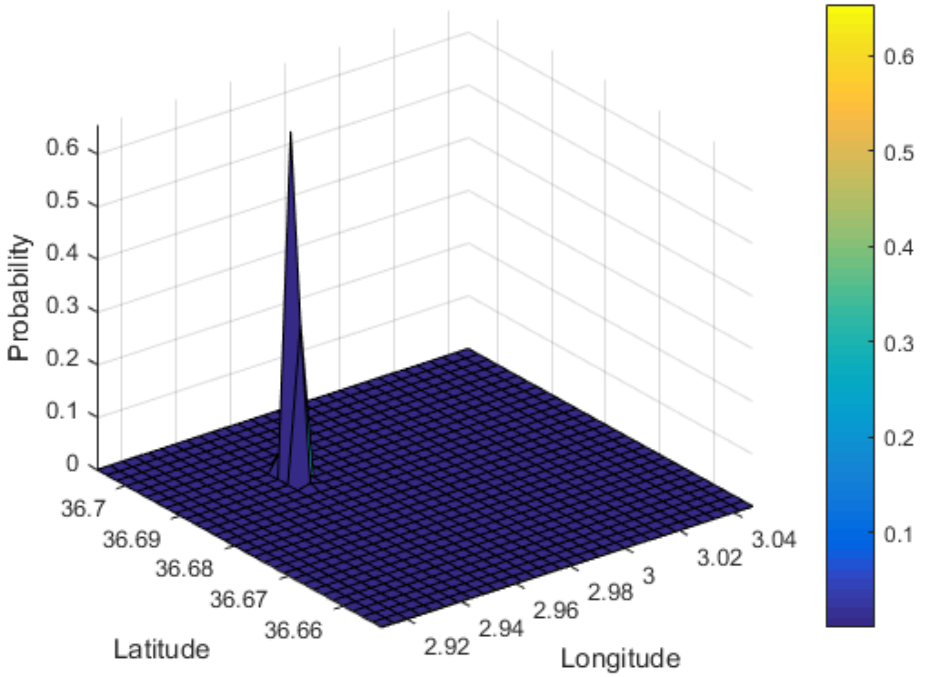


Figure 3.16: 3D Heat map histogram of Binary decision classification –dataset D

Chapter 4

Geometric Circles Method

The computation of intersection nodes of many circles is a challenging problem. While the intersection of two circles is straightforward, even three circles admit several configurations, each resulting in a different expression for the intersection area. Given the centers and the radii of the circles, the automatic discrimination among the various cases requires involved condition testing. If we consider cases with several circles the problem may appear unsolvable, as the close form expressions for the intersection areas become more and more involved and depend on the specific configuration among a huge number of possibilities.

Despite the wide range of applications of this geometric problem, a systematic approach is still lacking. It has been addressed in the literature for three circles, but only for some specific configurations.

However, no algorithmic solution is proposed to exploit the result in an organized and exhaustive way if there is no intersection at all.

The coverage range is the maximum distance between two nodes which guarantees the received power to lie within the admissible region. The resulting coverage area of a transmitter, is a circle centered on the transmitter with radius equal to the coverage range. Note that different transmission power levels, packet encoding rate and, in general, transmission parameters can be represented as multiple circles centered on the same node.

A node placed in a point of the plane covered by multiple coverage areas can communicate with all the nodes associated with those coverage areas The computation of the area of those regions enables a wide range of considerations in many scenarios of interest

In sensor networks, localization relies on the reception of beacons sent by nodes whose positions are known. The accuracy achieved by the localization algorithm depends on the number of beacon sources that the node can hear. This requires the computation of the probability that a node falls withinan area

covered by a certain number of circles. Furthermore,intersections of multiple circles are al sofound when addressing the problem of preserving complete sensing coverage of a certain area and connectivity.

The geometric approach selected attempts to draw circles of constant power ratio between observations pairs, in order to determine the transmitter location. The sector with a high number of new circles intersections has a higher probability rate for transmitter location.

The purporse is to determine blind node location within the scattered nodes. The proposed methodology consists of using power ratio and waypoints positions to creates virtual circles and guess Tx position.

4.1 Geometric circles method algorithm

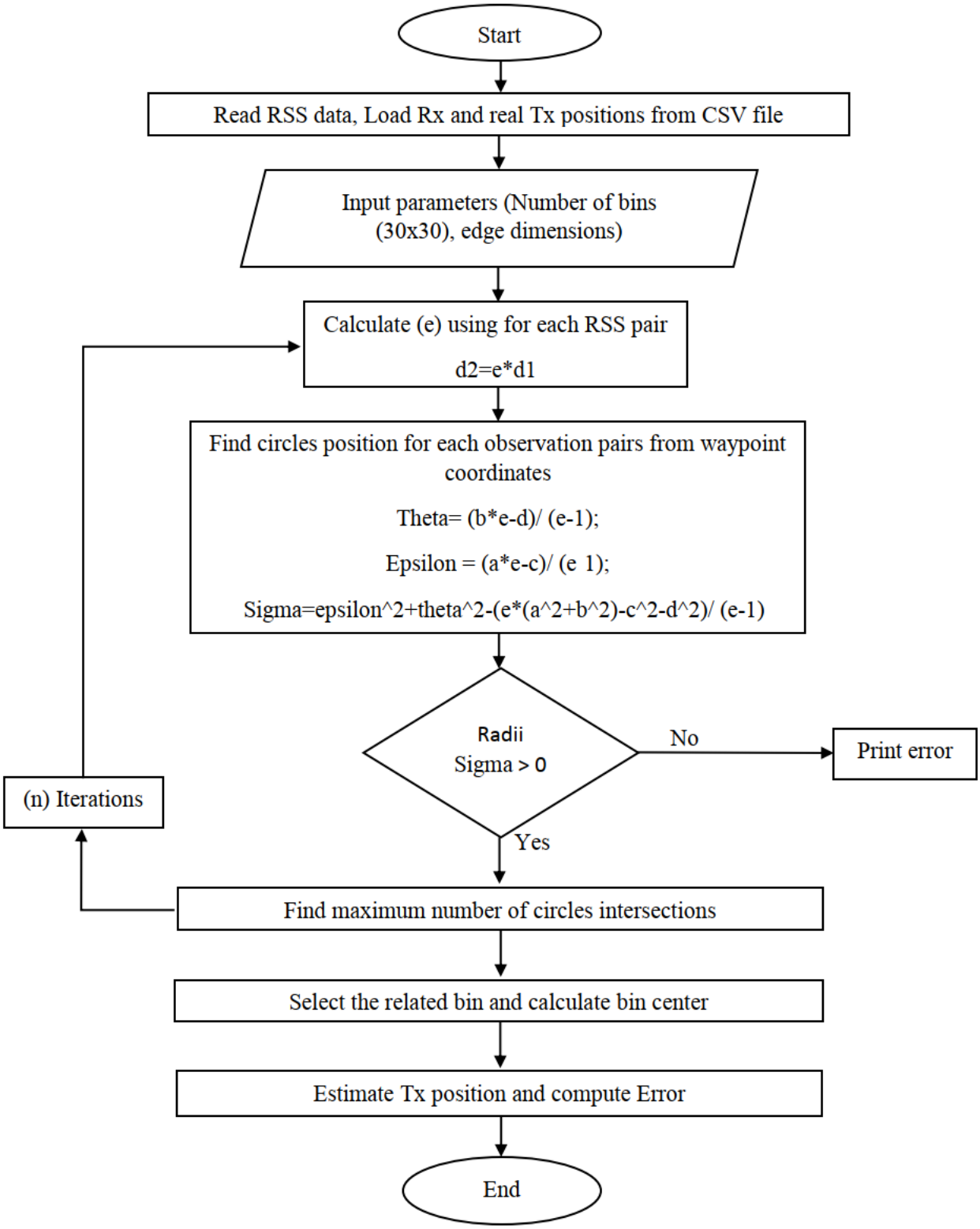


Figure 4.1: Geometric circles method flowchart

4.2 Method demonstration

To understand the method, let consider measurements of power received isotropic, a recognized power transmitted, known gains and frequencies, and assume quadratic power loss because of distance. Friis transmission equation can be solved directly to retrieve the distance.

$$d = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 P_r}$$

Drawing a circle of radius (d) to illustrate a locus of probable transmitter positions. It's mean that the transmitter is situated somewhere on the circle locus. When the transmitted power is not known and only two receivers or two passive observations are made, each can measure a received power $Pr1$ and $Pr2$.

$$Pr1 = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d_1}$$

$$Pr2 = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d_2}$$

The ratio of these two powers, simplify the equation, assuming everything is stationary, the distances *d* are constant, so this term can be reduced to a constant, *e*

$$d_2 = e.d_1$$

$$\frac{P_{r1}}{P_{r2}} = e$$

For example, if *e = 2*, then d_2 is twice as long as d_1. This means the observation at d_2 is twice as far away from the transmitter as the d_1 observation. Circles of

constant ratio radius can be drawn using the power ratio between the two observations.

The transmitter must be somewhere on the circle of constant radii ratio locus. When more observations are added, the location of the transmitter can be easily determined based on the circle intersections once we have 4 observations.

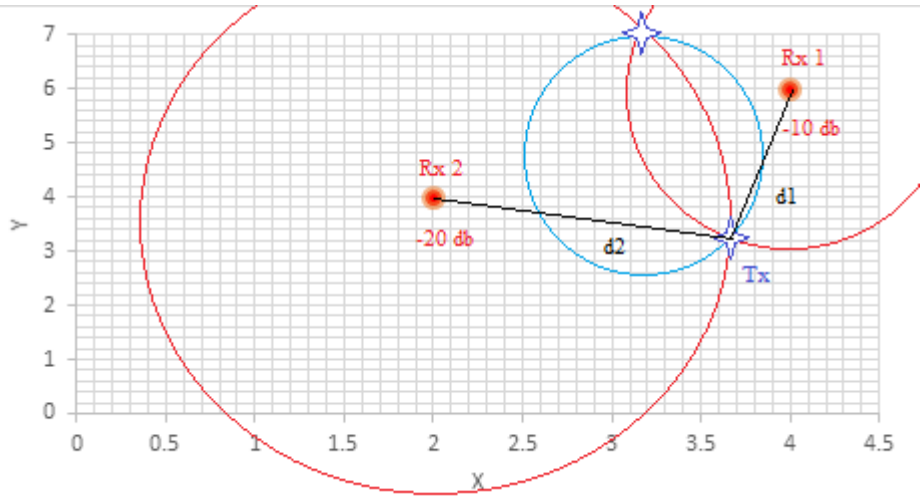


Figure 4.2: Illustration of two observations -ideal case

Let's consider two observation centered in *(a,b)* and *(c,d)* , the have different received signal strength, every observation has a circle locus around it and determined by the power strength.

Whatever is the radii value, *e* is the constant that represents a ratio between two received powers.

This new circle represents the locus of valid transmitter locations for the given power ratio and observation locations represented in *figure 4 1* with blue circle

In real-world environment additive noise introduced into the measurements In the context of the geometric circles algorithm, the locus of points may no longer intersect the true transmitter position. Circle intersections may no longer provide a good estimate of location. There can even be cases where there are none intersections at all [10, 11].

In general, the problem of additive noise can be overcome using more than just three observations.

Another significant type of noise is differing loss coefficients. The Friis transmission equation is for free space and therefore has a loss coefficient of 2 as the exponent to the distance term *d*.

Previous research have noted that differing loss coefficients happen often in real world environment, and that needs further research Allowing for differing loss coefficients, (*figure 4.3)* illustrates using four passive observations, the equation for received power, P_r, then becomes :

$$Pr = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^e}$$

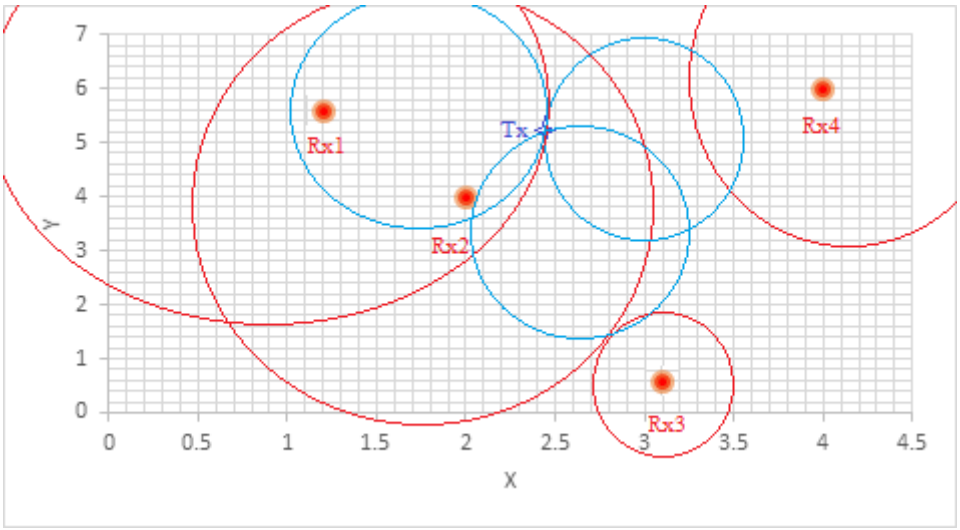


Figure 4.3: Illustration of four observations –ideal case with additional noise

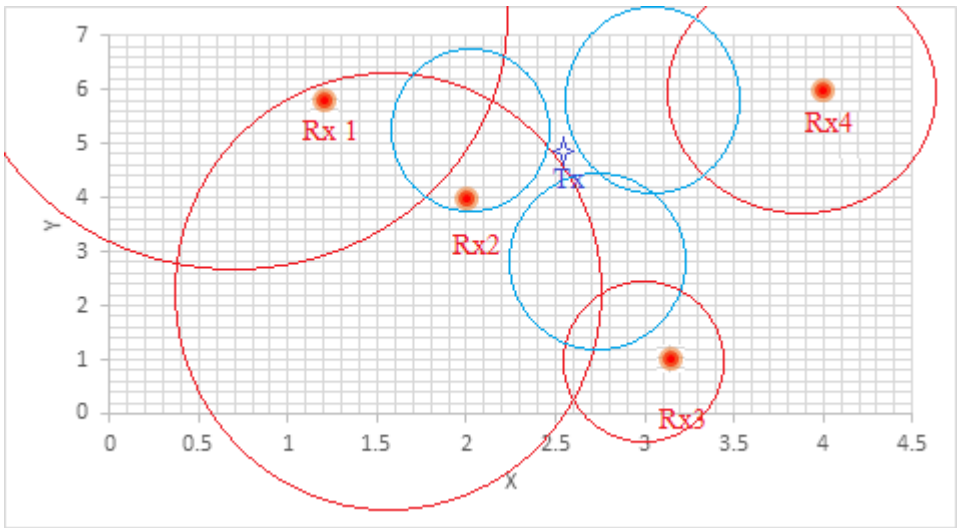


Figure 4.4: Illustration of four observations no ideal case with additional noise

Theorem:

The equation of a circle is sometimes seen in another form and can be derived from the one above.

$(x-a)^2 + (y\ \ b)^2 = r^2$

$x^2 \quad 2ax + a^2 + y^2 \quad 2by + b^2 = r^2$

$x^2 + y^2 - 2ax - 2by = r^2 - (a^2 + b^2)$ we know that the center of the circle is (a, b).

Let C (g, f), hence, $a=\ \ g$ and $b=\ \ f$.

Replacing a and b by $-g$ and $-f$, we can rewrite the equation in the form

$x^2 + y^{2+} 2gx + 2fy = r^2 \quad (g^2 + f^2)$

$x^2 + 2gx + 2fy + (g^2 + f^2) - r^2 = 0$ Letting $c= (g^2 + f^2) - r^2$, the equation becomes:

$x^2 + y^2 + 2gx + 2fy + c=0$. [12]

Theorem integration:

$(x - a)^2 + (y - b)^2 = r^2$ ... (1)

$(x \quad c)^2 + (y \quad d)^2 = e^2 r^2$ ... (2)

Divide (1) / (2):

$$(x - a)^2 + (y - b)^2 = \frac{1}{e^2}(x - c)^2 + (y - d)^2$$

$$(x^2 \quad 2xa + a^2 + y^2 \quad 2yb + b^2) = \frac{1}{e^2}(x^2 \quad 2xc + c^2 + y^2 \quad 2yd + d^2)$$

$$x^2 \quad 2xa + a^2 + y^2 \quad 2yb + b^2 \quad \frac{x^2}{e^2} + \frac{2xc}{e^2} \quad \frac{c^2}{e^2} \quad \frac{y^2}{e^2} + \frac{2yd}{e^2} \quad \frac{d^2}{e^2} = 0$$

$$\left(1 \quad \frac{1}{e^2}\right)x^2 \quad \left(a \quad \frac{c}{e^2}\right)2x + a^2 \quad \frac{c^2}{e^2} + \left(1 \quad \frac{1}{e^2}\right)y^2 \quad \left(b \quad \frac{d}{e^2}\right)2y + b^2 \quad \frac{d^2}{e^2} = 0$$

$$\epsilon = \frac{ae^2 \quad c}{e^2 \quad 1} \quad ; \quad \theta = \frac{be^2 \quad d}{e^2 \quad 1}$$

$$\sigma^2 = \sqrt{\epsilon^2 + \theta^2 \quad \frac{(e^2(a^2 + b^2) \quad c^2 \quad d^2)}{e^2 \quad 1}}$$

New circle equation: $(x - \epsilon)^2 + (y - \theta)^2 = \sigma^2$ ..... (3)

4.3 Results

Table 4.1: Geometric circles method efficiency

Dataset	*Searching area*	*Errors(meters)*
A	*164.139 km²*	*2746.66*
B	*10.933 km²*	*392.02*
C	*45.049 km²*	*1205.29*
D	*70.755 km²*	*733.58*

- **Dataset-A**

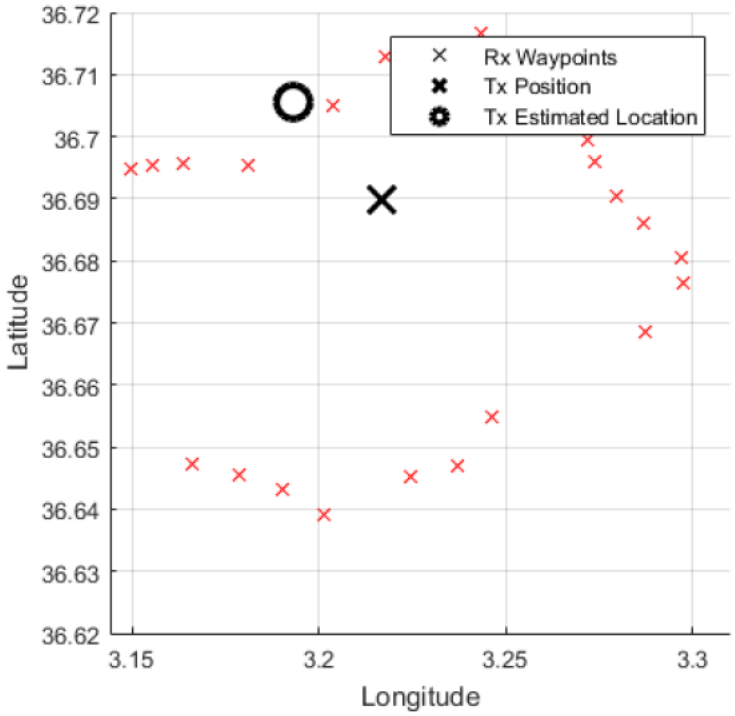


Figure 4.5: Diagram of geometric circles method dataset-A

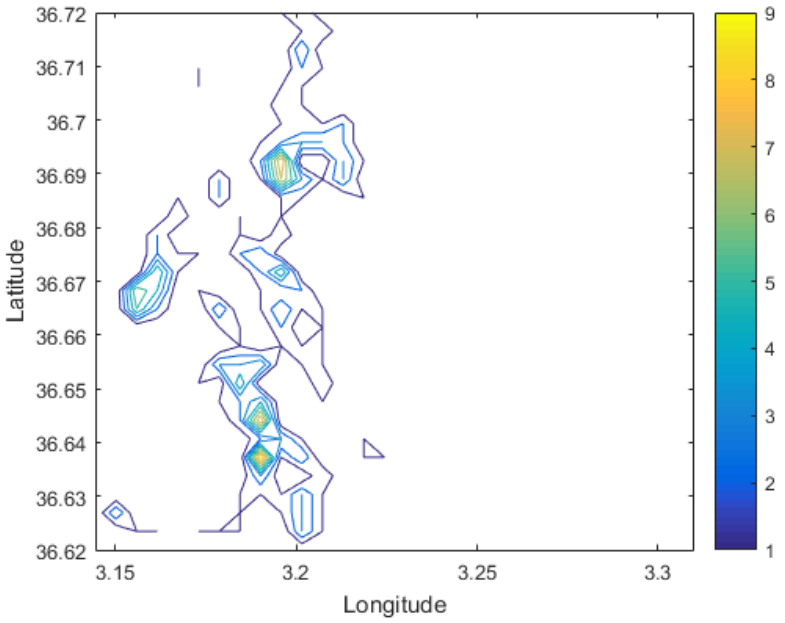


Figure 4.6 Contour map of geometric circles method–dataset-A

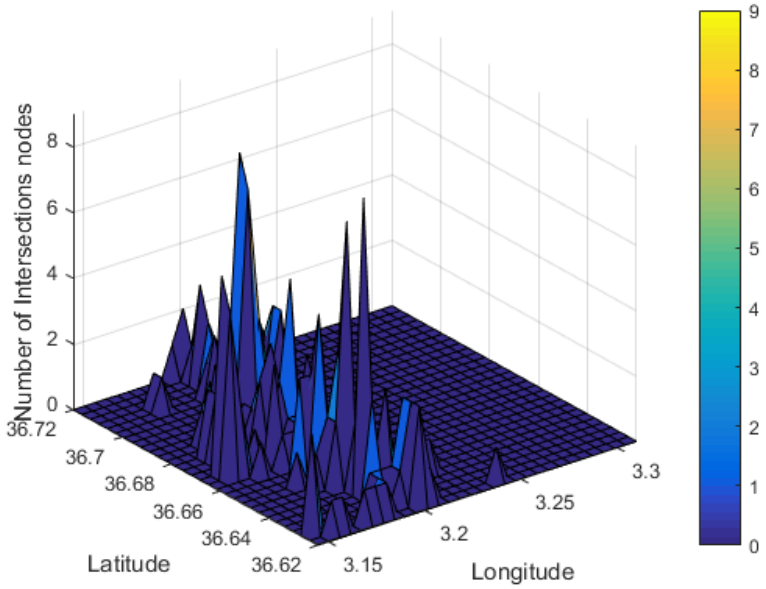


Figure 4.7: 3D Heatmap histogram of geometric circles method–dataset-A

Figure 4.6 and 4.7 above illustrates different colored contours, with yellow color being the area with the highest circles intersections nodes.

The blue color indicates a low number of intersections. The color code interpretation is the same for all datasets in this chapter.

- **Dataset-B**

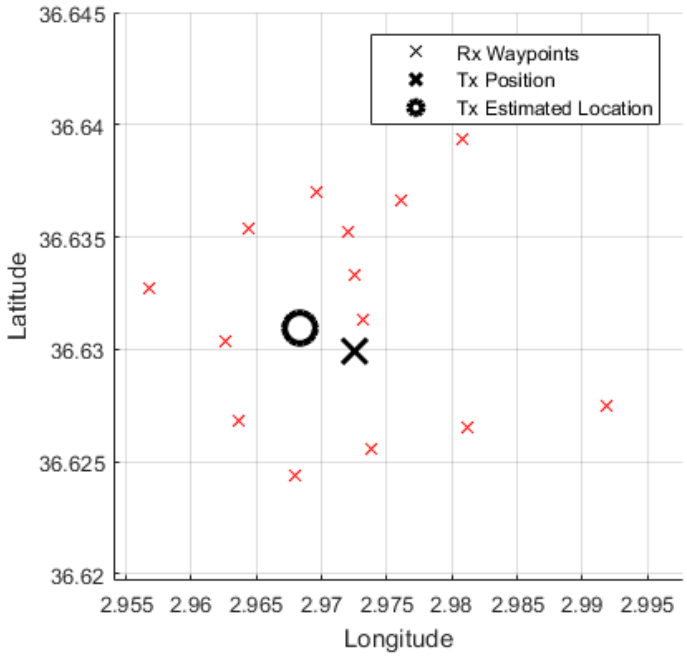


Figure 4.8: Diagram of geometric circles method dataset-B

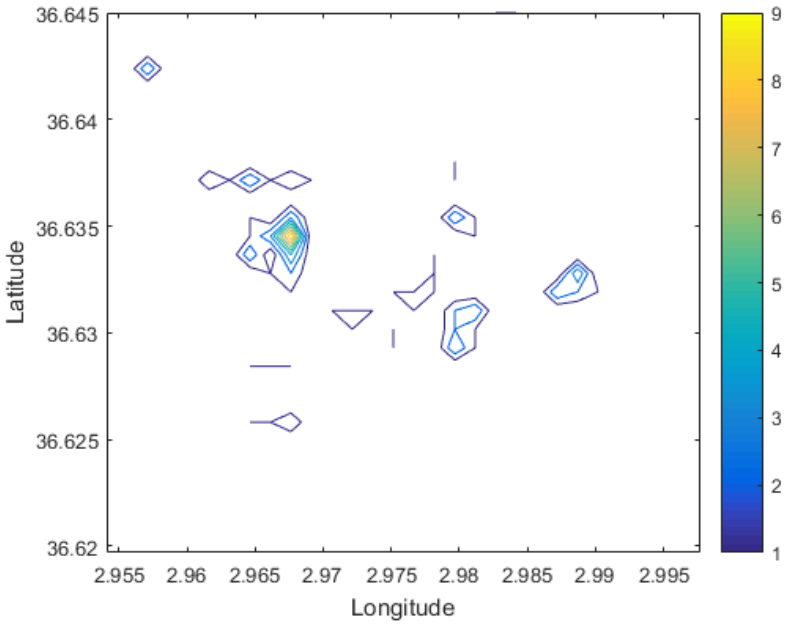


Figure 4.9: Contour map of geometric circles method dataset-B

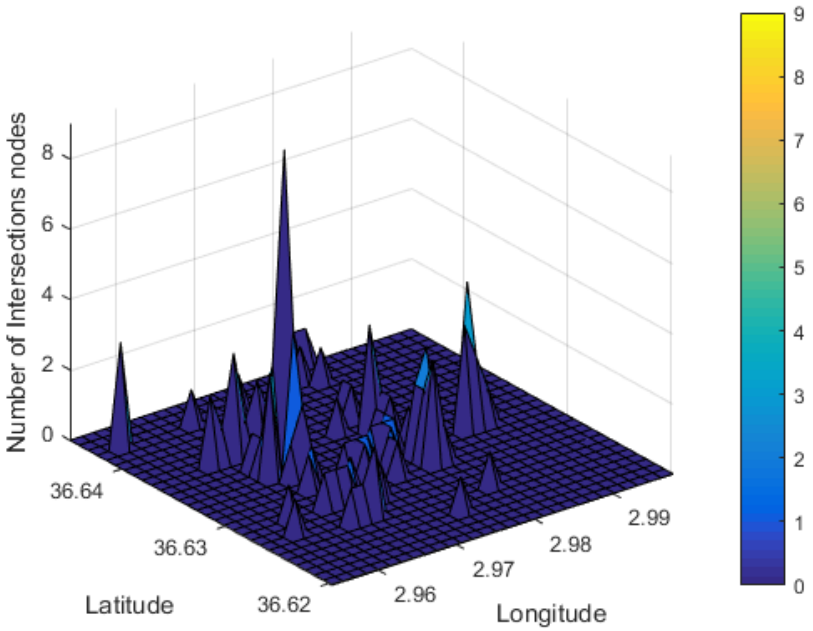


Figure 4.10: 3D Heatmap histogram of geometric circles method–dataset B

- **Dataset-C**

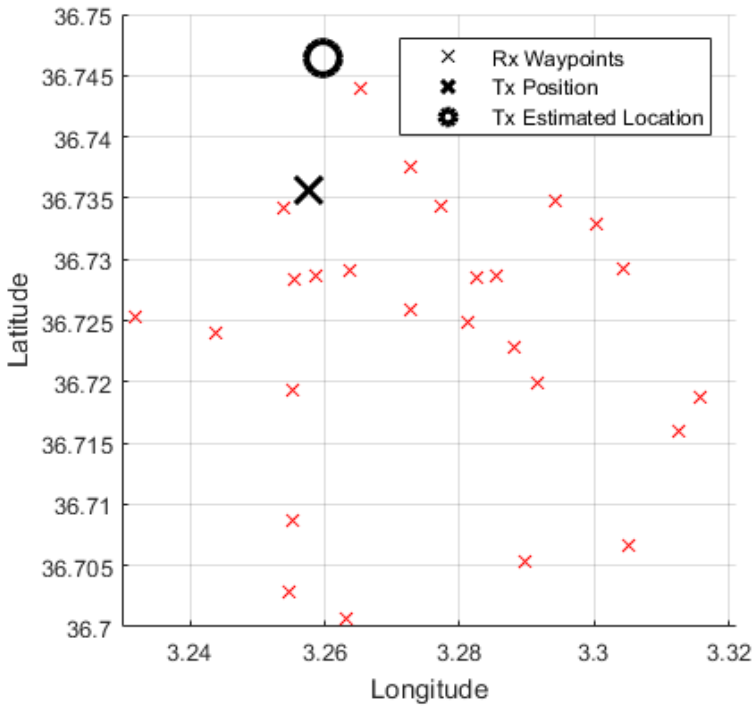


Figure 4.11: Diagram of geometric circles method–dataset-C

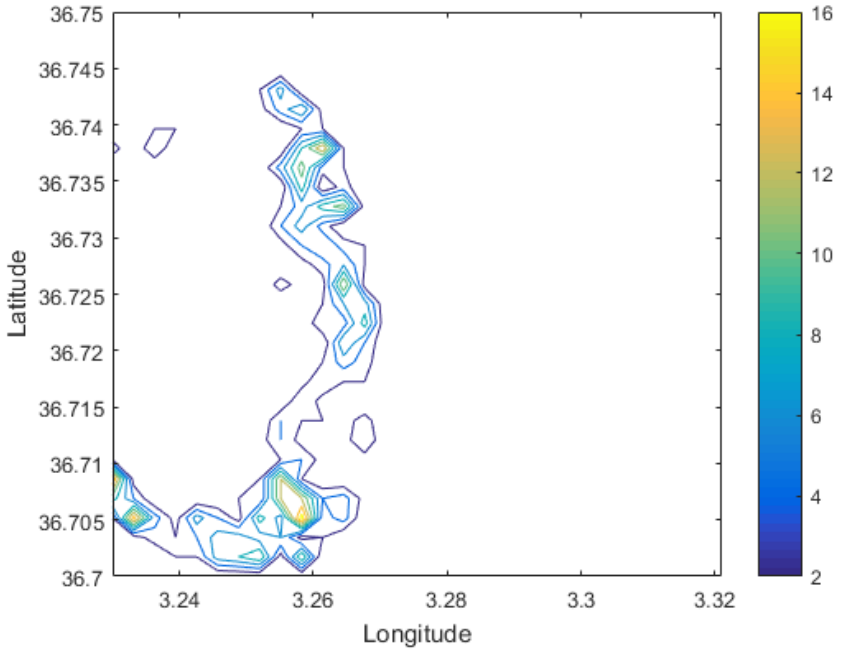


Figure 4.12 Contour map of geometric circles method–dataset-C

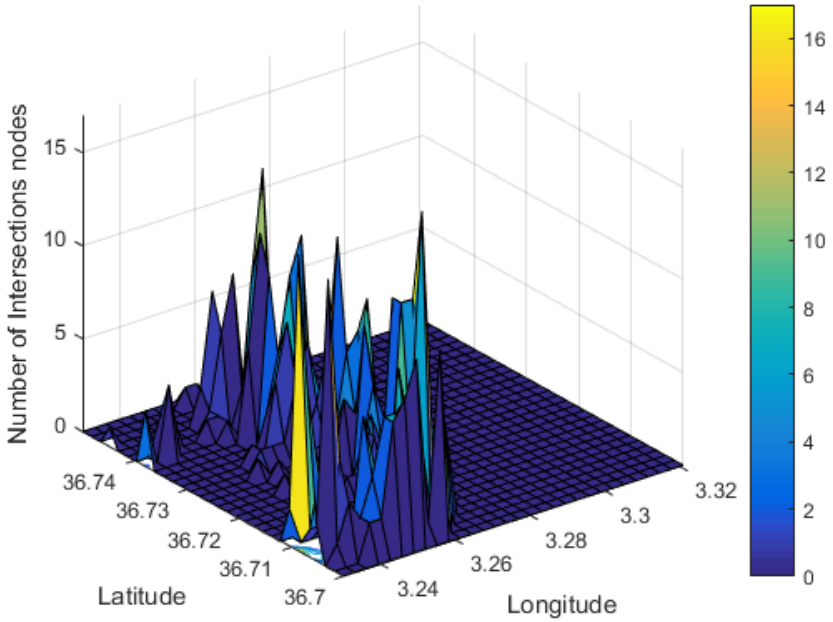


Figure 4.13: 3D Heatmap histogram of geometric circles method–dataset-C

- **Dataset-D**

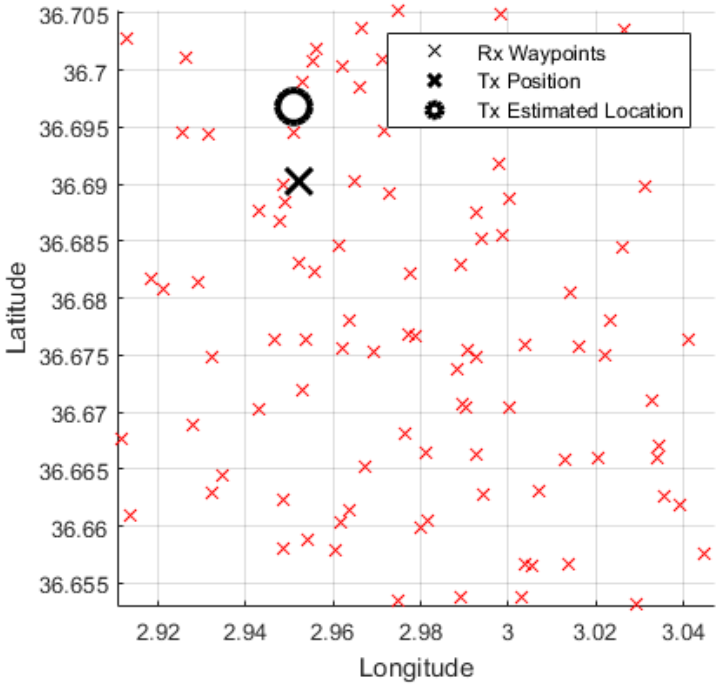


Figure 4.14: Diagram of geometric circles method–dataset-D

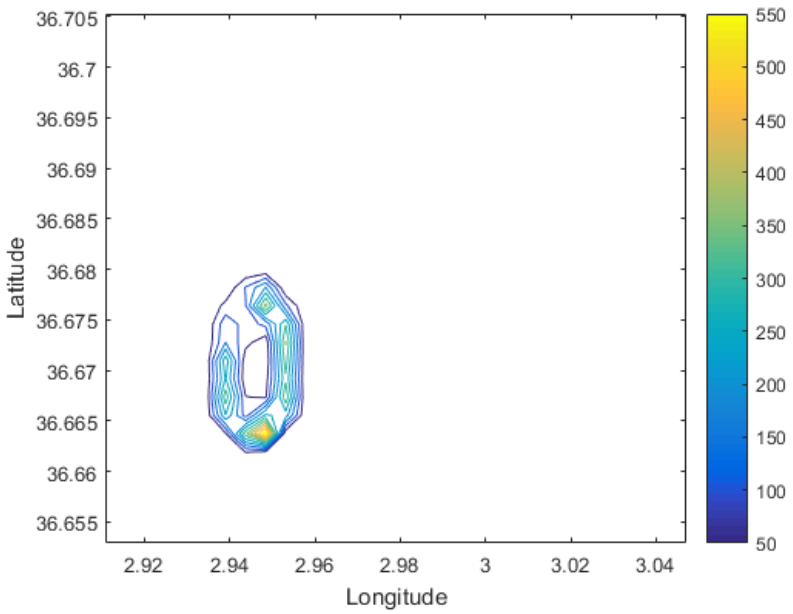


Figure 4.15: Contour map of geometric circles method–dataset-D

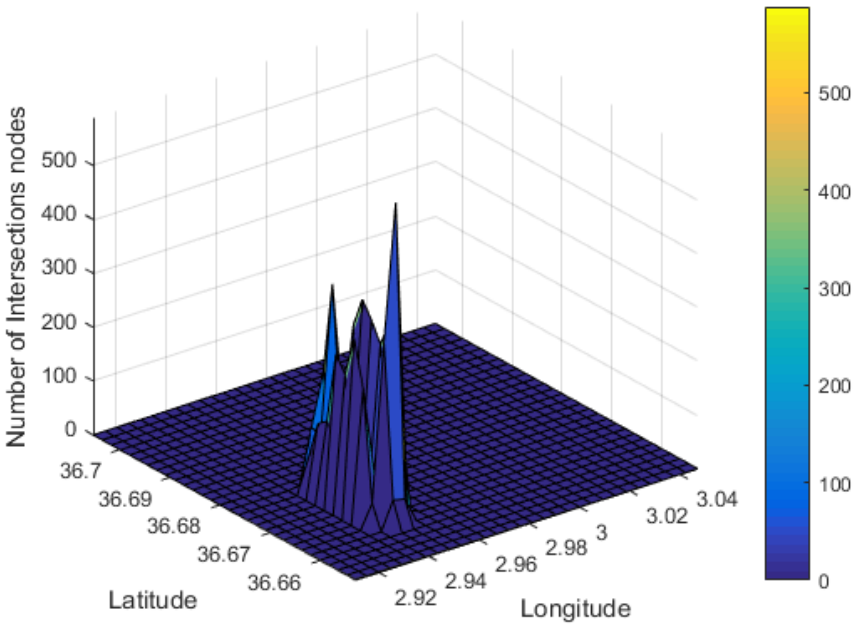


Figure 4.16: 3D Heatmap histogram of geometric circles method dataset-D

Chapter 5

Newton Raphson iterative method

The name "Newton's method" is derived from Isaac Newton's description of a special case of the method in (De analysi per aequationes numero terminorum infinitas -written in 1669, published in 1711 by William Jones) and in (De metodis fluxionum et serierum infinitarum - written in 1671, translated and published as Method of Fluxions in 1736 by John Colson). However, his method differs substantially from the modern method used in this thesis: Newton applies the method only to polynomials. He does not compute the successive approximations x_n, but computes a sequence of polynomials, and only at the end arrives at an approximation for the root x. Finally, Newton views the method as purely algebraic and makes no mention of the connection with calculus. Newton may have derived his method from a similar but less precise method by the French mathematician Franciscus Vieta. The essence of Vieta's method can be found in the work of the Persian mathematician Sharaf al-Din al-Tusi, while his successor Jamshīd al-Kāshī used a form of Newton's method to solve $(x^P - N) = 0$ to find roots of N (Ypma 1995). A special case of Newton's method for calculating square roots was known since ancient times and is often called the Babylonian method.

Newton's method was used by 17th-century Japanese mathematician Seki Kōwa to solve single-variable equations, though the connection with calculus was missing.

Newton's method was first published in 1685 in (A Treatise of Algebra both Historical and Practical) by John Wallis

In 1690, Joseph Raphson published a simplified description in (Analysis aequationum universalis). Raphson again viewed Newton's method purely as an algebraic method and restricted its use to polynomials, but he describes the method in terms of the successive approximations x_n instead of the more complicated sequence of polynomials used by Newton. Finally, in 1740, Thomas Simpson described Newton's method as an iterative method for solving general nonlinear equations using calculus, essentially giving the description above. In the

same publication, Simpson also gives the generalization to systems of two equations and notes that Newton's method can be used for solving optimization problems by setting the gradient to zero.

5.1 Method demonstration

Arthur Cayley in 1879 in The Newton–Fourier imaginary problem was the first to notice the difficulties in generalizing Newton's method to complex roots of polynomials with degree greater than 2 and complex initial values. This opened the way to the study of the theory of iterations of rational functions.
Briefly, the method is a root-finding algorithm which produces successively better approximations to the roots (or zeroes) of a real-valued function. The most basic version starts with a single-variable function f defined for a real variable (x), the function's derivative f', and an initial guess x_0 for a root of f. If the function satisfies sufficient assumptions and the initial guess is close, then

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$$

Is a better approximation of the root than x_0. Geometrically, $(x_1, 0)$ is the intersection of the x-axis and the tangent of the graph of f at $(x_0, f(x_0))$: that is, the improved guess is the unique root of the linear approximation at the initial point. The process is repeated as:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

Until a sufficiently precise value is reached. This algorithm is first in the class of Householder's methods, succeeded by Halley's method. The method can also be extended to complex functions and to systems of equations.

A large error in the initial estimate can contribute to non-convergence of the algorithm. To overcome this problem one can often linearise the function that is being optimized using calculus, logs, differentials, or even using evolutionary algorithms, such as the stochastic funnel algorithm Good initial estimates lie close

to the final globally optimal parameter estimate. The initial guess for newton vector is the minimum longitude value associated with minimum latitude value.
In nonlinear regression, the sum of squared errors is only "close to" parabolic in the region of the final parameter estimates. Initial estimates found here will allow the Newton–Raphson method to quickly converge. It is only here that the Hessian matrix of the sum of squared errors is positive and the first derivative of the sum of squared errors is close to zero.
When dealing with nonlinear systems of equations that has *k* variables and *k* functions
One may also use Newton's method to solve systems of *k* (nonlinear) equations, which amounts to finding the zeroes of continuously differentiable functions *(F):* $\mathbb{R}^k \to \mathbb{R}^k$. In the formulation given above, one then has to left multiply with the inverse of the $k \times k$ Jacobian matrix $J_F(x_n)$instead of dividing by $f'(x_n)$:

$$x_{n+1} = x_n - J_F(x_n)^{-1} F(x_n)$$

Rather than actually computing the inverse of the Jacobian matrix, one can save time by solving the system of linear equations [13, 14]

$$J_F(x_n)(x_{n+1} - x_n) = -F(x_n)$$

For the unknown $x_n + 1 - x^n$

As said earlier, the thesis is based on Friis transmission equation, let's consider e_i as individual loss coefficients for each observation.

$$d_i \frac{e_i}{2}$$

Introduce a distance squared term in space as:

$$d_i \triangleq (x_i - x_0)^2 + (y_i - y_0)^2 + (z_i - z_0)^2$$

In 2 dimensions, the equation becomes:

$$d_i \triangleq (x_i - x_0)^2 + (y_i - y_0)^2$$

x_i and y_i represents waypoints of measurements and x_0 and y_0 for the transmitter location. Terms that are not concerns in this model such as antennas gains and wavelength to form are excluded.

$$p_i = \frac{p_t}{[(x_i - x_0)^2 + (y_i - y_0)^2]^{\frac{e_i}{2}}}$$

Then the equation becomes:

$$p_i d_i^{\frac{e_i}{2}} - p_0 = 0$$

This function named J_i defined as a cost function for all observations

$$J_i(x_0, y_0, p_0) = p_i d_i^{\frac{e_i}{2}} - p_0$$

The following step is to reduce the size of the cost function. It is simpler to reduce the magnitude squared, and every J_i term should contribute to the overall cost, so sum ${J_i}^2 \forall i$. The new cost function for each individual observation cost is:

$$J_i(x_0, y_0, p_0) = \sum_{\forall i} {J_i}^2$$

Attempt to minimize the cost function in order to bring it as near to zero as possible.

This model allows for changes in x_0, y_0, and p_0 while keeping the loss coefficients e_i constant

Using Newton's technique to determine the minimum by finding the roots of the derivative. For a function of multiple variables, the first derivative′(x), turns into a gradient, and the second derivative′′(x), turns into a Hessian matrix.

The equation becomes then:

$$x^{n+1} = x^n - (\nabla^2 J(x^n))\ \ {}^1\nabla J(x^n)$$

Where $\nabla J(x^n)$ is the gradient, and $\nabla^2 J(x^n)$is the Hessian.

$$\nabla J = \begin{bmatrix} \frac{\partial J}{\partial x_0} \\ \frac{\partial J}{\partial y_0} \\ \frac{\partial J}{\partial p_0} \end{bmatrix}$$

$$\frac{\partial J}{\partial x_0} = 2\sum_i p_i e_i (x_0 - x_i)[\, p_i {d_i}^{e_i - 1} - p_0 {d_i}^{\frac{e_i}{2} - 1}]$$

$$\frac{\partial J}{\partial y_0} = 2\sum_i p_i e_i (y_0 - y_i)[\, p_i {d_i}^{e_i\ 1} - p_0 {d_i}^{\frac{e_i}{2}\ 1}]$$

$$\frac{\partial J}{\partial p_0} = 2\sum_i [\, p_0 - p_i {d_i}^{\frac{e_i}{2}}]$$

$$\nabla^2 J = \begin{bmatrix} \frac{\partial^2 J}{\partial x_0 \partial x_0} & \frac{\partial^2 J}{\partial x_0 \partial y_0} & \frac{\partial^2 J}{\partial x_0 \partial p_0} \\ \frac{\partial^2 J}{\partial y_0 \partial x_0} & \frac{\partial^2 J}{\partial y_0 \partial y_0} & \frac{\partial^2 J}{\partial y_0 \partial p_0} \\ \frac{\partial^2 J}{\partial p_0 \partial x_0} & \frac{\partial^2 J}{\partial p_0 \partial y_0} & \frac{\partial^2 J}{\partial p_0 \partial p_0} \end{bmatrix}$$

$\frac{\partial^2 J}{\partial x_0 \partial x_0} = 4\sum_i p_i e_i [\, p_i {d_i}^{e_i\ 1} - p_0 {d_i}^{\frac{e_i}{2}\ 1}] + 2 p_i e_i (x_0 - x_i)^2 [p_i (e_i - 1) {d_i}^{e_i\ 2} - p_0 (\frac{e_i}{2} - 1) {d_i}^{\frac{e_i}{2}\ 2}]$

$\frac{\partial^2 J}{\partial y_0 \partial y_0} = 4\sum_i p_i e_i [\, p_i {d_i}^{e_i - 1} - p_0 {d_i}^{\frac{e_i}{2} - 1}] + 2 p_i e_i (y_0 - y_i)^2 [p_i (e_i - 1) {d_i}^{e_i - 2} - p_0 (\frac{e_i}{2} - 1) {d_i}^{\frac{e_i}{2}\ 2}]$

$\frac{\partial^2 J}{\partial x_0 \partial y_0} = \frac{\partial^2 J}{\partial y_0 \partial x_0} = 4\sum_i p_i e_i (x_0 - x_i)(y_0 - y_i)\, [p_i (e_i - 1) {d_i}^{e_i\ 2} - p_0 (\frac{e_i}{2} - 1)\, {d_i}^{\frac{e_i}{2}\ 2}]$

$$\frac{\partial^2 J}{\partial x_0 \partial p_0} = \frac{\partial^2 J}{\partial p_0 \partial x_0} = -2\sum_i p_i e_i (x_0 - x_i)[\, {d_i}^{\frac{e_i}{2} - 1}]$$

$$\frac{\partial^2 J}{\partial y_0 \partial p_0} = \frac{\partial^2 J}{\partial p_0 \partial y_0} = -2\sum_i p_i e_i (y_0 - y_i)[\, {d_i}^{\frac{e_i}{2} - 1}]$$

$$\frac{\partial^2 J}{\partial p_0 \partial p_0} = 2\sum_i 1 = 2 * i \ mesurements$$

Whenever the loss coefficients are limited to 2 for all observations, the gradient and Hessian become much simpler to compute, this cancels out many of the more complex terms.

Gradient after simplification:

$$\frac{\partial J}{\partial x_0} = 4\sum_i p_i(x_0 - x_i)(p_i d_i - p_0)$$

$$\frac{\partial J}{\partial y_0} = 4\sum_i p_i(y_0 - y_i)(p_i d_i - p_0)$$

$$\frac{\partial J}{\partial p_0} = 2\sum_i (p_0 - p_i d_i)$$

Hessian after simplification:

$$\frac{\partial^2 J}{\partial x_0 \partial x_0} = 4\sum_i p_i(p_i d_i - p_0) + 2{p_i}^2(x_0 - x_i)^2$$

$$\frac{\partial^2 J}{\partial x_0 \partial y_0} = 8\sum_i {p_i}^2 (x_0 - x_i)(y_0 - y_i)^2$$

$$\frac{\partial^2 J}{\partial x_0 \partial p_0} = -4\sum_i p_i (x_0 - x_i)$$

$$\frac{\partial^2 J}{\partial y_0 \partial y_0} = 4\sum_i p_i(p_i d_i - p_0) + 2{p_i}^2(y_0 - y_i)^2$$

$$\frac{\partial^2 J}{\partial y_0 \partial p_0} = -4\sum_i {p_i}^2 (y_0 - y_i)$$

$$\frac{\partial^2 J}{\partial y_0 \partial x_0} = \frac{\partial^2 J}{\partial x_0 \partial y_0} \ ; \ \frac{\partial^2 J}{\partial p_0 \partial x_0} = \frac{\partial^2 J}{\partial x_0 \partial p_0}$$

$$\frac{\partial^2 J}{\partial p_0 \partial y_0} = \frac{\partial^2 J}{\partial y_0 \partial p_0} \ ; \ \frac{\partial^2 J}{\partial y_0 \partial p_0} = 2\sum_i 1 = 2 * i \ mesurments$$

Initial guess estimations for the loss coefficients are not known for real space datasets, this initialization,$e_i = 2$ will be utilized frequently throughout this method Additionally, the maximum number of iterations chosen is 10 since after

numerous simulation attempts, the final estimate does not needs more iteration for approximations.

The result demonstrates the influence on the overall quality of final estimate and a valuable evaluation experimentally [15].

5.2 Newton Raphson iterative algorithm

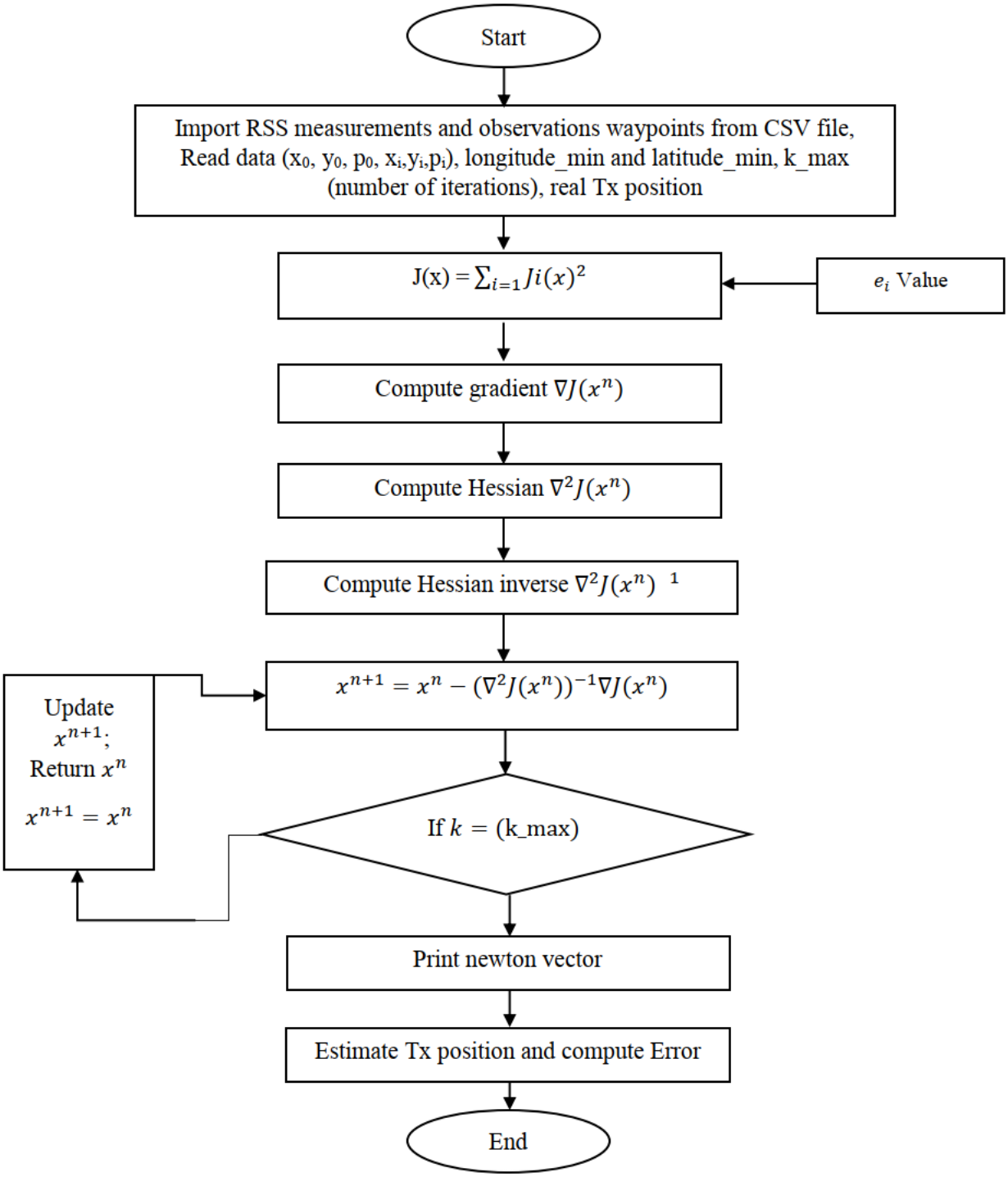


Figure 5.1: Newton Raphson iterative method flowchart

5.3 Results

Table 5.1: Newton Raphson iterative method efficiency

Dataset	*Searching area*	*Errors (meters)*
A	*164.139 km²*	*916.90*
B	*10.933 km²*	*244.53*
C	*45.049 km²*	*47.52*
D	*70.755 km²*	*160.11*

- **Dataset A**

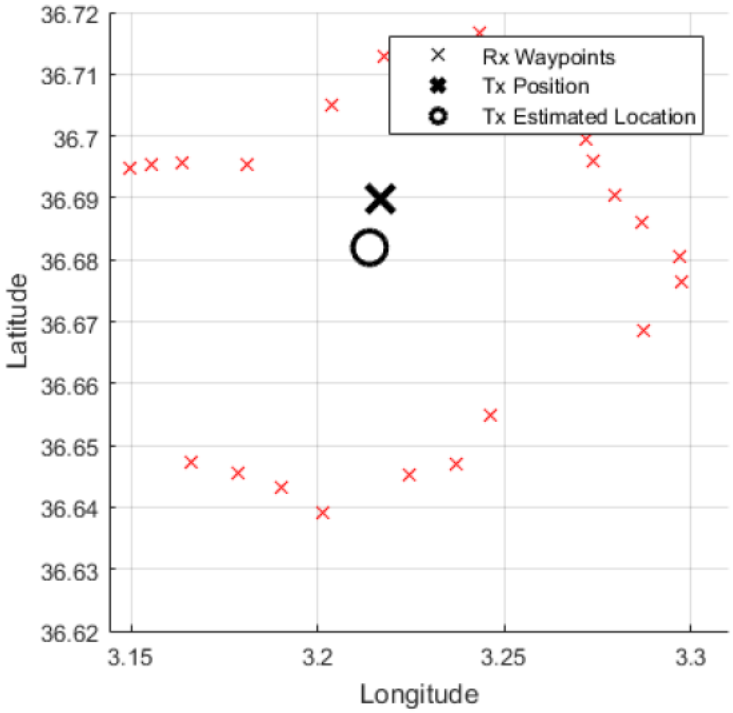


Figure 5 2: Diagram of Newton Raphson iterative method dataset-A

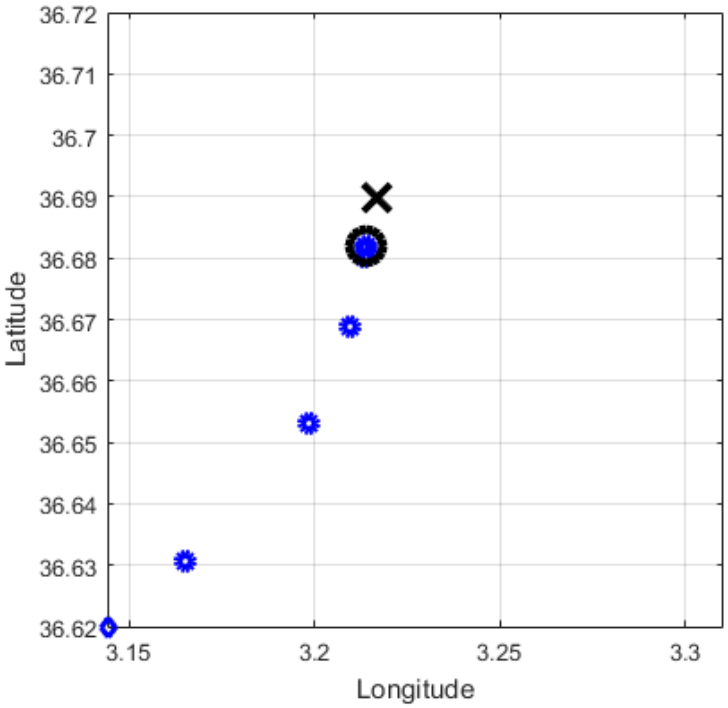


Figure 5.3: Illustration of Newton Raphson iterative method steps–dataset-A

The figure above illustrates newton vector iterations with blue markers

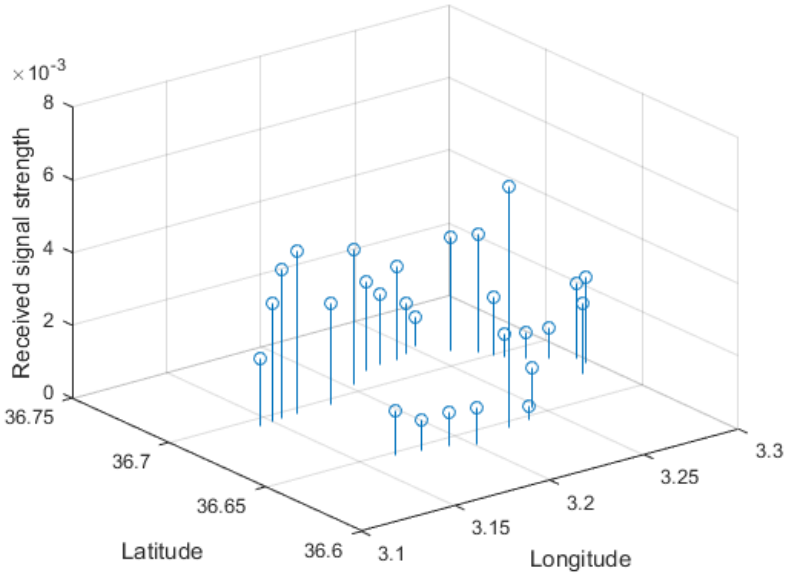


Figure 5 4: RSS illustration of input arguments for dataset A

- **Dataset-B**

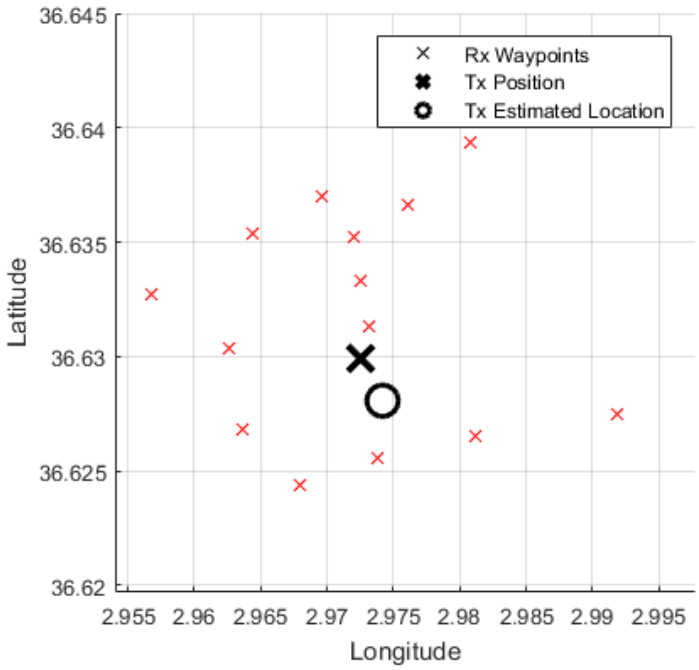


Figure 5.5: Diagram of Newton Raphson iterative method–dataset-B

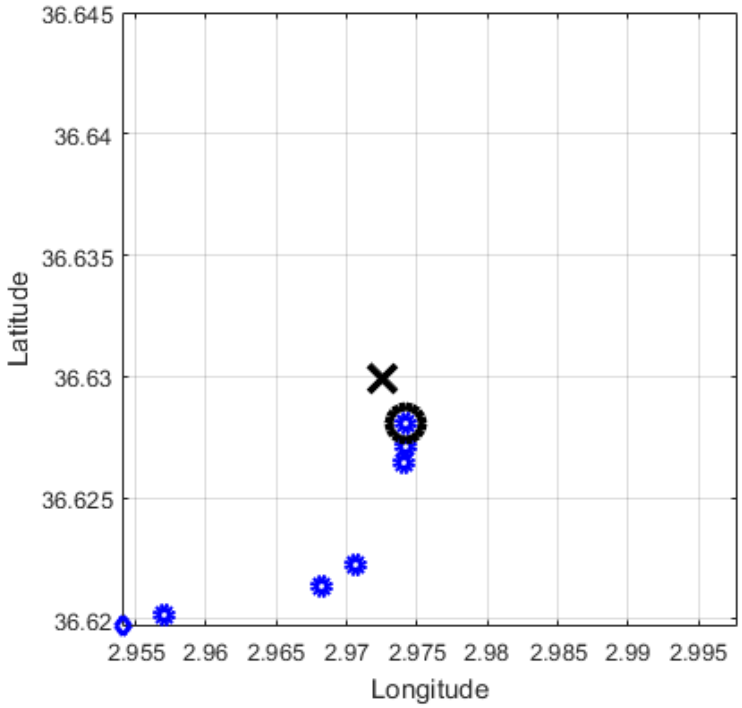


Figure 5 6: Illustration of Newton Raphson iterative method steps–dataset B

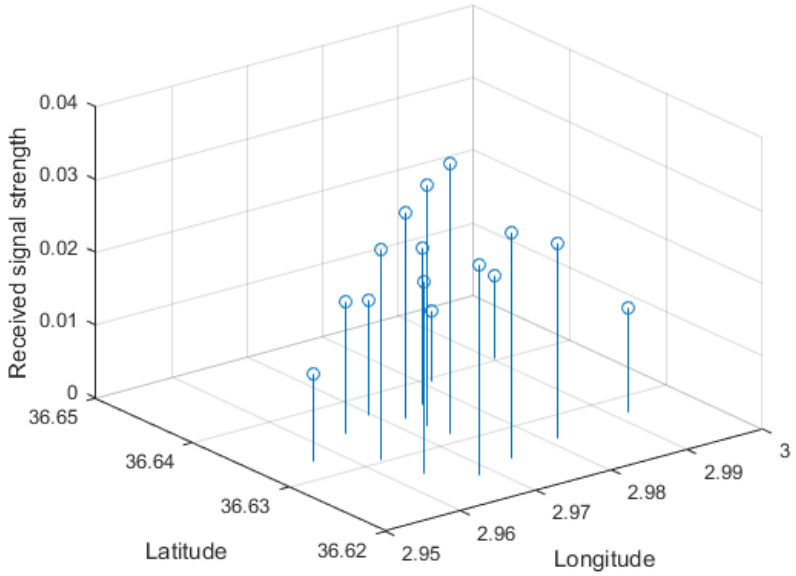


Figure 5.7: RSS illustration of input arguments for dataset-B

- **Dataset-C**

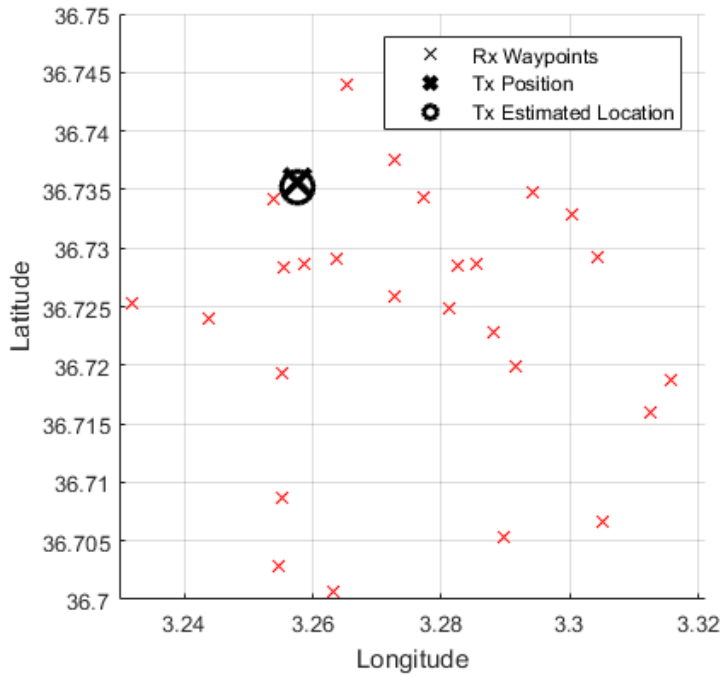


Figure 5.8: Diagram of Newton Raphson iterative method–dataset-C

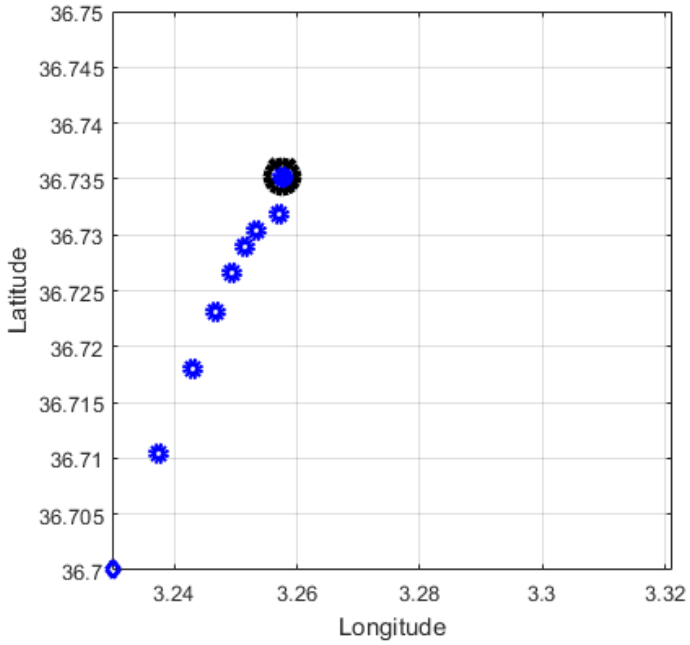


Figure 5.9: Illustration of Newton Raphson iterative method steps–dataset-C

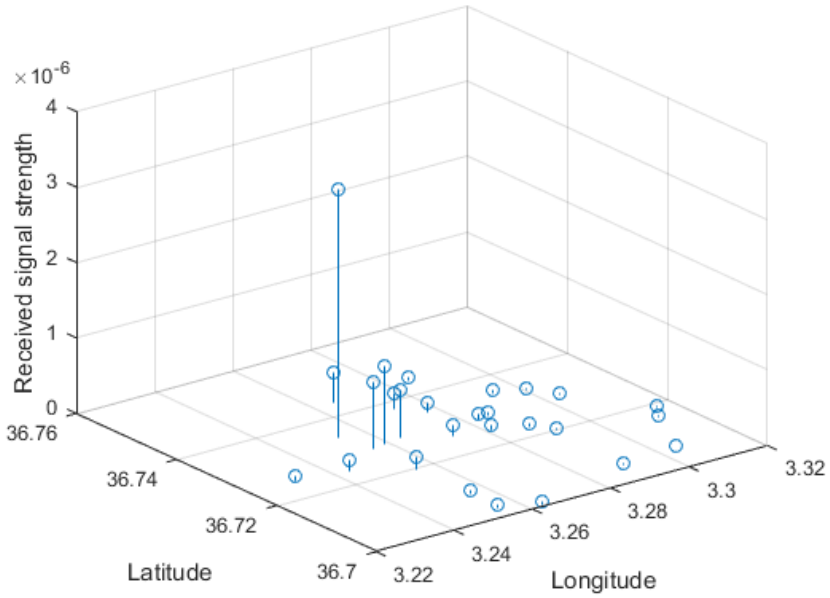


Figure 5.10: RSS Illustration of input arguments for dataset-C

- **Dataset -D**

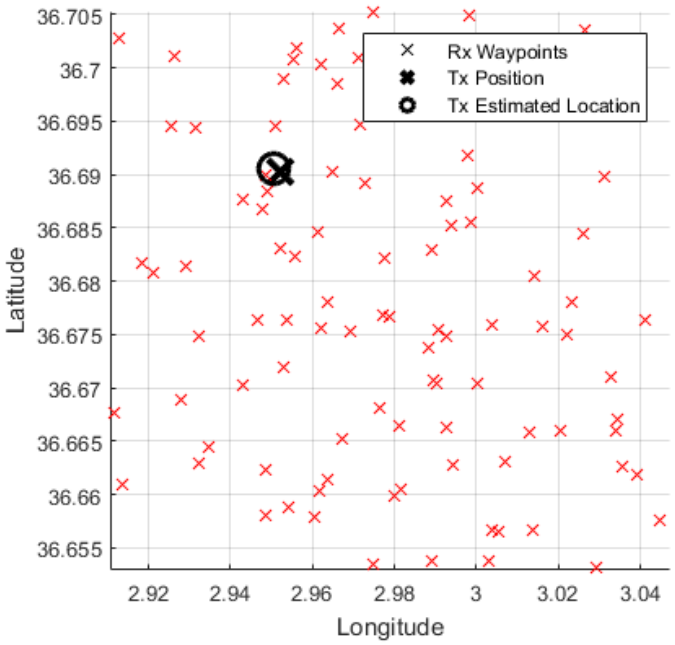


Figure 5.11: Diagram of Newton Raphson iterative method dataset-D

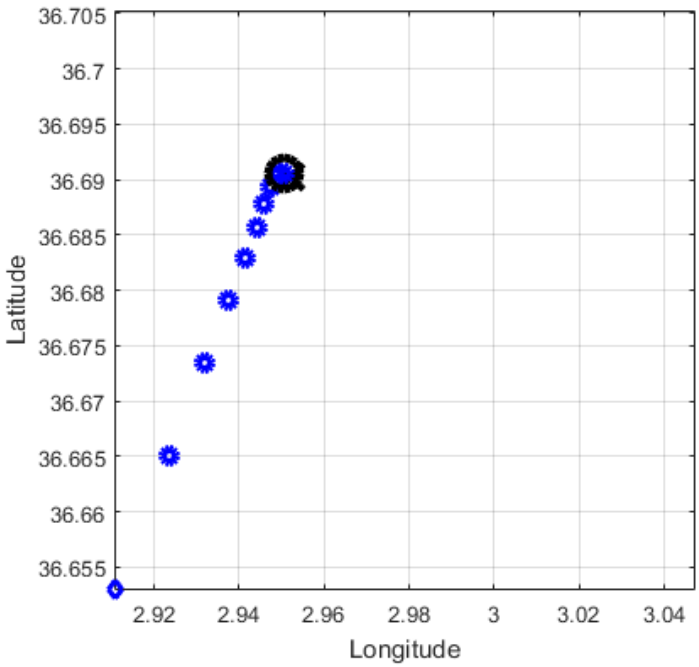


Figure 5.12: Illustration of Newton Raphson iterative method steps–dataset-D

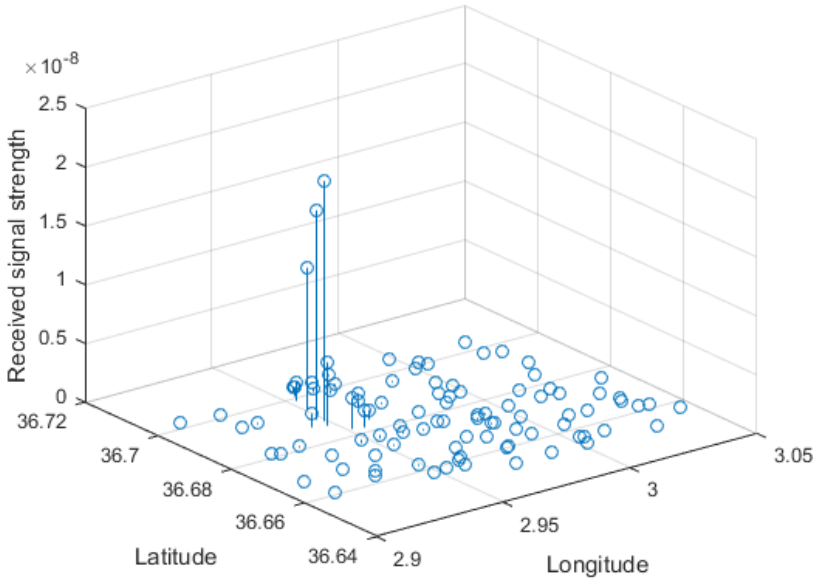


Figure 5.13: RSS illustration of input arguments for dataset-D

Chapter 6

General Conclusions

This chapter provides a summary of the major results of the work, along with why it is significant and what further actions and research possibilities that can be taken to improve and advance the work.

Methods Comparison

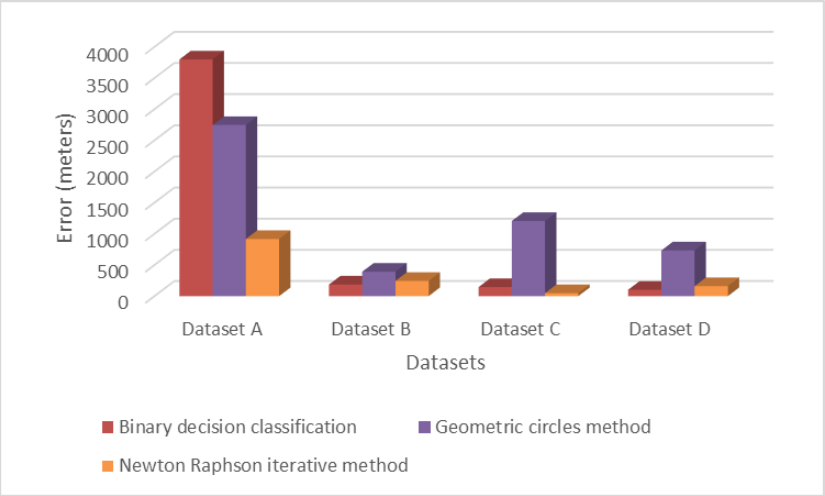


Figure 6.1: Error comparison by dataset in meters

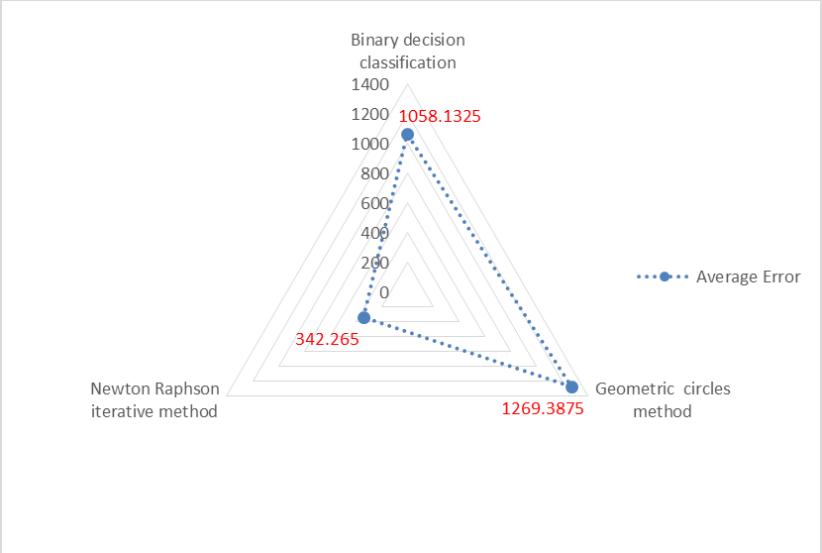


Figure 6.2: Radar chart demonstrating average error in meters for studied methods

The illustration, above *(figure 6 1)*, is a histogram showing results of a final trials. Each method is denoted by a bar of a certain color, evaluate position estimation errors for all the studied datasets. If this histogram were compared between different datasets environments, the result is more favorable for LOS situation, since all methods have noted average error below 500 meters.
Dataset (A) is in NLOS situation, and recorded a high error margin due to loss coefficients variations and a large area of interest (164.139 km^2).
An evident improvement expected to reduce error margin, when implementing suitable approximations of loss coefficients values for each observation.
If this histogram were compared to disclose methods effectiveness, Newton Raphson iterative method manifests an excellent results, the average error for entire datasets is adequate *(figure 6.2)*. Geometric circles method has recorded a poor average results
The worse estimate was noted for binary decision classification method in NLOS situation.

Conclusion

Geolocation of uncooperative RF transmitter is possible using received signal strength based on free space modelization in a noisy environment. Employing multiple distributed observations, while minimizing resource-consumption using a cheap RTL-SDR dongle is a challenging achievement to get an accurate estimate. Despite the fact that the results obtained are acceptable globally and reduce significantly searching area in LOS environment. The methods are not adapted well for NLOS environments for precise outdoor geolocation. Solving this problem using only Friis transmission equation is strenuous and needs additional algorithmic steps to reduce error margin for final position estimation. Even so, the work has been a valuable experience when demonstrating multiple optimization methods for real-world applications. In some situations, it is possible to reduce the effect of noise by avoiding buildings and obstacles situated between the transmitter and the receiver, to provide an accurate and realistic results
Furthermore, in a special scenario, there will likely be more than a single emitter, the legitimate one and the hostile one.

Distinguishing multiple emitters on the same centered frequency is a challenge that has not be considered in this work. Further work including signal processing is required in the section of separating and classifying multiple transmitters in a noisy radio frequency environment.
The simulated data with a loss coefficient superior than 2, demonstrates uniform path loss model which is different from real outdoor situation. This work turned out to be an exercise in examining the behaviour of sampled data at the receiver side and evaluating receiver capability too.

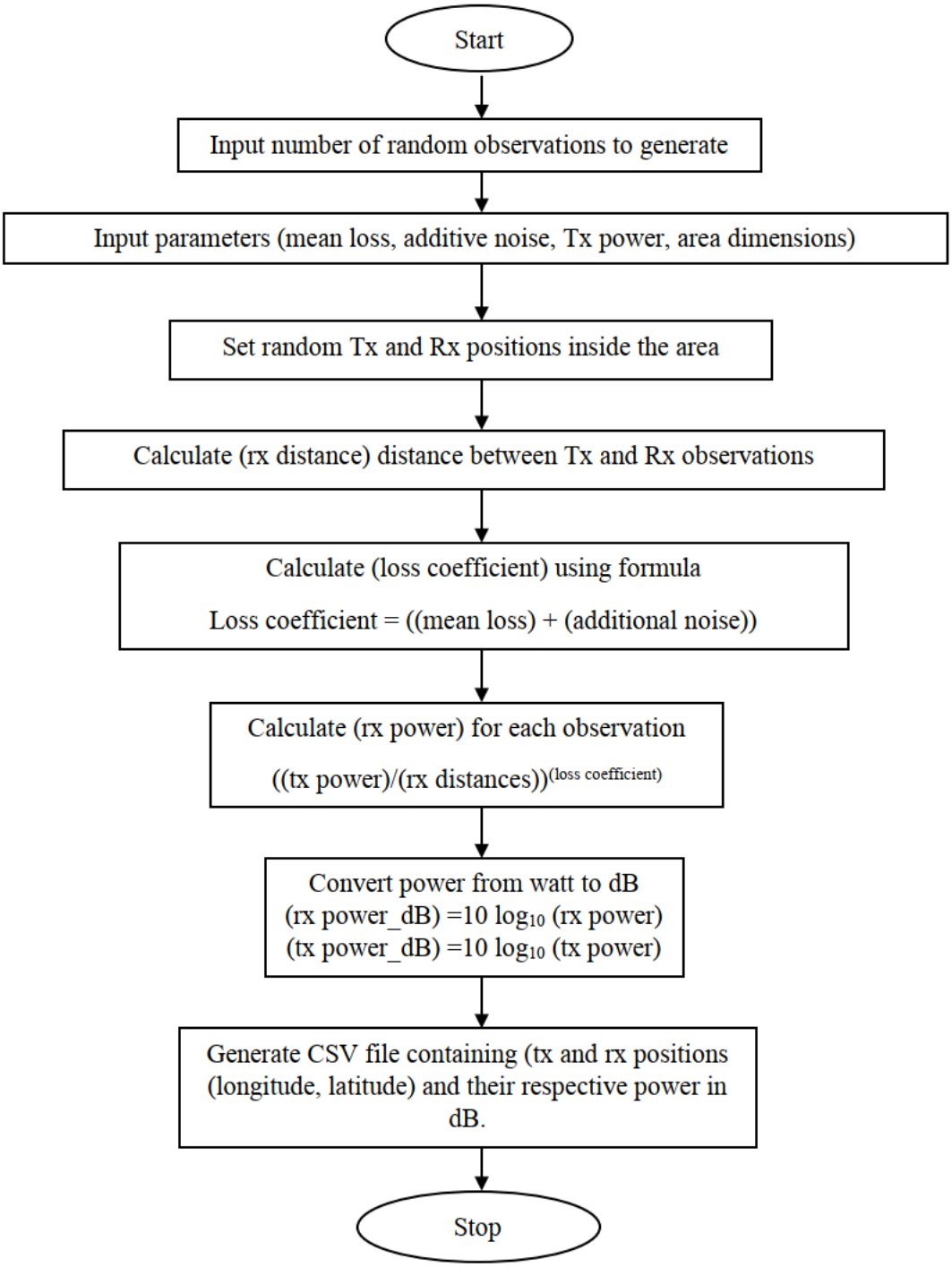
There is a correlation between distance to the transmitter and prediction accuracy. To maximize prediction accuracy, making at least one observation close to the transmitter is a good strategy, more advanced effort and time is needed to do so, and a higher number of observation is privileged. Generally, being closer to the emitter, will allow measuring high received signal strength. Therefore, noise will be less significant and predictions become very accurate.

Applying a theoretical studies, such as this, to the real world cases needs supplementary considerations for each different situation Even if the results therefore are acceptable for certain environments, there may be another aspects or issues that have not been taken into account in this work. In other words, even a theoretically implementation sounds accurate, it may encounter problems when put into practice.

Future work

This research initiates many possibilities for further research, I advocate algorithm development, to evaluate significally power loss coefficient for each measurement.
Designing a powerful VHF antenna to improve RF signal reception. Run direct sampling mode with a hardware modification to tune to the HF frequencies. Involve UAVs to estimate transmitter's elevation. Implement active measurement process and synchronize dongles to perform DoA-ToA-TDoA geolocation methods.
Additional work could be done to implement these algorithms in such a way that allows monitoring a mobile transmitter.
Active measurements could be utilized with a Kalman filter to enhance estimations.

Appendix - Flowchart for generating simulation datasets



References

[1] Curt A. Levis, Joel T. Johnson, Fernando L. Teixeira Wiley, “Radiowave propagation: physics and applications” ISBN 978-0-470-54295-8, 2010, pp.1-12.

[2] Small, Andrew J., "Radio Frequency Emitter Geolocation Using Cubesats”, 2014.Theses and Dissertations. 624. [Online]. Available: https://scholar.afit.edu/etd/624

[3] An Efficient Approach for Localization using Trilateration Algorithm based on Received Signal Strength in Wireless Sensor Network Niharika Singh Matharu Avtar Singh Buttar ECE Department Punjab Institute of Technology Kapurthala, India, IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8, August 2016.

[4] Camillo Gentile, Nayef Alsindi, Ronald Raulefs, Carole Teolis “Geolocation Techniques Principles and Applications”, 2012 ISBN 978-1-4614-1836-8.

[5] Mr. Carl Laufer, “The Hobbyist's Guide to the RTL-SDR: Really Cheap Software Defined Radio 1st Edition”, 2014, ISBN-13: 978-1514716694.

[6] Dennis Mantz, Tom Swartz, “Spectrum Analyzer for Android using the HackRF” [Online]. Available: https://github.com/demantz/RFAnalyzer

[7] “Binary classification”, [Website] Avalable: https://en.wikipedia.org/wiki/Binary classification

[8] Paul Scerri, Robin Glinton, Sean Owens, David Scerri and Katia Sycara, “Geolocation of RF Emitters by Many UAVs”, School of Computer Science Carnegie Mellon University Pittsburgh, PA 15213, USA.

[9] J. Macqueen, “Some methods for classification and analysis of multivariate observations,” in Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Statistics. Berkeley, Calif.: University of California Press, 1967, pp. 281–293

[10] P Brída, P Čepel, J Dúha, “Geometric Algorithm for Received Signal Strength Based Mobile Positioning” VOL. 14, NO. 1, APRIL 2005.

[11] Niharika Singh, Matharu Avtar, Singh Buttar, “An Efficient Approach for Localization using Trilateration Algorithm based on Received Signal Strength in Wireless Sensor Network - IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8, August 2016.

[12] Federico Librino, M. Levorato, Michele Zorzi, “An algorithmic solution for computing circle intersection areas and its applications to wireless communications”, Conference: Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2009. WiOPT 2009. 7th International Symposium.

[13] Gil, A.; Segura, J.; Temme, N. M. (2007). Numerical methods for special functions (https://www.researchgate.net/profile/Nico_Temme/publication/220693008_Numerical_Methods_for_Special_Functions/links/0912f5093e6b002a3d000000.pdf) (PDF). Society for Industrial and Applied Mathematics. ISBN978-0-89871-634-4.

[14] Süli, Endre; Mayers, David (2003). An Introduction to Numerical Analysis. Cambridge University Press. ISBN0-521-00794-1.

[15] Adrian Lam, “Demystifying the inner workings of BFGS optimization”, [Website]: https://towardsdatascience.com/bfgs-in-a-nutshell-an-introduction-to-quasi-newton-methods