Open University of Cyprus

Faculty of Pure and Applied Sciences

Postgraduate Dissertation
On Information and Communication Systems

Wireless Tracking and Positioning Radar System
In Wireless Networks

Alexandros Kritikopoulos

Project Supervisor Professor
Dr. Stavros Stavrou

May 2012

Open University of Cyprus

Faculty of Pure and Applied Sciences

Wireless Tracking and Positioning Radar System
In Wireless Networks

Alexandros Kritikopoulos

Project Supervisor Professor
Dr. Stavros Stavrou

This thesis was presented
in partial fulfilment of the requirements for obtaining
a postgraduate degree
in Information Systems
from the School of Pure and Applied Sciences
of Open University of Cyprus

May 2012

Abstract

Wireless communication was invented with the main goal of allowing a free wire channel communication over a medium (air) between devices with final purpose the exchange of information. Along with the deployment of wireless communication in nearly every day life electronic device rising from home appliances, cars, smartphone's and thousands more, the rapid increase of wireless communication brought along many challenges like security, benefits like mobility but also created a hall new wireless scientific area in which by taking into account characteristics of wireless signalling like time of flight, angle of arrival, signal strength and others gave the opportunity for researchers to create and study new algorithms and to companies and developers to create new applications vary in health, safety, industry monitoring, environment and many others with final cause the localization of different devises in space.

Perhaps the most well known system that emerged is GPS which is a wireless outdoor positioning system. Due to the complexity, the price and the fact that GPS is not functioning well in indoor spaces and recent advances in wireless technology gave the ability for creation of indoor wireless positioning systems based on the previous mentioned characteristics of wireless communication.

The purpose of this project is to create such a system based on values of WLAN received signal strength (RSSI) using mid range hardware devices available to everyone and open source tools. The system will compare RSSI signals values obtained at run-time (at an unknown position) with the ones collected during an off-line survey phase (fingerprint database) and also a second purpose is to investigate the accuracy and quality of the algorithm Nearest Neighbor RSS Location Method. One third goal is to investigate the effect and the impact of the position of a laptop screen (laptop angle) against on how the laptop finally receives the RSSI signal due to the fact that most laptops have the wireless card embedded in their screen.

Περίληψη

Η ασύρματη επικοινωνία επινοήθηκε με κύριο στόχο να επιτραπεί η επικοινωνία μέσω ενός ασύρματου καναλιού (αέρα) μεταξύ συσκευών με τελικό σκοπό την ανταλλαγή πληροφοριών. Μαζί με την ανάπτυξη της ασύρματης επικοινωνίας και την εφαρμογή της σε καθημερινές ηλεκτρονικές συσκευές όπως οικιακές συσκευές, αυτοκίνητα, smartphone και χιλιάδες άλλες, η ταχεία αύξηση της ασύρματης επικοινωνίας έφερε μαζί της πολλές προκλήσεις, όπως ασφάλεια αλλά και οφέλη, όπως η κινητικότητα. Επίσης δημιούργησε ένα νέο επιστημονικό κόσμο που βασίζεται στην ασύρματη τεχνολογία. Οι ερευνητές λαμβάνοντας υπόψη τα χαρακτηριστικά της ασύρματης σηματοδότησης όπως το χρόνο πτήσης, τη γωνία άφιξης, την ισχύ του σήματος και άλλα έχουν την ευκαιρία να δημιουργήσουν και να μελετήσουν νέους αλγόριθμους, εταιρείες και προγραμματιστές να δημιουργήσουν νέες εφαρμογές οι οποίες ποικίλλουν από την υγεία, την ασφάλεια, την παρακολούθηση της βιομηχανίας, θέματα περιβάλλοντος και πολλές άλλες, με τελικό σκοπό την εντόπιση μιας συσκευής σε ένα προδιαγραμμένο χώρο όπως ένα χάρτη.

Ίσως το πιο γνωστό σύστημα ραδιοεντοπισμού που προέκυψε είναι το GPS, το οποίο είναι ένα ασύρματο υπαίθριο σύστημα εντοπισμού θέσης. Λόγω της πολυπλοκότητας, η τιμή και το γεγονός ότι το GPS δεν λειτουργεί καλά σε εσωτερικούς χώρους αλλά επίσης και οι πρόσφατες εξελίξεις στην ασύρματη τεχνολογία έχουν δώσει τη δυνατότητα για τη δημιουργία εσωτερικών ασύρματων συστημάτων εντοπισμού θέσης με βάση τα παραπάνω χαρακτηριστικά της ασύρματης επικοινωνίας.

Ο σκοπός αυτής της διατριβής είναι να δημιουργηθεί ένα τέτοιο σύστημα που βασίζεται στις αξίες της ασύρματης επικοινωνίας λαμβανόμενου σήματος (RSSI), χρησιμοποιώντας φάσμα συσκευών και υλικού διαθέσιμο σε όλους και εργαλεία ανοικτού κώδικα. Το σύστημα θα συγκρίνει τις τιμές RSSI που λαμβάνονται κατά το χρόνο εκτέλεσης (σε άγνωστη θέση) με αυτά που συλλέγονται κατά τη διάρκεια μιας μη συνδεδεμένης φάση της έρευνας (βάση δεδομένων δακτυλικών αποτυπωμάτων) με σκοπό τον εντοπισμό μιας συσκευής. Επίσης, ένας δεύτερος σκοπός είναι να διερευνηθεί η ακρίβεια και η ποιότητα του αλγορίθμου τοποθεσίας πλησιέστερου γείτονα RSS. Ένας τρίτος στόχος είναι να διερευνηθεί η επίδραση και ο αντίκτυπος που έχει στα ασύρματα πακέτα η θέση της οθόνη (η οποία έχει ενσωματωμένη την ασύρματη κάρτα δικτύου) κάποιου φορητού υπολογιστή (γωνιά οθόνης) κατά πόσο αλλοιώνεται το τελικό σήμα RSSI.

Acknowledgements

I would like to thank my parents for their encouragement and financial support during my studies. Also my project advisor for his critical questions, which forced me to read more, think critically and write with better clarity and for teaching me that we learn by doing. Special thanks also go to my wife, who read my project report and helped me with the grammar and style. I would also like to express my gratitude to Panayiotis Valiandis and Nicos Theoklitou which are tow exceptional computer programmers colleague of me for their amazing knowledge and tips about networking operating environments and programming.

Table of Contents

List of Tables

The list of tables is included only if there are tables in your project report. These are listed here along with their caption (description) and the page number where they appear (see example).

List of Illustrations

Chapter 1 Introduction

1.1 Motivation

The rapid and worldwide deployment of wireless systems and networks like 3G, 4G, GPS, IEEE 808.11 b/g/n raised and created a new world of applications for mobile devices like laptops, PDA's, Smartphone's, car GPS which are based on the concept of the term localization. This kind of applications and services are called Location based services (LBSs). Some examples of such applications include navigation, people and assets tracking and guiding, security and coordination of emergency and maintenance responses to accidents and many others [2-3].

In order for those applications to work well they need accurate user coordinates of a designate area or open space environment. This is possible through the process of localization. Localization is the process of determining the physical position (coordinates) of a node or a machine.

Hence due to these applications there is a global growing interest in developing effective positioning and tracking systems. GPS and cellular mobile networks works well in outside environments but not in indoor spaces due to path loss, noise, metal and concrete obstacles and many others interference factors. Of course some variations of GPS exist today that can work well inside a close space. The Calibree model computes the distances between mobile phones that have at least one GSM cell tower in common and then construct's a graph with weight edges based on those distances and try to find the distance for future phones based on the graph [4]. Another indoor GPS is the Assisted GPS model which works by combining information's from a GPS receiver and from a server which downloads distances and coordinates from cellular bas stations [5]. Expect the fact that these methods need special GPS chipset's which cost some money are able to provide a good accurate position estimate indoors but not accurate enough in order to provide reliable LBS and also they are only applicable to mobile phones.

Also other types of wireless technologies can be deployed for indoor positioning like wireless sensors devices which records information's with the use of infrared, radio frequency, proximity sensors and ultrasound in order to detect a node with high accuracy. The downside of these wireless sensors systems is that they need special equipment and installation which costs a lot of money and this is a discourage factor that prevent there widely deployment.

With the cheap wide deployment of the wireless protocol IEEE 802.11 b/g/n in nearly every building worldwide, software developers and researchers can take advantage characteristics of the wireless protocol a build a good positioning WLAN system. Angle of Arrival (AOA), Time of arrival (TOA) and time difference of arrival (TDOA) are techniques that can be used for localization. Although these techniques have a good high accuracy they need complicate setup and configuration and in some cases special equipment in order to produce valid results. On the other hand the received signal strength indicator (RSSI) is a metric to measure the strength of an incoming signal and it can be extracted programmatically by any Access Point (AP) either directly from them AP or by software installed on it or even by a request made from a wireless client.

Finally this thesis aims to build a very low cost and as accurate as possible wireless tracking and positioning system using open source tools and systems, cheap hardware that already exist in the market world wide and that can be easily implemented in already wireless infrastructures.

1.2 Location Based Services (LSBs)

The rapid evolution of mobile phones, both on hardware and software level, combined with an explosion of highly personalized applications, high capacity cellular networks and recent developments in positioning technologies created the location based service (LBS) which basically is a software application for an IP capable mobile device that requires knowledge about where the mobile device is located. Although location-based services have been around since 2000, they have mostly been used in commerce with a subscription-based business model. The release of Apple's 3G iPhone and newer along with Google's LBS enabled Android operating system has allowed developers to introduce millions of consumers to LBS. One simple example is when type or talk to an Android Google Maps mobile phone and ask for the nearest hospital, restaurant or gas station. Traffic advisories, navigation help including maps and directions, and roadside assistance are natural location-based services. Other services can combine present location with information about personal preferences to help users find food, lodging, and entertainment to fit their tastes and pocketbooks.

1.2.1 Categories of Location Based Services (LSBs)

1.2.1.1 Global Positioning System (GPS)

GPS satellites circle the earth and transmit signal information to earth. GPS receivers take this information and use triangulation to calculate the user's exact location. Essentially, the GPS receiver compares the time a signal was transmitted by a satellite with the time it was received. The time difference tells the GPS receiver how far away the satellite is and the receiver can determine the user's position and display it on the unit's electronic map.

1.2.1.2 Geographic Information Systems (GIS)

Geographic Information Systems (GIS) provide the tools to provision and administer base map data such as man made structures (streets, buildings) and terrain (mountains, rivers). GIS is also used to manage point-of-interest data such as location of gas stations, restaurants, etc.

1.2.1.3 Location based information

As mention before this category provides highly personalized services to the user of a WLAN cable mobile phone like searching for the nearest ATM, hospital and etc.

1.2.1.4 Location based billing

Through location based billing, the user can establish personal zones such as a home zone or work zone. Through arrangements with the serving wireless carrier, the user could perhaps enjoy flat-rate calling while in the home area and special rates while in other defined zones.

1.2.1.5 Location Emergency services

All wireless carriers must provide a certain degree of accuracy in pinpointing the location of mobile users who dial an emergency number. Such a service would be extremely useful, especially to users who are far from home and don't know local landmarks.

1.2.1.6 Location Tracking

This is a large category that contains everything from the difficult fleet applications to enabling mobile commerce, asset and people tracking, driving safety and many others. Fleet applications typically entail tracking vehicles for purposes of the owning company. Tracking is also an enable of mobile commerce services. A mobile user could be tracking and provided information that he has predetermined he desires, such as notification of a sale a store close to the user's current proximity.

1.3 Major Positioning Systems

There are three broad categories of positioning systems: systems that use satellites and are mostly vehicle based positioning systems, the cellular network based positioning systems which are operated by cellular communication network operators and systems based on wireless network technology such as Wi-Fi and Bluetooth.

The vehicle based positioning systems acquire information's from at least three satellites in order to triangulate the location of a mobile device. Examples include systems like Global Positioning System and Galileo Satellite Systems. These positioning systems are highly precise and relatively low cost since GPS chips are increasingly embedded in devices as a feature. The drawbacks are that they require a high level of power consumption, and have a weak signal inside buildings.

Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) provide positioning methods in cellular network based positioning systems such as, cell tower calculations, Cell of Origin positioning (COO), time difference of arrival positioning (TDOA) and angle of arrival positioning (AOA). Cell tower calculations locate the mobile device based on which tower the mobile device is connected to. The COO method determines the location based on the base station which the mobile device is connected. When TDOA is in use three base stations measured the time difference that a signal requires to travel between the base station and the device and from that time the location and distance can be derived. AOA calculates the angle of the user's mobile device by looking at the direction of radio signals based on information received on and after some geometric calculations the position can be found.

Wi-Fi based positioning systems is an attractive positioning technology due to the widely deployed WiFi access points (APs) and the growing number of WiFi-enabled mobile devices on the market. Also Wi-Fi based positioning systems have become useful in areas where GPS signals can be weaker, or where the use of GPS consumes the device's battery quickly. For example a device can sent a query to a geological map database through a nearby Wi-Fi access point and the database replies with the location of the device based on the matching Wi-Fi access point. Bluetooth may also be tracked and positioned indoors, however limited range and density make this less practical, whereas Wi-Fi access points are more commonly present.

1.4 Problem Statement and Objectives

Perhaps the most typical scenario of an indoor wireless tracking system is as follow: a mobile user moves around in the dinosaur section wing of a large museum admiring the size and aggressiveness of those creatures while it's connected to the free Wi-Fi network provided from the museum. Then he touch a button on his smartphone and he receives a message on the museum application that he previously downloaded and installed to turn right in order to face the fossils of a huge T-Rex tyrannosaur and a hall other details. This Wi-Fi positioning system consist the following big players: a user with a Wi-Fi 8022.11x enable device, access points in the room (APs) and a database server. The user collects RSS signal strength from the nearby APs which transmit RSS broadcast beacons constantly in a specific channel and also it can extract information, such as MAC address, SSID and RSS db power from them. The database server stores the RSS fingerprints collected by the mobile device. The localization process takes place when the user clients sent a query to the database server and in turn the server compares the RSS signals of the client with the ones store in the dataset and extracts location estimation coordinates through some measurements techniques.

This thesis focuses on the creation of a WLAN positioning and tracking system that can locate and track accurate a mobile user that has a Wi-Fi enable device and can be implemented on existing wireless network infrastructures. RSS is the measurement metric. The innovation of this project relies on the fact that this system works completely different from the typical scenario mention earlier. This system is of course consisted from the same players as before but now the user is completely unaware that is been track down from the network administrator. This innovation raises many privacy issues but the main purpose of this system is to serve finally as a security positioning measurement in a network building infrastructure and not as a guideline or informative positioning system. The way it works is actually very simple. At first a database is built up consisted from RSS sample readings taken from reference points in the actual space and then broadcast beacons in all 802.11x channels are sent out from APs which in their turn receive back replies from wireless devices located in the predefine area. The APs produce an integer RSS db power indication with the use of a special tool call Wiviz. Then the server which has installed the application can transfer those readings locally using Netcat and manipulate them in such a way thus by comparing the live RSS from a mobile user against the database readings through a localization algorithm produces an estimation of the user position on map. Also another innovation is that the system is built up from free open source tools and applications and requires minimum cheap equipment. To summarize, contributions of this thesis are extensive to the security of network environments, technical problems of wireless environments and also to the accuracy and evaluation performance of the localization algorithm in use.

Chapter 2 Background and Theory

2.1 Localization

Localization is the process of determining the physical position of a mobile device either through a wireless medium like 802.11x or a physical medium like an eye recognition device on a safety door. This position can either be expressed descriptive as for example room 4, or locally in an area using the Cartesian coordinates such as (4, 8). A physical position can also be expressed in the global coordinate system in a form of latitude/longitude.

2.1.1 Indoor Localization Technology Systems

Indoor localization as increasingly gain worldwide interest due not only to the wide deployment of different wireless networks kinds but also to the emerge and discovery of new ideas develop into applications like helping a blind man navigate his self inside a hospital, track an important company asset and many others. A positioning system determines the location of an object in a particular space, such as an enterprise facility or warehouse. Indoor localization systems can be categorized according to the medium they use to the following categories.

2.1.1.1 Active Radio Frequency Identification systems (RFID)

Radio frequency identification (RFID) is a generic term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an object or person wirelessly, using radio waves. It's grouped under the broad category of automatic identification technologies. RFID scanners installed throughout a facility scans for signals from active or passive tags attached to objects. Active tags use batteries and allow up to a twenty foot range between the scanner and the tags. Passive tags don't use batteries, and they receive energy when being scanned and consequently they must be relatively close (within inches or a few feet) to the scanner. A centralized station stores the tag codes that the scanners collect. Because the scanners are placed in known positions throughout a facility, the centralized station is able to identify and display the location of each tag (and of course the client device that the tag corresponds with). Active RFID systems determine position based merely on the *presence* of the object in a particular area, within range of a RFID scanner. When a person wearing an Active RFID tag enters a room, for instance, the system indicates the existence of that person as soon as it detects the tag's signal. As a result, the accuracy of an Active RFID system is highly dependent on the positioning of the scanners. One scanner per room only provides location accuracy to the size of the room. This kind of systems can be very costly due to the large number of RFID scanners needed to be installed as per room and also in addition, some RFID systems operate in the same frequency band as wireless LANs, which poses RF interference issues in a wireless LAN network. RFID systems can be built up on Bluetooth protocol or the newer protocol called ZigBee.

2.1.1.1.1 Bluetooth systems

Bluetooth systems use of course the well known IEEE 802.15.1 standard which is located almost in every mobile phone and other appliances. Bluetooth is designed for very low power use, and the transmission range will only be 10m at best in an open space. In these systems user carry a Bluetooth enable device and when they enter into a specific cover radio range of a Bluetooth locator device they can exchange information and finally to estimate the target position. Main disadvantage is the limited range of the protocol IEEE 802.15.1.

2.1.1.1.2 ZigBee systems

ZigBee technology is a low data rate, low power consumption, low cost, wireless networking protocol targeted towards automation and remote control applications originally based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). ZigBee solutions are widely applied in many areas, such as home automation, healthcare, smart energy and other consumer and industrial equipment that require short-range wireless transfer of data at relatively low rates. The low cost allows the technology to be widely deployed in wireless control and monitoring applications. Low power-usage allows longer life with smaller batteries.

2.1.1.1.3 ZigBee vs. Bluetooth

ZigBee looks rather like Bluetooth but is simpler, faster, has a lower data rate and spends most of its time snoozing. This characteristic means that a node on a ZigBee network should be able to run for six months to two years on just two AA batteries. ZigBee can be implemented in mesh networks larger than is possible with Bluetooth. ZigBee compliant wireless devices can transmit up to 10-75 meters depending on the RF environment and the power output consumption required for a given while Bluetooth delivers only up to 10m. The data rate of ZigBee is 250kbps at 2.4GHz, 40kbps at 915MHz and 20kbps at 868MHz whereas that of Bluetooth is 1Mbps.

2.1.1.2 Infrared systems (IR)

An IR location system determines position of an object based on the presence of an object. Each object being tracked includes a proprietary emitter that periodically transmits an IR beacon invisible to human eye which contains a unique code. Specialized IR receivers placed throughout the facility detect the beacons and determine the approximate position of the object because of the known location of the

IR receiver. An IR system is practically immune to interference from wireless network because it operates on a lower frequency but many disadvantages exist such as because IR signals don't penetrate materials, such as walls or ceilings, an IR tracking system must often have several receivers in each room to avoid losing sight with the tag on the object. Also the IR tag must be place in such a way on the object or the person in order not blocking sight with the IR readers. These drawbacks add to the cost and complexity of the overall solutions and as with Active RFID systems, scaling these proprietary solutions can become very costly.

Figure 1: Helicomm ZigBee tags and readers

2.1.1.3 Ultra-Wideband (UWB)

Similar to most other positioning solutions, UWB positioning systems have proprietary scanners installed throughout the facility that continuously monitor UWB radio transceivers attached to clients. UWB tags generally transmit several beacons each second, which makes batteries last approximately one year. UWB systems, operate using radio signals having very wide bandwidth, and position calculations are made based on time-of-arrival techniques instead of signal strength. This leads to fairly good location accuracy. The use of UWB signaling considerably reduces signal impairments, such as RF interference and multipath propagation, which makes the coexistence with Wi-Fi networks acceptable. The downside of these systems is that UWB hardware is expensive to purchase and scale and battery replacement can be costly. Furthermore the public use of UWB is still under consideration with the FCC, which makes the future of this technology unclear.

2.1.1.4 Sensor Networks

In a sensor network solution, mobile nodes or objects bearing a battery powered radio module transmit an RF beacon containing a unique identification to a receiver. Other types of proprietary sensor networks include those that operate by measuring the time is takes for a signal to travel between the sensor and the tracked object, commonly referred to as Time Difference of Arrival (TDOA). These systems makes use of modified Wi-Fi access points or separate sensors installed throughout a facility that receive the beacons containing the identity of the client like timing information of the packets transmitted and then a centralized software interprets the position of a particular client using a triangulation method based on differences in signal strength measurements retrieved from three or more access points. TDOA systems also rely on having a relatively clear line of sight between the sensor and the tag. In complex environments such as factories and hospitals, TDOA systems would require an exceptionally high number of sensors to achieve decent positional accuracy which in turn may completely destroy the business case for a location tracking system. TDOA systems on the other hand perform better in outdoor spaces where there are fewer obstructions blocking the signal path between the sensors and the tags. In this type of environment combining GPS with WiFi may however be a more cost-effective alternative. Most of the sensor network tracking solutions allows the access points to carry typical data traffic associated with Wi-Fi users. This is a strong benefit over the other positioning systems, such as RFID and IR that make use of only proprietary equipment. Disadvantages include battery replacements, purchase of specialized software and tags are relatively large, with each measuring roughly two by four inches and weighing a couple ounces. The addition of this size of device for tracking purposes can be unacceptable in some cases. Also real time tracking is not optimal because the tags beacon transmission rate is very low and as a result a people moving pretty fast will not be able to track it.

2.1.1.5 WiFi-based Positioning

With the widespread adoption of wireless LANs, Wi-Fi is an ideal technology as the basis for positioning technologies. A standard WiFi-based positioning system, is completely software-based and utilizes existing Wi-Fi access points installed in a facility and radio cards already present in user devices. The critical issues of the positioning technologies discussed so far include the proprietary nature of the scanners and tags, needs for an infrastructure that is completely separate from a company's data network, and limited real-time operation. These common attributes make the systems costly to deploy, scale, and support. Without the need for additional hardware, a company can install the system much faster and significantly reduce initial and long-term support costs. The positioning system works wherever there is Wi-Fi coverage. In addition to cost savings in hardware, a standards WiFi-based positioning system significantly reduces the potential for RF interference. The total Wi-Fi positioning system shares the same network along with other network clients, so there is no additional installation of a separate wireless network (as RFID requires) that may cause RF interference with the existing wireless network. These systems use the received signal strength indicator (RSSI) as the basis for positioning and target estimation is done by signal propagation models, proximity or fingerprint techniques. A downside is that the signal strength values change analogue to the location of a device and so accuracy may vary depending on the environment type, access point density, antenna types and site calibration density. On the other hand some advantages are: they can work both in indoor and outdoor areas, quick installation, cost effective scalability and no disruption to existing operations and infrastructures.

2.1.2 Outdoor Localization Technology Systems

Outdoor localization is not a new technology trend, rather is an old one which keeps getting better in matters of quality of service and worldwide deployment by everyday users and industry services.

2.1.2.1 GPS (Global Positioning System)

GPS is commonly deployed in a variety of devices, such as handheld GPS receivers that provide latitude and longitude as well as moving maps for navigating airplanes and automobiles. The GPS consists of satellites in located geostationary orbit around the Earth. These satellites remain in a fixed position relative to the ground and continuously transmit coded beacon signals. A GPS receiver located on a client receives simultaneous signals from multiple GPS satellites and uses a time-based approach for calculating position. The successful reception of at least three satellite signals is enough to calculate x-y coordinates. With a greater number of satellite signals, however, accuracy is better, and it’s even possible to determine elevation. An issue is that GPS signals are relatively weak, making it only usable in areas with an unobstructed path between the GPS receiver and the sky. In fact, GPS is not usable at all inside buildings. Tree foliage also significantly limits GPS signals. As with the positioning technologies discussed so far, GPS requires a dedicated chipset in the client device. This entails the installation of GPS circuitry, which adds to the expense and complexity of the user device.

2.1.2.2 Cell of Origin (COO) /Cell ID (CID)

The most basic and simple way to locate a mobile device might be to find its cell area.

The location of the base station or antenna in this cell area is the estimated location of the mobile device. Although simple, fast and low cost, the locating accuracy of this method is quite rough.

2.1.2.3 Cell tower calculations

Cell tower calculations locate the mobile device based on which tower the mobile device is connected to. Cell towers are divided into cells which can be meters or kilometers large. The accuracy of this technique is quite low because it depends on the density of cell towers which is sporadic.

2.2 Location Sensing Methods and Measurements

There are several fundamentally different techniques that may be used to estimate the location of a person or an object. In general they can be classified in the following classes: time of arrival (TOA) and time difference of arrival (TDOA), angle of arrival (AOA) and Signal Strength (RSS Location Methods). Frequently location aware systems combine these approaches to achieve higher accuracy or precision.

2.2.1 Time of arrival (TOA) and Time difference of arrival (TDOA)

TOA and TDOA methods use geometric principles and calculations to calculate the distance between a wireless node and a number more than three AP’s in order to determine the coordinates of the mobile target. The TOA method is based on the time of arrival of a known signal sent from the mobile device and received by three or more base stations, where the TDOA method values are calculated by pair wise subtracting the differences of the arrival times between the target and the base stations. This approach opens up a number of timing and clock synchronization questions that each system that employs this approach has to address it.

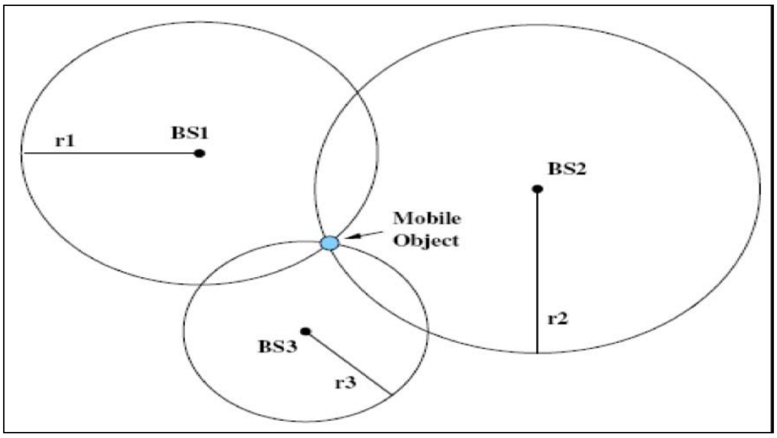

Figure 2: Location-sensing based on Time of Arrival (TOA)

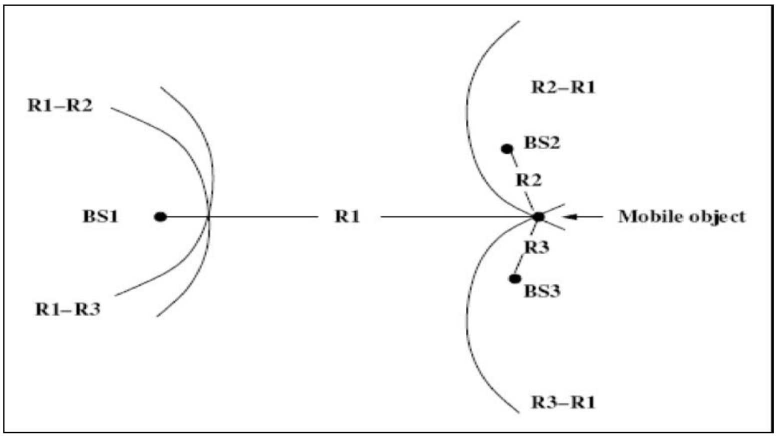

Figure 3: Location-sensing based on Time Difference of Arrival (TDOA)

2.2.2 Angle of arrival (AOA)

Angle of arrival (AOA) is probably the oldest method because it doesn’t need any special hardware except a directional antenna. Angle of arrival (AOA) is a network-based method of determining position that does not require a mobile device to operate. In AOA, a mobile device's signal is received by multiple base stations. The base stations have additional equipment that determines the compass direction from which the user's signal is arriving. The information from each base station is sent to the mobile switch, where it is analyzed and used to generate an approximate latitude and longitude for the mobile device. An advantage of AOA is that it supports legacy handsets. Disadvantages include the fact that every base station needs to have an equipment upgrade. Users might also be concerned about privacy issues because they are not able to disable positioning from the handset. AOA systems are able to find the location and distance by a using a technique called triangulation.

2.2.2.1 Triangulation & Lateration Techniques

Triangulation is the process of determining the location of a point by measuring angles to it from known points at either end of a fixed baseline. Lateration is the same process as triangulation but instead angles distance measurements to the target are used.

2.2.2.1.1 Angulation

Angulation as explain before at 1.3.2 angles are used for determining the position of an object and it is used in the triangulation technique. In general, two dimensional angulations require two angle measurements and one length measurement such as the distance between the reference points.

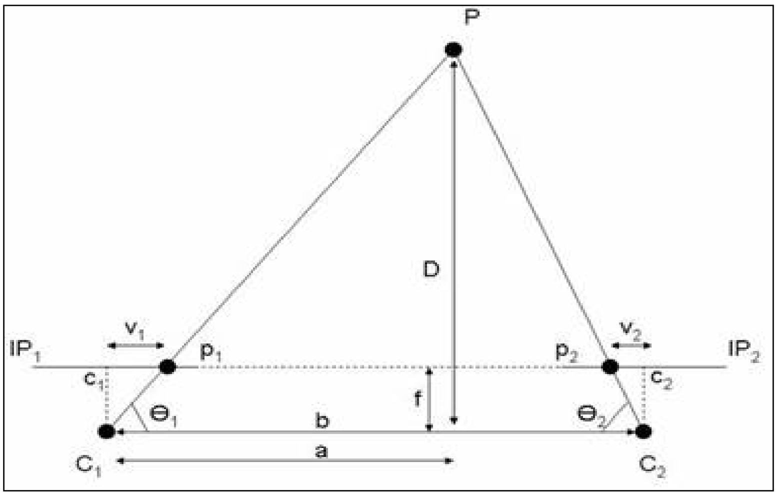

Figure 4: Angulation example in two dimensions

2.2.2.1.2 Lateration

Lateration computes the position of an object by measuring s distance from multiple reference positions by using the RSS signals from AP'S which are converted to distance according to the signal propagation model. Calculating an object's position in two dimensions requires distance measurements from minimum 3 points. In 3 dimensions, distance measurements from 4 points are required. There are three general approaches to measuring the distances required by the lateration technique. The direct approach where the measurement of distance is a physical action or movement. For example a tape measure. The Time-of-Flight method which the distance is estimated from an object to some point P using time-of-fight means measuring the time it takes to travel between the object and point P at a known velocity. And finally by measuring the distance through signal attenuation. The intensity of an emitted signal decreases as the distance from the emission source increases. The decrease relative to the original intensity is the attenuation. Given a function correlating attenuation and distance for a type of emission and the original strength of the emission, it is possible to estimate the distance from an object to some point P by measuring the strength of the emission when it reaches P.

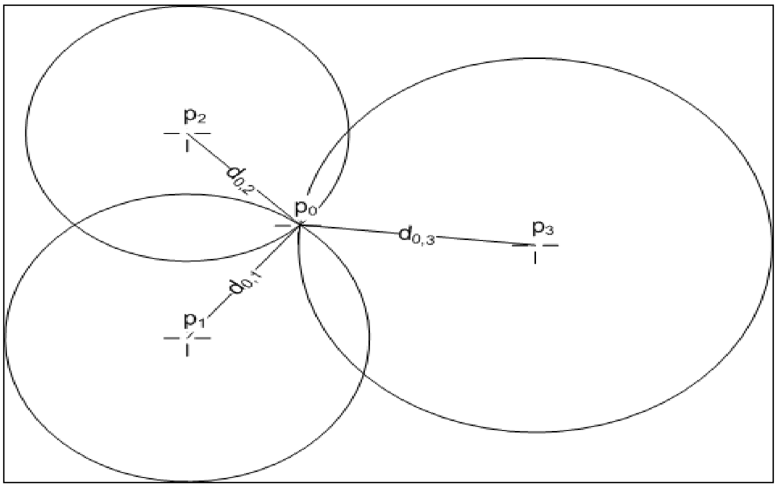

Figure 5: Trilateration example

2.2.2.1.2.1 Multilateral Systems

In a multilateral system the mobile target transmits beacons in a predefined area towards some fixed known coordinates AP's. The location is calculated from measurements taken by those receivers whose positions are known. An advantage is that these systems can run on servers with great storage and computational power. On the others hand a network administrator can track a target without the targets permission which it may consider a violation of privacy.

2.2.2.1.2.2 Unilateral Systems

In a unilateral the system the mobile target computes its own location from received signals strengths from multiple terminals whose positions are known. In these systems no privacy rights are violated because all the computations are taking place on the mobile target by its self. Also another advantage of this method is that many mobile nodes can find their location simultaneously since computations are distributed among them. On the other hand these systems cannot be used as a security wireless positioning system because it will serve no purpose.

2.2.3 Signal Strength RSS

Positioning systems that make use of signal strength (RSS) actually they mainly have as a base the WLAN IEEE 802.11b/g/n standard used for providing wireless internet access for indoor areas. That doesn't mean that are restricted not to use other wireless protocols like Bluetooth or infrared or RF or ultrasound. These systems are further divisible into two categories: the ones that use proximity and the ones that use fingerprint to locate a mobile target. The advantage of scene analysis is that the location of objects can be inferred using passive observation and features that do not correspond to geometric angles or distances.

2.2.3.1 What is RSSI

RSSI stands for "Receive Signal Strength Indicator", which is a circuit to measure the strength of an incoming signal. The basic circuit is designed to pick RF signals and generate an output equivalent to the signal strength measured in db (decibel). The ability of the receiver to pick the weakest of signals is referred to as receiver sensitivity. Common devices with inbuilt RSSI are cell phones, wireless network adapters and even remote control. In an IEEE 802.11 system RSSI is the relative received signal strength in a wireless environment. RSSI is an indication of the power level being received by the antenna.

2.2.3.2 Proximity

A proximity location sensing technique entails determining when an object is near a known location. The object's presence is sensed using a physical phenomenon with limited range. This means that the detection of a mobile terminal takes place in specific signal radio area of a fixed predefine location which the target lies in that specific range. Monitoring a mobile device in a range of one or more access points in a wireless cellular network is an implementation of a proximity location technique. This method it's easy to implement but does not provide high accurate results.

2.2.3.3 Fingerprint

Wi-Fi Fingerprinting creates a radio map of a given location based on the RSSI data from several access points (more than tree) and generates a probability distribution of RSSI values for a given (x, y) coordinate location. In the given location RSSI samples readings are taken usually like a grid known points and store in a database. These samples are called fingerprints. Afterwards live RSSI taken from mobile terminal located inside the specific area are compared to the fingerprints to find the closest match and generate a predicted (x, y) location.

2.3 RSSI Location Methods

2.3.1.1.1 RSSI Location Method based on Range Estimators

The location coordinates in this method can be calculated based on mathematical propagation models of free space like Friis equation figure 3 or from methods based on geometry like the intersection of circles in 2D dimension or intersection of spheres in 3D dimensions like the ones used in TOF systems. The error rate in RSS systems is greater than the TOF systems due to the different environment conditions that have a positive or negative effect on signal strength power value. An example of these method are smart sensor networks which they only have distance knowledge for neighbor sensors. To find the location of a target tree sensors constitute the tree side lengths of a triangle and then the angles and sides are calculated and so the coordinates of a mobile target

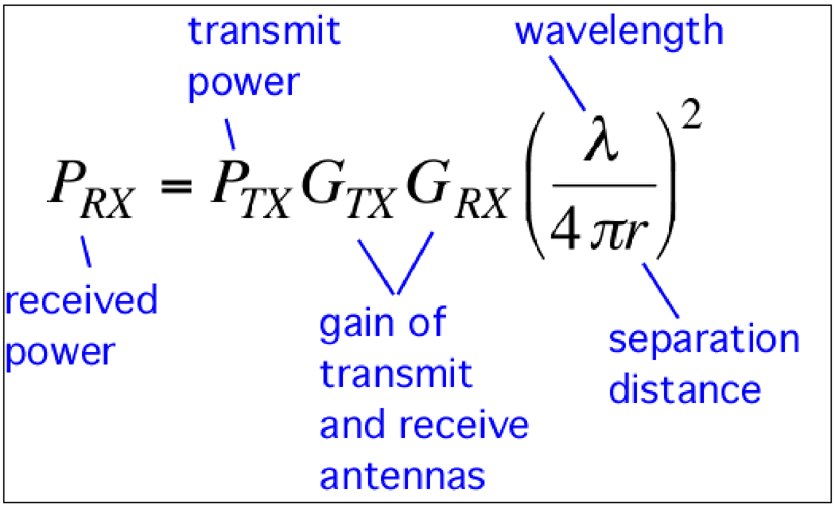

Figure 6: Friis equation

2.3.1.1.2 RSSI Location Method based on Database Comparison

This method works by comparing a set of live RSSI signals of a mobile target which is located in a known area with signals measurements in a fingerprint database. The fingerprints signals were measure and sample in an offline phase usually called fingerprint phase and store in a database according to each access point. These techniques are called fingerprinting or pattern recognition [1]. This technique can be used for both indoor and outdoor areas.

The location estimation method has two phases. The first phase, as said called fingerprint or offline or survey phase is the creation of the fingerprint database. In a predefine space reference points are decided in a grid manner having a good distance apart. Then sample RSSI readings area collected from those reference points for each access point that exist in the area and thus creating a radio map. The accuracy of the estimated position of the user depends highly on the number of reference points collected in the fingerprint database. At each reference point a mobile terminal is placed which transits beacons to the access points while it is oriented in the four directions: North, East, West and South in order to build a more comprehensive fingerprint database. The reason why the mobile terminal must transit a beacon in all directions is that because its antenna is not omnidirectional, meaning an antenna which is capable of transmitting and receiving radio signals equally in any direction in the horizontal plane, and thus the transmitted signal strength reading is dependent on the location of the antenna on the device. Also the signal also depends on the location of the operator body if it is blocking the line of sight between the mobile terminal and the access point. Furthermore other factors that may affect an RSSI signal is different objects in the area, other people, other signals, shadows, walls, movement of device and many others. That's why the need for the different orientations and also the need to take many samples for each orientation. Then the readings are imported into a database in order to create the fingerprint database categorized from each AP. Next in the second phase, the location real time phase when a mobile user whether holds a laptop or a smartphone or any device able to emit an RSSI signal can calculate its position in that area if it is a unilateral system or to be tracked down if it is in a multilateral system. Online signals recorded on all access points are compared with the ones in the fingerprint database against all reference points and the result is calculated from the closest match reference points. The advantage of the fingerprint database is that because it is built on actual real signals measurements the different environment effects like multipathing, path loss, obstacles and etc minimally affects the final estimated location result. Although the other effects caused from hardware like antenna transit power or antenna orientation still contribute negative the results are quiet accurate. Also perhaps the biggest disadvantage of this method is the fingerprints database itself and its maintenance. Because the database is built only for a specific area it applies only to that particular and nowhere else. Also over time the current RSS readings slowly deviate from the readings in the database due to the environment with danger for the database to turn out useless, if it is not updated periodically. Furthermore the offline fingerprint phase is very time consuming and expensive to create but much cheaper from many other methods because it doesn't need any special equipment or software that is not already available in a company wireless environment. Because the RSS readings collected by different network cards may be different is suggested to use two different mobile devices and even more for the collection of RSS readings from each reference point. When for comparing the live online RSSI signals against the fingerprint database many ways have been developed which are not in the scope of this thesis except two which will be briefly explain. The one uses the Euclidean distance as a distance measurement and it is called Search Nearest Neighbor and also is the one chosen to be used in thesis because it is a simple and effective method for indoor positioning systems, and the other one is a statistical way that uses and called the Bayesian Inference location method.

2.3.1.1.2.1 Database Comparison by Search Nearest Neighbor Algorithm

Also called similarity search or closest point is an optimization problem for finding closest points in metric spaces. In the traditional Nearest Neighbor the goal is to preprocess a set of objects, so that later, given a query object, one can find efficiently the data object most similar to the query. The problem is how quickly this preprocess is done and in what way it's better to be cluster in order to minimize the response time in a query. This algorithm is widely used for classification, clustering and texture mapping. The search for nearest neighbours in a high-dimensional database is complicated by the size of the database and the dimensionality of the space. In the wireless system developed for this thesis this algorithm is been adopted because it's relative easy to be implemented, quick for the data that has to handle, it doesn't need any special equipment to work and it produces good accurate results.

In NN RSS location method the first step is to create the fingerprint database. So in each reference point RSSI sample readings are gather from each AP and form a vector $(S_1.......S_K)^T$ whose values are the average normalized RRS db value at each AP *K*. Then these vectors are store in the fingerprint database. Afterwards when an online RSS measurement vector is obtained the algorithm uses the Euclidean distance to calculate a distance D for each vector store in the database as follow:

$$Dn = \sqrt{\sum_{i=1}^{K} \left(S_{T_i} - S_{i,n}\right)^2}$$

D represents the distance of the target from a particular sample vector, S_T is the user online signal strength vector, *S* is the database vector collected earlier, *i* is the index number of the AP and *n* is the index number of the reference point. When the Euclidean distance part finishes the results are store in a ascending order and the first *K* reference points coordinates are chosen. Basically the minimum *K* results are chosen. Then in order to obtain the Cartesian coordinates of target the algorithm sum up the coordinates of the reference points chosen and average them as follow:

$$x = \frac{1}{L}\sum_{l=1}^{L} x_l \quad , \quad y = \frac{1}{L}\sum_{l=1}^{L} y_l$$

where L is the number of minimum reference points and x , y are their integer know coordinates.

Because by moving from one point to another to collect signal strength readings can be very time consuming other techniques to collect them exist such as the following propagation formula:

$$PG_{db=}\ 20\log\left(\frac{\lambda}{4\pi d_0}\right) +\ 10 \bullet n \bullet log\left(\frac{d_0}{d}\right) +\ X_\sigma$$

PG_{db} stands for Path Gain which is the ratio of the received power to the transmitter radiated power [1]. λ is the wavelength at distance d and πd_0 is the separation distance. X_σ and n are random variables which their values can be found from table 1 [1].

The accuracy of this technique depends heavily on the environment because indoor radio propagation channel is highly unpredictable and time-varying, due to severe multipath in indoor environment, shadowing effect arising from reflection and refraction caused by obstacles and walls.

Environment	Frequency (MHz)	Exponent n	Variance σ (dB)
Retail store	914	2.2	8.7
Office, hard partition	1500	3.0	7.0
Office, soft partition	900	2.4	9.6
Factory, line of sight	1900	2.6	14.1

Table 1: Variation of Propagation Parameters

2.3.1.1.2.2 Bayesian Inference RSS Location Method

This is a statistical method which uses probabilities in order to determine the target's location. During the offline phase at the reference points signal strength are gathered for each AP in the area and they are transformed into statistics and vectors group into states *S*. The vector collected is:

$$S_k = (x_k \; y_k \; p_k)^T$$

where *(x_k, y_k)* are the Cartesian coordinates of the location and p_k is the mobile target orientation. The set of all states is:

$$S = \{s_1 \;\; s_2 \;\dots\; s_k \;\dots s_K\}$$

where *K* is the total number of states which is equal to the number of reference points multiply the number of orientations in point.

These vectors are store in groups called sets in a database in a form called *observations o*, which consists the received signal strength and usually the MAC address of the base station associate with the signal thus creating again the fingerprint database. The idea is to find the posterior distribution of the location, which is the conditional probability estimated from Bayes rule written as:

$$P(s_k|o') = \frac{(o'|s_k)\;(s_k)}{\sum_{k=1}^{k} P(o'|s_k)\;P(s_k)}$$

where *o'* is the real time observation of the mobile target. The expression is calculated for all states s_k and the maximum $P(s_k|o')$ is probably the location of the target.

Furthermore the previous expression cannot derive a numeric value for $P(s_k|o')$ from the statistics derived from the observations and so two probabilities relationships called histogram are used. Basically they are two statistical graphs showing the relation of the signal strength (db) and the probability frequency of a signal against the probabilities they occur in the offline phase. The fist probability is the relative frequency which equals the number of signal strength measurements in the observation that are associated with an access point address divided by the total number of signal strength measurements as *P*(*fi* | *sk*), *M*, in that observation [1]. The second probability relationship describes the distribution of signal strengths between a target and each access point given *sk*, expressed as *P* (σj | *b*, *sk*) [1]. The statistics from those relations form the histograms, two for each AP. Then, the likelihood probability for a particular RSS value can be obtained from the histograms. In order to have a good reliable histogram a large amount of RSS must be collected and thus this is a major drawback of this method.

2.3.1.1.2.1 Comparison between Nearest Neighbor and Bayesian Inference RSS Location Method

First of all the Bayesian method uses more information for each signal strength reading and thus applies that it has a much larger database than Nearest Neighbor. The Nearest Neighbor is just doing simple math calculations instead of complex probabilities and tends to give less accurate results from the Bayesian one, especially when the samples taken are not many. Finally in both methods the offline phase is taking place first and the sample signal readings are affected by environmental and hardware factors.

2.4 WLAN Standards

WLAN stands for Wireless Local Area Network. A wireless LAN (WLAN) is a flexible data communication system implemented as an extension to or as an alternative for, a wired LAN within a building or campus. Using electromagnetic waves, WLAN transmit and receive data over the air, minimizing the need for wired connections. Thus, WLAN combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs.

2.4.1 IEEE 802.11

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) created the first WLAN standard. They called it 802.11 after the name of the group formed to oversee its development. Unfortunately, 802.11 only supported a maximum network bandwidth of 2 Mbps - too slow for most applications. For this reason, ordinary 802.11 wireless products are no longer manufactured.

2.4.2 IEEE 802.11a

802.11a supports bandwidth up to 54 Mbps and signals in an unregulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions. Its modulation scheme is OFDM, and uses WEP and WPA to implement security.It has 12 non-overlapping channels and it's less potential for radio frequency interference than 802.11b and 802.11g

2.4.3 IEEE 802.11b

IEEE 802.11b is the most widely used WLAN standard. 802.11b uses the same unregulated radio signalling frequency (2.4 GHz) as the original 802.11 standard. Vendors often prefer using these frequencies to lower their production costs. The data rate of IEEE 802.11b is up to 11Mbps in the 2.4GHz band. Its modulation scheme is DSSS with CCK, and uses WEP and WPA to implement security. It offers high-speed access to data at up to 100 meters from the base station and it has 14 overlapping channels but it's prone to interference from microwave ovens, cordless phones, and other appliances using the same 2.4GHz band.

2.4.4 IEEE 802.11g

802.11g attempts to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa. The data rate of 802.11g is up to 54Mbps in the 2.4GHz band. Its modulation scheme is OFDM and DSSS, and uses WEP and WPA to implement security. It has 14 overlapping channels and it has the same interference problems as 802.11b.

2.4.5 IEEE 802.11n

802.11n is a new wireless standard that improves network throughput over the previous standards by adding a new technology called multiple-input multiple-output (MIMO). MIMO uses several antennas to move multiple data streams from one place to another. Instead of sending and receiving a single stream of data, MIMO can simultaneously transmit three streams of data and receive two. This allows more data to be transmitted in the same period of time. This technique can also increase range, or the distance over which data can be transmitted. Another technology being incorporated into 802.11n is channel bonding, which can use two separate non-overlapping channels at the same time to transmit data. This technique also increases the amount of data that can be transmitted. 802.11n connections support maximum theoretical network bandwidth up to 300 Mbps depending primarily on the number of wireless radios incorporated into devices and also offers a better operating distance than current networks.

2.5 Indoor Wireless Channel Effects

In a WLAN deployment, performance and capacity are impacted by several factors that must all be considered to meet the requirements of a high availability and high performance network environment. The wireless medium is a very dynamic shared environment affected by several factors. The indoor environment has unique properties that influence the radio frequency signals used by the sensors of positioning systems. Some of these factors can be controlled while others are fundamental limitations of the wireless medium that must be recognized and taken into account when planning a WLAN. The following factors should be taken into account when deploying a wireless RSSI positioning system because they can play a critical role in the accuracy of the system. Ways of dealing them should be develop and face through the location methods and techniques as to change a building environment it's rather hard.

2.5.1 Indoor Wavelength Propagation

2.5.1.1 Reflection

When a signal is reflected there is normally some loss of the signal, either through absorption, or as a result of some of the signal passing into the medium. A variety of surfaces can reflect radio signals. A variety of surfaces can reflect radio signals differently depending on the physical properties such as the surfaces' geometry, texture and material composition. For relatively short range communications, many buildings, especially those with metallic surfaces provide excellent reflectors of radio energy. As a result of this signals travel via a variety of paths to and from in a Wi-Fi and other short range wireless communications. An office environment contains many surfaces that reflect radio signals very effectively.

2.5.1.2 Refraction

When radio waves travel through substances of different densities, the wave will bend (refract). This is due to the fact that radio signals move slower through substances of greater density. Typically, refraction will be most noticeable at night and in the early morning hours, when moisture in the air is highest.

2.5.1.3 Diffraction

Diffraction occurs when a travelling signal encounter an obstacle it tend to travel around it. This can mean that a signal may be received from a transmitter even though it may be blocked by a large object between them and there is no line of site. The result of diffraction of a wave at an obstacle edge is that the wave bends around and behind the obstacle edge and as a result the signal power decreases. Diffraction is best demonstrated by the radio signal being detected close to the inside walls around corners and hallways.

2.5.1.4 Scattering

If there are many objects in the signal path, and the objects are small relative to the signal wavelength, then the propagated signal will break apart into many directions.

The resultant signal will scatter in all directions adding to the constructive and destructive interference of the signal. Most modern buildings contain steel throughout the wall supports that support scattering. Furthermore, construction materials such as conduit for electrical and plumbing service can add to the scattering effect.

2.5.1.5 Doppler Effect

When radio wave travels between two objects, the wavelength changes if one or both of them are moving. The Doppler Effect is observed whenever the source of waves is moving with respect to an observer.

All these propagation effects have as a result the following signal transformations and paths categories.

2.5.2 Signal Transformations and Paths Corruption

The main problem that exists for indoor environments is that the signal propagated from the transmitter antenna will experience many different signal transformations and paths corruption with a small portion reaching the receiver antenna. Awareness of this process will assist the user to better understand radio performance limitations.

2.5.2.1 Path Loss

In free space, the radio waves travel outward from the transmitter in an expanding sphere and as a result the strength of radio wave decreases as the distance between the transmitter and receiver increases. Path loss is difficult to calculate for an indoor environment because of the variety of physical barriers and materials within the indoor structure which attenuate and corrupt a signal. Free space loss can be calculated as $FSPL = \left(\frac{4\pi d}{\lambda}\right)^2$ where d is distance in meters between the transmitter and receiver, and λ is the wavelength in meters. This equation also implies that as the frequency increases the loss will be proportionally higher.

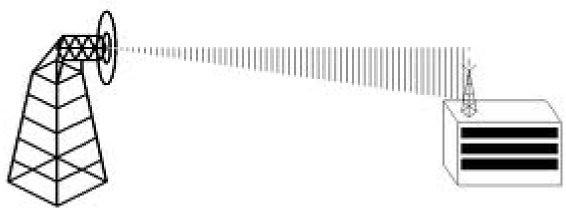

Figure 7: How much the signal has weakened over a distance d (FSPL)

2.5.2.2 Multipath Fading

When a radio frequency signal is transmitted towards the receiver, the general behaviour of the signal is to grow wider as it is transmitted further. On its way, the signal encounters objects that reflect, refract, diffract or interfere with the signal. When a signal is reflected off an object, multiple wave fronts are created. As a result of these new duplicate wave fronts, there are multiple wave fronts that reach the receiver. Multipath propagation occurs when signals take different paths from a source to a destination. A part of the signal goes to the destination while another part bounces off an obstruction, then goes on to the destination. As a result, part of the signal encounters delay and travels a longer path to the destination. Multipath fading can be caused from refraction, reflection and diffraction propagation signalling. Effects of multipath distortion include: data corruption, signal cancelling and increased or decreased signal amplitude.

2.5.2.3 Shadowing Fading

Shadow fading occurs when an obstacle gets positioned between the wireless device and the signal transmitter. This interference causes significant reduction in signal strength because the wave is shadowed or blocked by the obstacle. Shadowing is the effect that the received signal power fluctuates due to diffraction. Fast fading shadow is also referred to as small-scale fading, which accounts for the rapid variation of signal levels, when the user terminal moves within a small or local area. There are many physical factors in the radio propagation channel, which result in fast fading, which typically include: Doppler Effect, diffraction, reflection, radio frequency, bandwidth and etc.

2.5.2.4 Wireless Interference

Wireless interference is when wireless devices that use the same radio band clash with each other in the airwaves resulting to data corruption and loss. In mobile receivers, interference is from other base stations that transmit the same frequencies as the serving base station. In wireless LANs in the 2.4 GHz unlicensed band, interference can come from other LANs, cordless phones, Bluetooth devices, wireless video cameras, outdoor microwave links, wireless game controllers, ZigBee devices, fluorescent lights, WiMAX, and so on. The problem with wireless interference is that it will likely change over time. For example, a neighbour may purchase a cordless phone and start using it frequently, or the use of wireless LANs in an area may increase. This means that the resulting impacts of wireless interference may grow over time, or they may come and go. As a result, in addition to data corruption and loss another problem caused by wireless inference is the poor performance of the wireless network.

2.6 Laptop opening antenna angle effects

The majority of laptops today have a built in wireless antenna position on the top horizontal plastic shield of the screen. The user rarely notices its position. The size of the antenna depends greatly on the thickness of the laptop case. The antenna performance strongly depends upon its location on the laptop, because an antenna positioned in a specific location most probably will not suffer from the same effects in another position but also the RSS signal power while receiving and transmitting will be differ. Another factor except from the location of the antenna inside the mobile node is the height of its position (angle). By changing the angle of the screen unwilling the height of the antenna changes and so combine the new position with the previous signal and path corruption events describe in 2.5.2 the hall RSS signals spectrum changes resulting in different power values. So the height of the antenna can result to a false coordinate result from a wireless positioning system but also other factors generated from the mobile node equipment can play a significant role. Metal laptop components nearby the antenna and the size limitation due to the plastic can reduce bandwidth, add noise corruption and degrade the radiation efficiency. Also other sources of interference on the system platform, such as EMI spectrum from CPU, LCD, and memory, which may be in the form of radiation or conduction emission, but also the human body interaction electromagnetic inference which absolves the RSS signals, have a negative impact on the quality of signal perceived at the transceiver.

Chapter 3 Wireless Positioning System Overview and Development

As mention in the previous chapters RSS signals vary according to the environment located and also are affected from numerous factors. Due to this unstable nature of RSS most wireless positioning vendors use the RSS Fingerprint method to their systems. So by considering that an RSS signal basically adopts environment characteristics and reflects those environmental negative factors to its power value wireless positioning RSS systems can achieve good accuracy results and be implemented relative easily compared to other systems. In this thesis such a system has been developed and the core localization algorithm is Search by Nearest Neighbour.

3.1 System Overview and Development

The Wireless Positioning System is a software tool which works completely as a stand alone application installed preferably on a network environment server which its unique purpose is to estimate the location of a mobile target in an area map. The system consists of two phases: the offline and online phase. In the offline phase the fingerprint database is generated and in the online phase the localization process is taking place. Also along with the development of the system the antenna angle effects mention in chapter 2.6 will be under investigation because the fingerprint database will be develop three times for three angles measurements. The system will calculate the position of a mobile target independently for each angle fingerprint database in order to get a better understanding on how the laptop angle affects the RSS signal indicator.

3.2 System Architecture

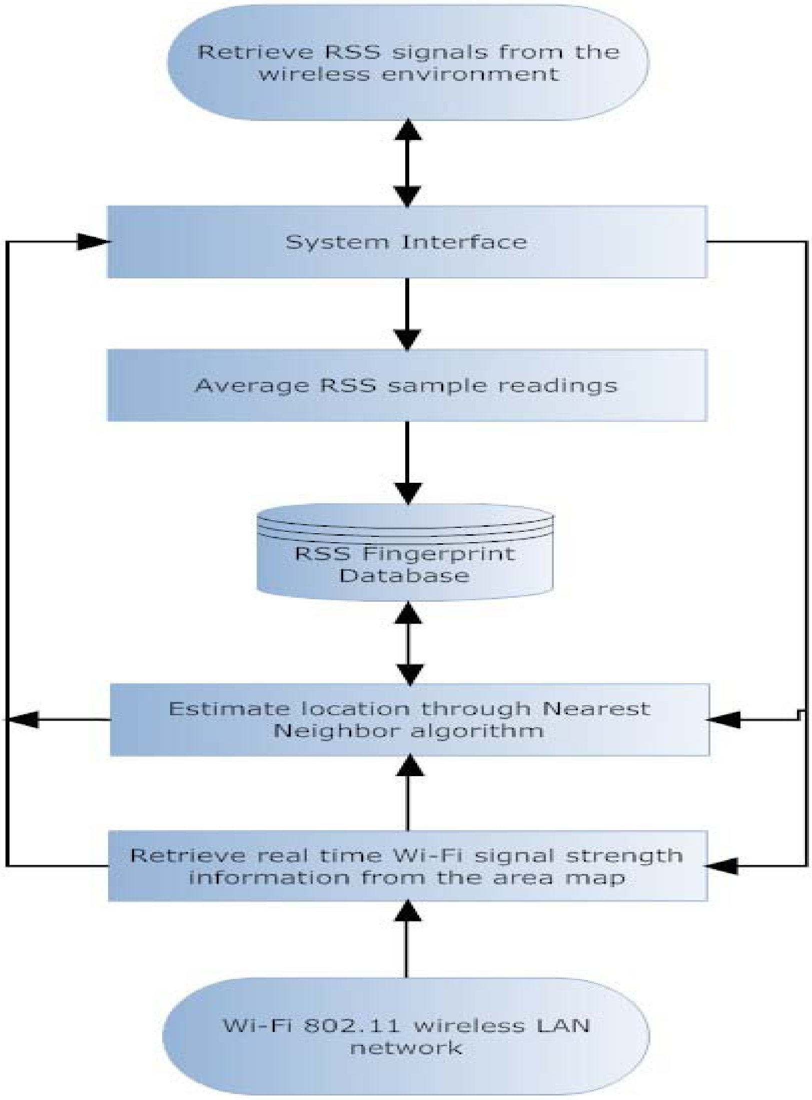

Figure 8: System Architecture

The figure in this page briefly describes the operation of the positioning system. From top to bottom at the beginning of the project the fingerprint database (offline phase) development is taking place (data collection) in order to build an RSS sample indicator area in which the algorithm will find the nearest neighbour of a mobile target. After building the fingerprint database the positioning can take place in the predefined space after the input of the necessary information's into the system like the access points credentials and IP’s and other which are guided by the application. Through the system interface a network administrator can initiate a graphical representation with all the mobile users located in the area and then decide to track one or to just position them on the map: online phase where RSS readings are obtained for the actual localization to take place.

System interfaces helps the user to build signal strength databases, to locate mobile devices, and to configure how to use the software. Data collection has two functions. One is collecting signal strength information and storing them in signal strength database. The other is collecting real-time signal strength information for positioning. In signal strength databases, the signal strength information collected is stored. It is the most important and expensively time consuming part of the software especially in this system which it makes use of three different fingerprint databases base on the angle on the laptop angle. It is the basis of wireless positioning.

3.3 System Requirements

In this section the software and hardware requirements to set up a low cost working positioning system of this thesis are briefly mention.

3.3.1 Software Requirements

First of all the system is designed to work only in pc’s running Windows operating systems from Windows Xp to WIN 7 and in Administrate mode. It is better to be installed on a machine with great computational power available (preferably newer quad or I series processors) and of course the amount of available RAM to be more than 4 GB. As mention before due to the crucial consideration before developing this system was to be as low cost as possible only free software are implemented. This consideration applies that with the deployment of the following free software’s not only their advantages are inherited into the project but also their disadvantages such as unexpected shut down failures and etc. The free software's with their purpose serving are:

1) Netcat: is a simple command line network utility which reads and writes data across network connections, using TCP or UDP protocol. It was first implemented in UNIX and afterwards to other operating systems. It is a reliable back-end tool that can be used directly or easily driven by other programs and scripts. It's a wonderful tool for debugging all kinds of network problems. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of TCP/UDP connection. In the simplest usage, the command *nc host port* creates a TCP connection to the given port on the given target host. Then any input like for example a command from the keyboard is sent to the host and anything that comes back across the connection is sent back as an output. This continues indefinitely, until the network connection is terminated or lost. Netcat can also function as a server, by listening for inbound connections on arbitrary ports and then doing the same reading and writing. It has many possibilities and capabilities which are out of this thesis scope but some features are the following: it can be used as port scanner, a backdoor, a port redirector, a port listener, transfer files between clients and lots of other. In this project Netcat is embedded into the installation file and thus the user doesn't need to download the Windows version. The role of Netcat in this project is to transfer the results of the active wireless targets that the access point detect and save then locally to a text file which in turn the platform parses and presents the clients into the

application interface. So Netcat provides a reliable free transfer pipe between the access points and the local terminal.

2) Wiviz version 1 & 2: is an open source project created by Nate True which can be installed on routers or access points running Linux based firmware systems. It stands for wireless network environment visualization and it's a visualization tool which creates and projects a radio signal map around an AP. It scans the frequencies belonging to the wireless spectrum and then it examines all the wireless packets replies from mobile nodes or even from other access points coming into the interface and extracts valuable information about the surrounding wireless infrastructure such MAC addresses, channel settings like encryption and channel number, SSID's, RSSI signal strengths values and others. Then it uses that information's to build a java based web interface map of the surrounding network which is updated in real time. In this thesis the project makes use this excellent software in order to force the access points to scan their surrounding in all wireless channels and thus acting as an expensive radar system. When the scanning is completed or terminated by the user the results including all the information's about the packets are locally situated into the temporary folder of the access point and then Netcat is called to transfer them locally. When running Wiviz in the web interface because its dynamic nature and graphics-effects it consumes many recourses from the pc, especially RAM and thus it creates local overhead and slows down the application. A solution to this is to run the tool from the telnet command window, this option is included in the system. So Wiviz provides the significant advantage of instead to have an expensive radar software or specialized equipment such as RF tags, adds the

wireless radar scanning functionality to the system for free. But along with the main advantage from this tool some disadvantages came along such as the recourses overhead and also the scenario of failing to scan a particular client when scanning is performed more than one time repeatedly. This can happen when the target wireless card doesn’t transmit anything and is in idle mode because Wiviz doesn’t force the card to transit a beacon or a reply. On the other hand the innovation advantage that Wiviz adds to the system which supports the hall idea to act as a security positioning system is that it scan and examines all the packets coming in an access point from all wireless channels without the permission of the client mobile user and without the need to have a wireless machine to be connected to a local network access points or any other. So a mobile user that has enable the wireless card and not connected when entering in a specific area, the system can give an estimated coordinate location and a representation on the area map without the user be aware of it.

3) DD-WRT v.24 & OpenWrt v.8.09: are a free third party developed firmwares for many ieee802.11a/b/g/h/n wireless routers based on a Broadcom or Atheros chip reference design. They are an open-source Linux-based alternative firmware for routers. They contain special features and optimizations designed to improve on the standard firmware that router manufacturers provide with their products. For example, DD-WRT provides functionality that other types of firmware may lack such as converting a router into a Wi-Fi hotspot, static routing, VPN, Quality of Service (QoS) options, IPv6 capability and many others. They also unlock settings that aren’t accessible normally, like antenna power and over clocking. Originally

designed for use with certain models of Linksys routers, they have expanded over the years to be compatible with other popular brands and also router manufactures like Buffalo ship their products with DD-WRT preinstalled. The main reason that these two firmware's were chosen over other free ones is that in the newer versions of DD-WRT from v.23 and higher Wiviz ver.2 comes pre installed and ready to work and OpenWrt provides the installation of Wiviz ver. 1 through the router interface directly. Also they are relative easy to install them on compatible routers and they are very stable firmware's. Of course they are available for specific models of routers which are listed in their documentation online. They are powerful firmware's that can turn a regular simple manufacturer router into a professional worth much more.

4) PuTTY: s a free terminal emulator that supports SSH, Telnet and many other protocols. PuTTY was originally written for Microsoft Windows and it is very useful for connecting to a UNIX or Linux SSH server or to telnet on a router and issue commands on it. PuTTY has a graphical configuration interface with many useful features such as storage of connection data for quick reconnection, port forwarding, IPv6 support SCP and SFTP support and many others. PuTTY has been ported to Linux and other Unix-like operating systems and in this system it is used by the application to login into the routers and to terminate or initiate the Wiviz process. It is also included into the installation file.

3.3.2 Hardware Requirements

The only hardware that this project needs is of course a power enough server to run the positioning system with access to the network infrastructure and a minimum of three access points compatible to run DD-WRT or OpenWrt or a higher number of access points in order to provide sufficient wireless coverage in the area and better accuracy.

3.4 System Interfaces

In this section a briefly guide of the application interfaces is presented in order for a better understanding how the system works. Figure 9 is the main window of the Wireless Positioning System. At first use the user can choose *"Build Fingerprint Database"* in order to jump to the fingerprint interface figure 10 and start building the signal database. Other functions that can be performed from this interface after the user has completed the information's textboxes are:

I. If OpenWrt is in use then the router's wireless card should be first put on monitor mode using (*"Start Monitor 1or Start Monitor 2"*)

II. Start the Wiviz scanning tool on all routers (*"Start Wiviz for all routers from Browser or SSH"*)

III. Transfer the results locally from the routers (*"Get the Wiviz data from all routers while the Browser mode is ON or OFF or through Telnet"*)

IV. Parse them and import them into the system (*"Import Data to Database"*)

V. Choose targets or target to localize by going to the locale interface figure 11 (*"Choose an item to locate"*).

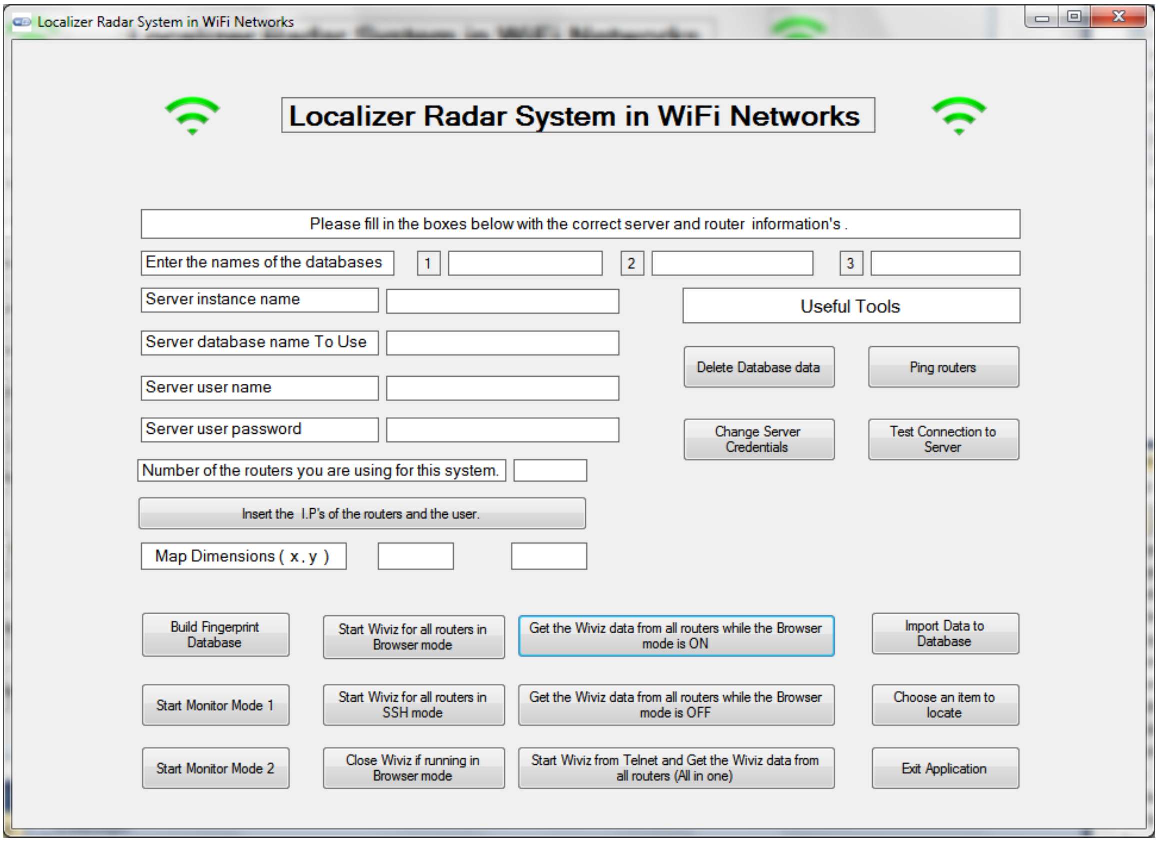

Figure 9: Main Interface

Also the other buttons represent small useful functions that can support debugging test such a ping all the routers in order to check if they are operational. The following interface in figure 11 is the fingerprint database interface in which as indicated by the name the user after fill in all the info textboxes can go forth with the collection and the building of the fingerprint database signals. The system supports the use of one and more mobile terminals which the sample readings are gathered. To use more than one mobile terminal in this phase is recommended because the average results that will be save in the database and use by the algorithm will face in a small degree the problems of multipath fading.

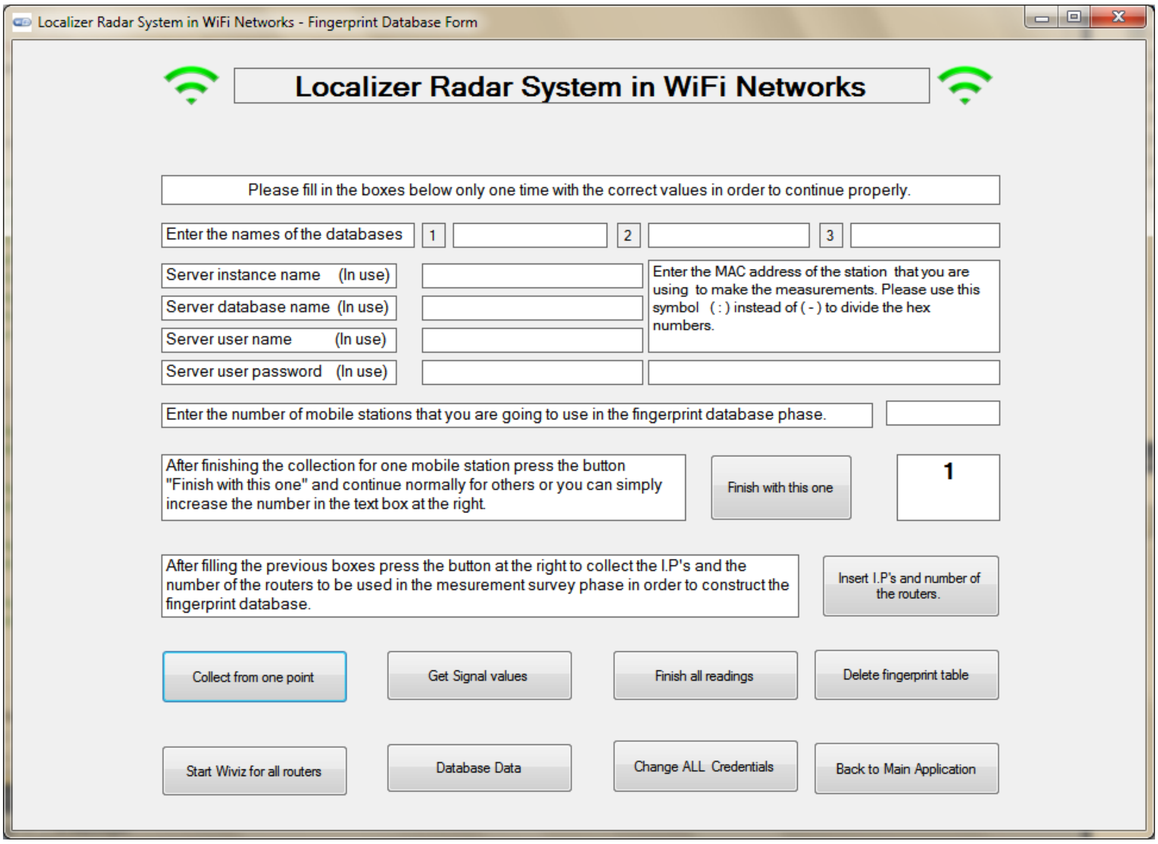

Figure 10: Fingerprint Database Interface

The next interface in figure 11 as name implies the user can choose which targets wants to locate, one or all, and see the estimate location on the map. The map can change according to the user are by simply inserting a picture map file in the folder *C:\Netcat\pic* and name the file map.jpg. The user can use the load button if necessary to load at the moment other map image. Also other functions include : rotate the map image, show a grid cell on map, track a user by using the Wiviz visually or by telnet and others. If the user wants to start and scanned other targets from the begginning then he will go back to the main interface and start the procedure on page 44.

Figure 11: Item Selection and Localization Interface

Finally the last interface in figure 12 is the Database Data interface in which the user can check all the data that are store in the database used by the application and even to update them or add new.

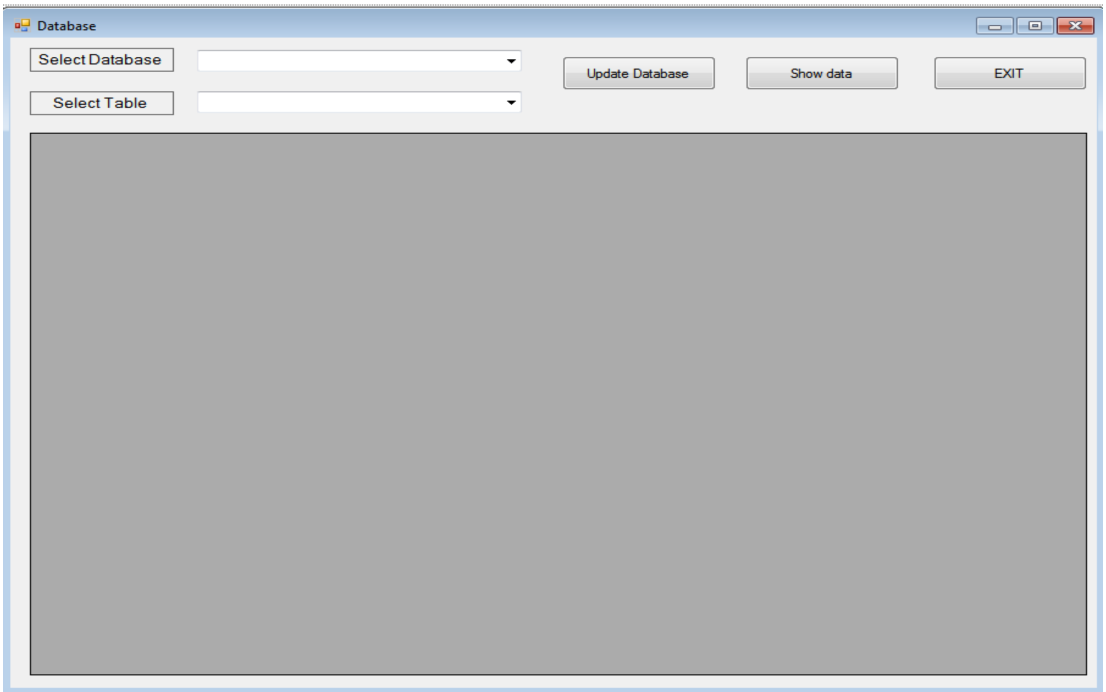

Figure 12: Database Data interface

3.5 Fingerprint Offline phase

Offline phase is the period that allows the positioning system to collect RSS data at the area of interest. The system also process and store the collected data into the database in order for the system to be able to estimate the mobile device's position in the online phase. This training must be done wherever the positioning system is first deployed. The time required for the training depends on the size of the survey site, the number of the reference location points, if more than one mobile terminal will be use and in this project case the numbers of databases to be develop. Usually this phase is very time consuming and costly and thus is the biggest disadvantage of it. Moreover, the database may need to be rebuilt if the surrounding environments of the area of interest changes significantly like add some wall partitions or a stack of furniture's. One of the most common setups for fingerprint database building is an infrastructure-based approach. Several fixed base stations transmit and receive beacons to and from a specific terminal. Then those readings are reporter back to a central server and store in a database. A less common is an infrastructure less approach, which only uses mobile nodes and distributes the database across the nodes. Storing the database on either a central computer, the base stations, or on the mobile node itself has its advantages and disadvantages in terms of scalability, privacy, resource-requirements etc. Storing the database on the mobile node is attractive because of the inherent support for privacy. On the other hand, mobile nodes are often resource-poor and can therefore only store a part of the database. Storing the database on a central computer on the other hand, can be a problem in terms of privacy, since the mobile node has to communicate with the server to determine its positions. In this thesis the database is store on the same centralizing server which the system is installed. Privacy issues is not a concern because as mention earlier this system is to be used as a security positioning application and therefore a mobile terminal in the area of interest in unaware that is been tracked.

Signal strength databases are the basis of wireless positioning. This system uses the free version of Microsoft SQL Server as a database tool. The software must be downloaded and installed by the user. Also the user is responsible to set it up and create the three data stores that reflect the three sample angle readings signals which the system will use. The first operation of the offline phase is to do a physical view test of the area of interest and then decide how many access points are enough for good space coverage. Of course if the access points are already installed in a wireless environment is good to consider going through the area with a mobile terminal and checking if their current network performance using a tool that measures signaling and throughput like *iPerf*. Then if possible to reallocate to achieve a better performance it would be for the best. Other factors when considering wireless AP's implementation are: avoid physical obstructions or barriers, avoid reflective surfaces such as windows and avoid locations that are closed to other wireless devices that can cause interference such as cordless phones. Then the fingerprint data collection can begin. During this stage sample RSS readings from all AP's are collected by a WLAN-enabled mobile device at desired known positions, referred to as the reference points. Usually the reference points can be chosen to form a grid for simplicity reasons. In this thesis, RSS readings are collected at all four directions, namely North, East, South and West and at the three different laptop angles of 90^o, 120^o 145^o degrees. This procedure is taking place in all reference points not only once but twice with the use of two different mobile devices. Afterwards all results are average and store in the database server along with the Cartesian coordinates of each point. The reason why this time consuming data collection method is essential is because by sampling RSS readings from all directions and different clients the results can address in a degree the wireless environment effects that corrupt the signals and results mention in chapter 2. For example the four direction collection rivals against the problems of multipath and the human signal blocking direction. Also the use of two different mobile terminals addresses the problem of the different antennas power signaling and location in the device. Generally it helps to reduce those problems but not significantly.

In short the steps of building the signal strength databases in this thesis are:

1. On site survey for wireless signaling network performance for better access point installation or reallocation if possible.
2. Reference point's location decision and tagged on a map.
3. The necessary information's of the wireless environment and server are entered into the application fingerprint database interface
4. A mobile terminal is positioned and measured at each reference point, at each direction and at each angle. This is repeated five times for each direction.
5. The previous procedure is repeated again with a different mobile terminal.
6. When finished the readings are averaged and store in the database for each access point.

After the fingerprint collection is done the system averages the results along with the coordinates of the reference points. After this phase the online detection phase can begin. These data are then used in the online phase for the computation of position estimations.

3.6 Online phase

To locate a mobile device online, the system needs to measure the real-time signal strength values of it. During the online phase, the device carried by a mobile user can be pointed to an unknown orientation and that's why in the offline phase measurements from all directions are taken into account. The system as mention uses Wiviz to scan unnoticed the wireless environment of the designated area. Then when the administrator chooses he can transfer the RSS readings from the access points locally, parse them and import them into the database for the application to use them.

Afterwards the system uses the online signals to produce a table with mobile terminals which have at least more than three RSS online signals so they can be positioned. The localization algorithm in this thesis as mention in page 24 is the Search by Nearest Neighbor.

The process of estimating the location coordinates of a target terminal is as follow: For example consider an online RSS measurement for a particular terminal located in the area of interest from three access points. The measurement is transformed into a vector denoted as:

$$PT = (-A1\ dbm - A2\ dbm - A3\ dbm\ )^T$$

Then the vector is normalized into:

$$PT = (((0)\ ((-A2\ dbm) -\ (-A1\ dbm))((-A3\ dbm) -\ (-A1\ dbm))\ )^T$$

Also the table which holds the RSS data sorted by access point in ascending order is also normalized the same way as the online RSS vector. Then the Euclidean distance formula at page 25 is applied between them, resulting in a new table listing an estimated measurement metric in meters for each reference point. This measurement represents the estimated distance calculated at each reference point from the three access points in respect to the RSS vector of the mobile terminal at time t. Then three reference points are chosen related to the smallest measurement values which reflect to the nearest neighbor of the mobile target. Finally the x and y coordinates of those points are averaged using the formula at page 25 with $L=$ the number of points chosen, which is the number of access points and an estimated result is produced. The accuracy of the estimated result both heavenly on the fingerprint database readings and also on the algorithm structure itself.

3.6.1 Accuracy of Search Nearest Neighbor RSS

As mention earlier in chapter 2.5 RSS signals are affected negative by numerous factors, even the number of people and the day of time affect the wireless signaling inside a building. In both offline and online phases the RSS sample and real time readings contain an error of disruption due to environment factors that affect wireless signaling. During the offline phase the method followed in this thesis, sampling signals from all directions, from three different angles, using two mobile terminals and sampling multiple signals from all previous instances minimizes in some degree and basically reflects the influence of those factors on the finals value s store in the fingerprint database. On the other hand in the online phase when the system scans the area it only “grasp” a particular instance of the network environment at a time *t*. At that time the possibility of a mobile terminal experiencing the same RSS values as the ones in the database during measurement are minimal. Due to these reasons is difficult to estimate the accuracy of the algorithm because it is working under different situations but nether less in a study [7] taken place in an office wireless environment the accuracy was measured as better than 3m with a probability of 50% and 4.7m for a probability of 75%. The office size was 43 x 25 m and three access points were in use and 70 reference points were sampled. It seems not be an impressive ratio but if considering that this system works in a constantly unstable environment, needs no extra hardware and infrastructure devices such as tag because is mainly a software solution with an attractive low cost then it is an impressive system which provides good accurate results in a large space. Also better accuracy can be achieved by increasing the number of access points.

3.6.2 Privacy Concerns during the Online phase

There is little doubt that location aware mobile devices have enormous potential for enhancing safety, convenience, and utility in our lives. Already emergency services are being improved by the ability of responders to quickly locate persons making emergency calls or involved in accidents in location-aware vehicles. Unfortunately, the same technologies that bring benefits like the ones mentioned above raise hundreds of privacy issues due to their capability to collect, store, use, and disclose the locations of those who use them. The system develop for this thesis act as a security positioning system and thus is able to position a mobile target without its knowledge when enter in the area of interest such as an office building. In any under circumstance this system collects and store private data from mobile targets. The positioning capability of this system is not intended to be used to reveal damaging and perhaps embarrassing information, or lead to discrimination or for employee monitoring. Also special attention must be given to the security of the wired and wireless network in order to prevent unauthorized access which can lead to the exposure of the fingerprint database or to the system application from unwanted users.

3.7 Chapter Summary

This chapter has presented a detailed guide how to set up the system and the software and hardware requirements. The system involves two phases. The offline phase in which the fingerprint database is created from RSS sample readings and the online phase in which the positioning is taking place using the Nearest Neighbor algorithm.

Chapter 4 Experimental Setup and Results Analysis

This chapter describes the experimental setup of the positioning system, the measurements and fingerprint databases construction and provides a small comparison of the results of both online and offline phase. The proposed system is evaluated in two different experimental RSS maps using the devices mentioned in section 4.1. Also the RSS readings are collected in real indoor environments in order to evaluate the performance of the proposed system in a dynamic and unpredictable wireless indoor environment.

4.1 Software Platform and Devices

The software is written in Visual Basic 2010 Express (free version) and it is compatible only with Windows operating systems of version XP and later. Also the free version of Microsoft SQL Server 2010 is installed locally and three databases are created namely angle90, angle 120 and angle145 representing the three different laptop angles under testing. The platform is develop and tested in my house second floor. A small independent network has been created using three access points and a router. The three access points are use to collect RSS samples and the router to direct those RSS readings to an HP dc5750 pc that the platform is installed on it. The access point’s model is the well known Linksys WRT54GL ver. 1 and it is chosen because their ability to install DD-WRT or OpenWrt firmware easily, run Wiviz and support also Netcat. The following figure number 13 presents the minimum hardware needed to run the positioning system and also the two laptops used to collect RSS sample readings during the offline phase for the fingerprint database creation.

Devices	Processor Speed	RAM	WLAN	Purpose
HP dc5750	AMD Dual Core 2.0 GHz	3 GB	NO	Database server and system installed on it. The administrator runs the system.
IBM Lenovo 3000 N100	Intel Core 2 Duo 1.66 GHz	2 GB	802.11 b\g	Collect RSS samples in fingerprint database
Sony VGN-BX196SP	Intel Pentium M 1.86 GHz	2 GB	802.11 b\g	Collect RSS samples in fingerprint database
Linksys WRT54GL ver.1	Broadcom BCM5352 200 MHz	16 MB	802.11 b\g	To scan the area for wireless targets. Build fingerprint database.
Linksys WRT54GS ver.1	Broadcom BCM5354 240 MHz	16 MB	802.11 b\g	To serve as a router connecting the access points, the server pc and providing internet access.

Table 2: System Devices

4.2 Offline Phase Experiment and Setup of Map 1

As mentioned earlier the experimental testbed is the second floor of my house, shown in Figure 14. It is an area of 4 x 18.6 meters, including wall partitions and other wireless obstacles such as furniture's or mirrors. At the beginning different locations were consider for the access point installation but in the end after RSS power measurements taken using the two laptops mention in figure 13 from the OpenWrt interface directly it is decided to be installed as in figure 14 because they provide better coverage especially for the close environment spaces. Then the reference point's location should be decided. Due to the small place the reference point's number should not be too many and not too close in order to snap the RRS deviation and variation effects. In order to test that theory it was decided as a first step to take

RSS measurements at x points 1.2, 2.4 and 3.6 m for the x horizontal axis and for the vertical y axis just increasing the space in such a way in order to get a minimum of one measurement in all rooms. The reference points are shown in figure 14 as dot circles. In this experiment only one laptop (Lenovo) were used to build the database and also measurements were taken only for angle 120^{o} because we are interested only to test if theoretically the small parse and distance of the reference points between them should lead to false results.

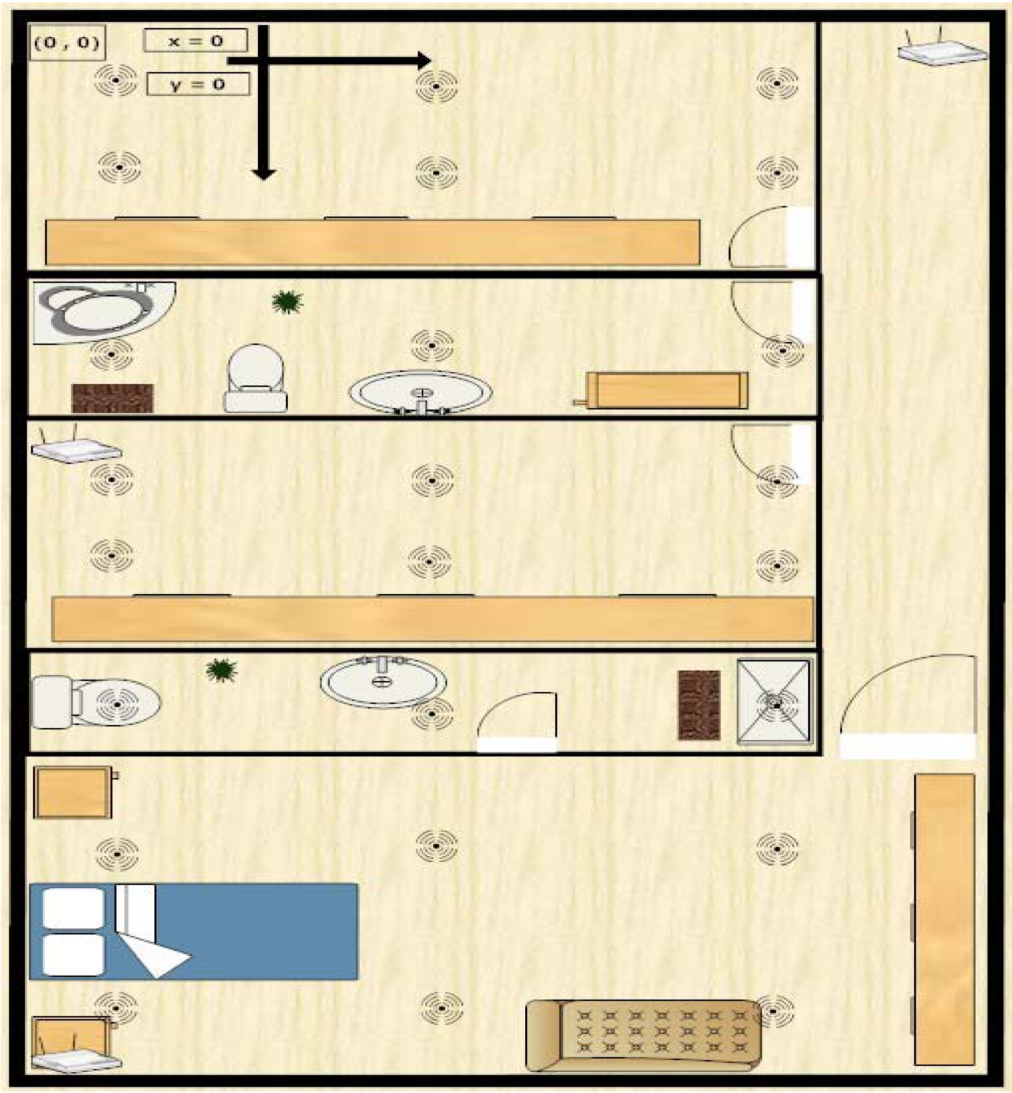

Figure 13: First Experimental Setup Map

There were 20 samples for each reference location, 5 for each direction. The data were read out by the system, normalized against access point 1 and the average value was calculated and stored in the database as shown in figure 15 in order to be used as offline data to do positioning.

ALEXK-PC\ALEXK...RMALIZED_TOTAL

id	x	y	AP1	AP2	AP3
1	1.2	1.5	0	-5	-26
2	2.4	1.5	0	-21	-41
3	3.6	1.5	0	-32	-42
4	1.2	3	0	-14	-37
5	2.4	3	0	-17	-38
6	3.6	3	0	-18	-45
7	1.2	6	0	7	-22
8	2.4	6	0	1	-28
9	3.6	6	0	-9	-31
10	1.2	9	0	-22	-17
11	2.4	9	0	12	-21
12	3.6	9	0	-8	-24
13	1.2	11	0	5	-20
14	1.2	11	0	5	-17
15	3.6	11	0	5	-13
16	1.2	13	0	-5	-4
17	2.4	13	0	-10	3
18	3.6	13	0	-3	-1
19	1.2	15	0	17	18
20	2.4	15	0	4	16
21	3.6	15	0	7	3
22	1.2	17	0	2	32
23	2.4	17	0	3	28
24	3.6	17	0	1	24

Figure 14: Many Reference points RSS readings

Then the Lenovo laptop was used as a mobile target during the online phase. The system was scanning the wireless area and the network administrator was issuing a positioning procedure when the target was visible. This was done in various locations and the results are shown in the following table 3. The distance error is calculated from the following formula:

$$E\ (Distanse\ Error) = \left(\sqrt{(x - \hat{x})^2 + (y - \hat{y})^2} \right)$$

Where the estimated location is $(\hat{x}, \hat{y})$ and the true location is(x, y) .

Point id	Real locations (m)		Estimated locations (m)		Distance Error (m)
	x	y	x	y	*E*
1	3.10	5.00	1.50	8.00	3.40
2	2.10	10.00	1.20	8.60	1.66
3	0.40	16.60	2.33	15.60	2.17
4	2.50	13.00	2.33	15.00	2.01
5	4.00	9.00	1.33	8.66	2.69
6	1.00	7.00	1.40	7.80	0.89
7	3.16	0.30	2.33	4.00	3.79

Table 3: Estimated Results for many reference points

Table 3 shows the estimated location points and the distance error for each one. The average distance error for 7 location points is 2.37 m which is a relative bad result. It is a relative bad result because in some cases like a big open space where the estimated target locations provide visual sight estimation can be consider as a relative good result. On the other hand in a close building environment a distance error could mean that a target is located in a different room that the one estimated by the Cartesian coordinates on the map. Also another observation is that the estimated locations have tendency to converge towards the middle of the area. This is due to the close reference points RSS measurements taken for the fingerprint database. Because the reference points are too close between them the RSS sample taken earlier do not change significantly in terms of power value and so when the algorithm is looking for the nearest neighbours and perform the necessary computations all neighbours are too close between to the center. It is safe to state now that the approach of having too many reference points in a small close environment are should be avoided.

4.3 Offline Phase Experiment and Setup of Map 2

Next by abandoning the previous idea a more scatter radio map with less reference points having a greater distance between them is decided to be develop. Again in this phase as the previous one the laptop angle factor is not taken into account. The access points will remain at same place as previous but now the RSS measurements will be taken at x points 1 and 3 m for the x horizontal axis and for the vertical y axis increasing the space for 2.5 m in such a way in order to create a grid manner scale. Again 20 sample readings will be collected for each reference point, 5 for each direction. The RSS map of this experiment is showing in figure 18. Also in this experiment two databases will be constructed. The one will contain only RSS sample collected using only the Lenovo laptop and the other will contain the average RSS samples from both laptops. This done in order to check how much the accuracy improves as the number of RSS samples from different stations increases.

First in order to show the behavior and more accurate the deviation that an RSS signal is going through due to the different wireless factors figure 17 presents a comparison for all RSS sample readings collected from all new 14 reference points from the three access points. It is obvious that in most reference points measurements the RSS signals corresponding to the two different laptops do have a small but also a large value difference. This figure proves the theory of the RSS signaling disruption and justifies why the RSS fingerprint database should be built from samples of more than one terminal. Figure 15 and 16 presents the sample RSS reading from the Lenovo and Sony laptop respectively, collected during the offline phase which are not normalized against the first access point RSS value. These new reference points represent the idea of a more scatter RSS map in the area of interest.

ALEXK-PC\ALEXK.test2 - dbo.FINGER1

id	x	y	AP1	AP2	AP3
1	1	1	-45	-63	-89
2	3	1	-48	-57	-86
3	1	3.5	-49	-58	-84
4	3	3.5	-46	-57	-85
5	1	6	-55	-47	-78
6	3	6	-56	-50	-81
7	1	8	-60	-43	-74
8	3	8	-62	-38	-76
9	1	11	-64	-47	-72
10	3	11	-63	-42	-70
11	1	14.6	-59	-56	-55
12	3	14.6	-71	-57	-54
13	1	18	-61	-64	-47
14	3	18	-67	-69	-42
NULL	NULL	NULL	NULL	NULL	NULL

Figure 15: Lenovo laptop RSS samples readings

ALEXK-PC\ALEXK.test2 - dbo.FINGER2

id	x	y	AP1	AP2	AP3
1	1	1	-52	-62	-87
2	3	1	-47	-60	-85
3	1	3	-44	-57	-86
4	3	3	-55	-59	-85
5	1	3	-58	-50	-82
6	3	3	-52	-56	-84
7	1	8	-66	-44	-78
8	3	8	-60	-45	-82
9	1	11	-63	-41	-77
10	3	11	-67	-43	-74
11	1	14.6	-74	-68	-56
12	3	14.6	-60	-62	-54
13	1	18	-74	-67	-44
14	3	18	-62	-68	-50
NULL	NULL	NULL	NULL	NULL	NULL

Figure 16: Sony laptop RSS samples readings

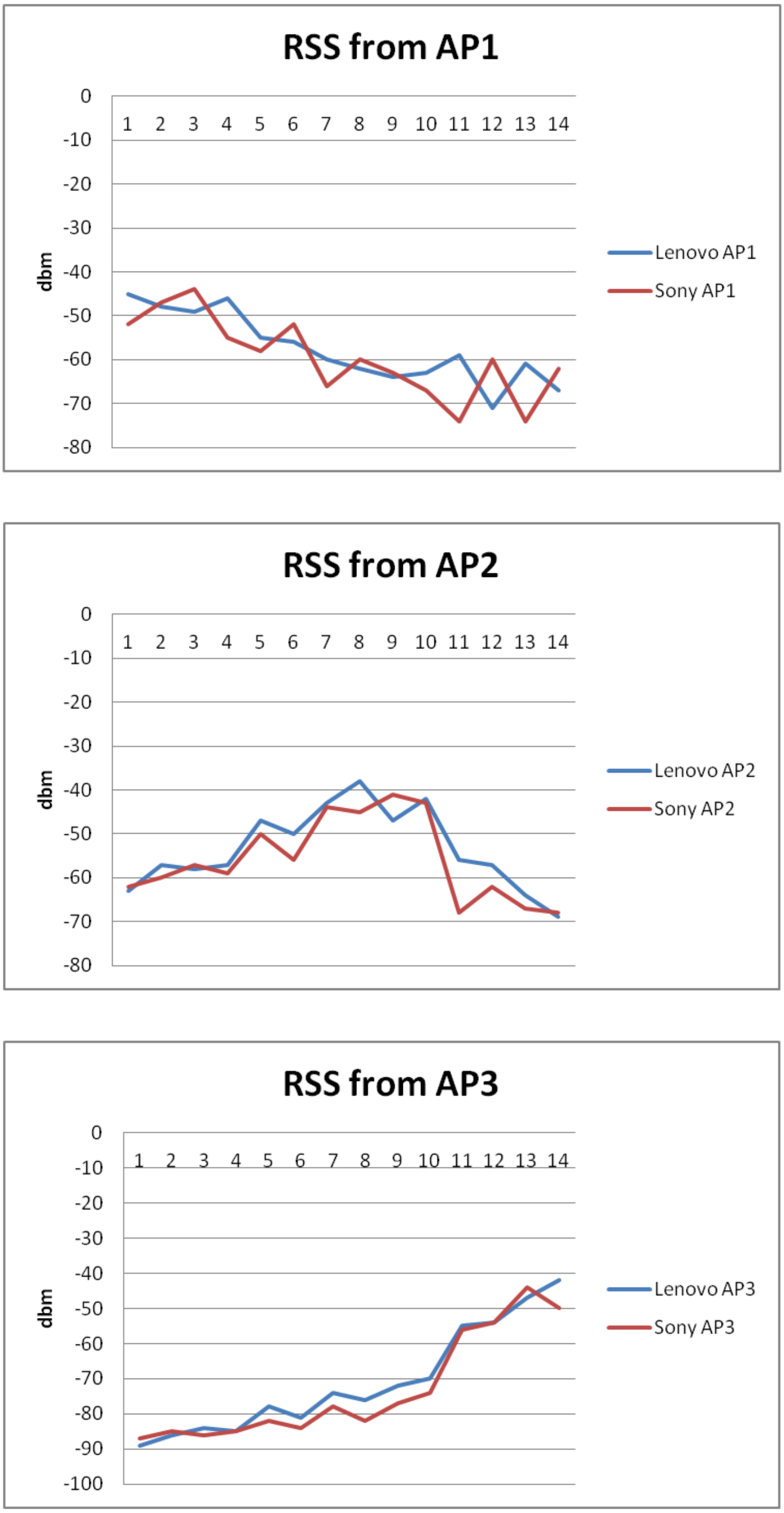

Figure 17: Comparison between RSS samples from two laptops

The comparison charts in figure 17 clearly state the unpredictable and dynamic wireless environment and the effects on RSS signalling. In most cases the RSS samples have a different value between the two laptops. For this reason is best to measure the accuracy of this algorithm not with absolute values but in terms of distance measurements. Of course the goal is always to minimize the distance error and improve the estimated location result. The following table 4 shows the real and the estimated location points and the distance error for each one for the database containing the average RSS samples taken from both laptops. Comparing with the previous table 3 in page 58 for the first experimental setup the average distance error has been reduced to 2.09 m from 2.37 m. The estimate locations results have an increase of accuracy of 11.8 % by reducing the reference points but also using two the measurements from two laptops and not one.

Point id	Real locations (m)		Estimated locations (m)		Distance Error (m)
	x	y	x	y	*E*
1	3.10	5.00	2.33	6.667	1.83
2	2.10	10.00	1.67	7.33	2.71
3	0.40	16.60	1.67	16.00	1.00
4	2.50	13.00	1.67	14.33	1.57
5	4.00	9.00	2.33	7.66	2.14
6	1.00	7.00	2.33	5.33	1.70
7	3.16	0.30	2.33	3.00	2.82

Table 4: Estimated Results for less reference points (2 databases)

As said at the beginning of this experimental phase two databases will be constructed. The one is has been presented earlier at pages 61 and 62 and it contains RSS sample readings measurements with the new RSS map with less reference points but averaged RSS samples from both laptops. In the following table 5 the estimated results for the same location points as previous are presented but this time the fingerprint database contains only the RSS samples from the Lenovo laptop listed at figure 15.

Point id	Real locations (m)		Estimated locations (m)		Distance Error (m)
	x	y	x	y	*E*
1	3.10	5.00	1.66	6.66	2.20
2	2.10	10.00	1.00	8.33	2.00
3	0.40	16.60	2.33	17.00	1.97
4	2.50	13.00	1.66	13.66	1.07
5	4.00	9.00	1.66	6.66	3.31
6	1.00	7.00	1.66	5.33	1.80
7	3.16	0.30	2.33	3.00	2.82

Table 5: Estimated Results for less reference points (1 database)

The average distance error in this case is 2.17 m. It is more accurate from 2.37 m measure in the section 4.2 by 8.43 % but less accurate than the one measure earlier in this experiment by 3.67 %. By precision terms the most precise results are provided by the experiment with fewer reference points and the fingerprint database made up from the averaged RSS values from both laptops because 4 points out 7 have distance error within the distance range of 0-2 m and 3 within the distance range of 2-4 m. The other experiment in this section estimates 3 points out 7 have distance error within the distance range of 0-2 m and 4 within the distance range of 2-4 m. On the other hand the experiment phase in section 4.2 estimates 2 points out 7 have distance error within the distance range of 0-2 m and 5 within the distance range of 2-4 m.

The following table 6 presents the precision accuracy in terms of probabilities, of an estimated target to be physically located with in the range of 0-2 m or of 2-4 m from the estimated Cartesian coordinates on the map.

Concluding its best to say that in a small but also and in a large area reference points should at least have a minimum distance of 2 m and preferably higher in order to be able to actually reflect the changes that an RSS signal is suffering. Also it is logically to assume that by increasing the number of access points, the number of measurements of RSS sample readings for each direction and also the number of devices that the samples are taken like the first experiment in this section a better estimate results in terms of accuracy and precision will be achieve.

Experiment Map	Laptops	Fingerprint Database	Probability within in 0-2 meter	Probability within 2-4 meters
Section 4.3-a	1	from1 laptop	4/7=57.2%	3/7=42.8%
Section 4.3-b	2	from2 laptops	3/7=42.8%	4/7=57.2%
Section 4.2	1	from1 laptop	2/7=28.6%	5/7=71.4%

Table 6: Estimated Probabilities

4.4 Offline Phase Experiment and Setup of Map 3

In this section the final experimental phase will represent the actual implementation of the system. The reference points and access points will remain the same as section 4.3. Also in this experimental phase the measurements will contain the values for the three different angles in order to built three different databases (angle90, angle120, angle145). Again the sample RSS measurements will be collected using the average values from both laptops. The RSS radio map for this scenario is illustrated in figure 18. In order to be able to compare the estimate locations results produce from the system are going to be outputted in a txt file called *results.txt* on the local *C* drive, containing the estimate results for each angle fingerprint database and the final average location (x, y). Also by creating the new angle databases we can compare the RSS distribution over time with the database created in section 4.3 since the radio map and configuration remains the same. The fingerprint collection is exactly the same as before. At each reference point 5 samples are collected at each orientation for each angle database. This procedure is repeated twice using two different laptops. Finally the system average and save the results in the database server locally.

It is important to compare the relationship between the RSS deviation cause by the antenna position because users in a real life scenario do not handle their wireless enable devices such as smart phones, pads and others in a standard position of angle and height. So by slightly change the antenna position the RSS signal that a laptop experiences changes automatically. Due to this uncontrolled user variation, measuring different RSS angles it is assume a better estimated result will be produced.

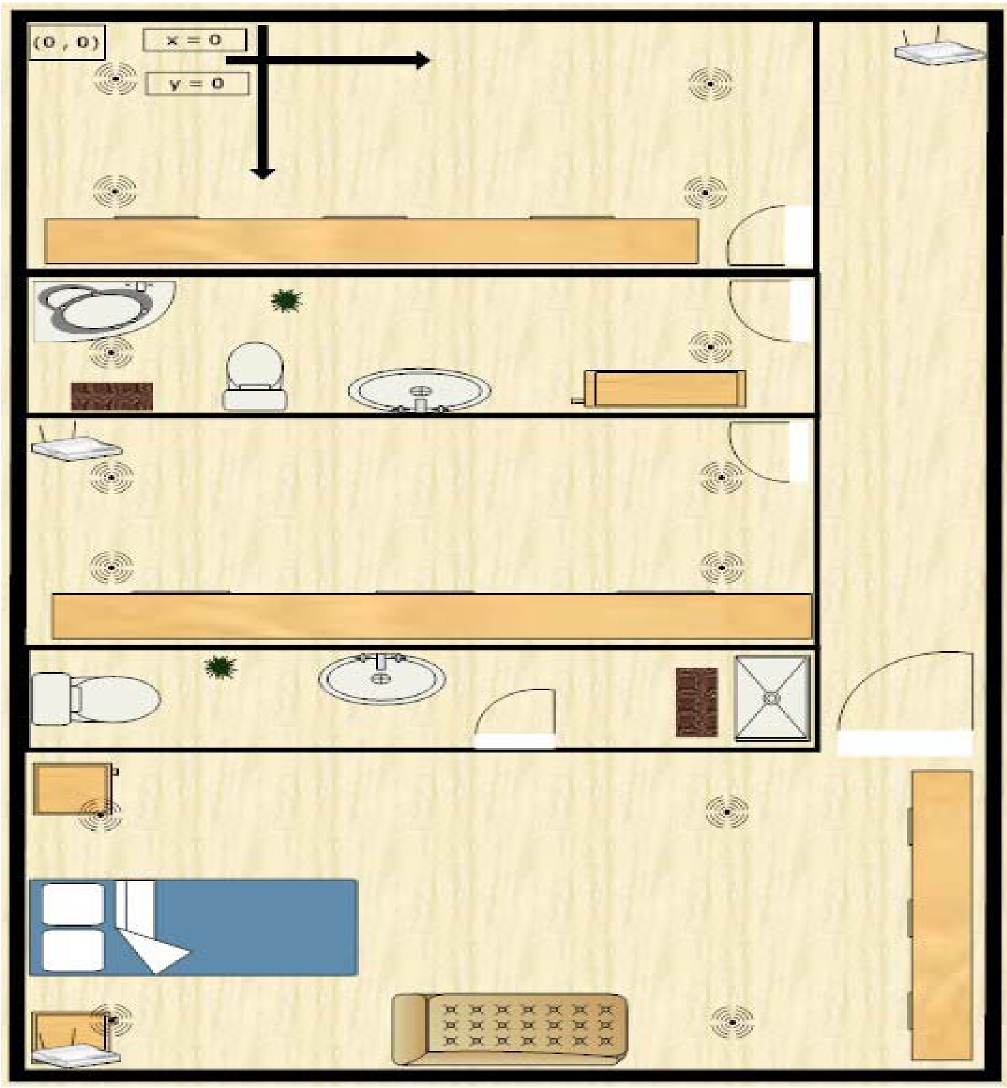

Figure 18: Second Experimental Setup Map

In order to show the deviation of RSS distribution over time a comparison between sections 4.3 with the databases created in this experiment is presented at page 68, but first the RSS samples taken for the angle databases are presented at the next page. It is worth mentioning that the RSS readings at section 4.3 were taken by not considering the angle of the laptop.

RSS Samples Angle 90 from Lenovo

ALEXK-PC\PROJEC...0 - dbo.FINGER2 | ALEXK-PC\PROJEC...0 - dbo.FINGER1

id	x	y	AP1	AP2	AP3
1	1	1	-51	-63	-83
2	3	1	-49	-67	-88
3	1	3.5	-55	-58	-86
4	3	3.5	-46	-64	-85
5	1	6	-58	-47	-77
6	3	6	-45	-55	-80
7	1	8	-55	-36	-74
8	3	8	-53	-47	-72
9	1	11	-66	-49	-71
10	3	11	-65	-45	-70
11	1	14.6	-59	-66	-50
12	3	14.6	-72	-60	-57
13	1	18	-60	-63	-41
14	3	18	-67	-65	-48
NULL	NULL	NULL	NULL	NULL	NULL

RSS Samples Angle 120 from Lenovo

ALEXK-PC\PROJEC...20 - dbo.FINGER1

id	x	y	AP1	AP2	AP3
1	1	1	-53	-64	-84
2	3	1	-47	-68	-90
3	1	3.5	-55	-57	-85
4	3	3.5	-50	-63	-86
5	1	6	-59	-46	-80
6	3	6	-47	-56	-81
7	1	8	-59	-37	-73
8	3	8	-49	-47	-74
9	1	11	-63	-52	-70
10	3	11	-61	-48	-73
11	1	14.6	-62	-66	-49
12	3	14.6	-71	-60	-56
13	1	18	-66	-67	-44
14	3	18	-72	-64	-50
NULL	NULL	NULL	NULL	NULL	NULL

RSS Samples Angle 145 from Lenovo

ALEXK-PC\PROJEC...45 - dbo.FINGER1

id	x	y	AP1	AP2	AP3
1	1	1	-50	-63	-83
2	3	1	-54	-67	-93
3	1	3.5	-58	-59	-84
4	3	3.5	-52	-60	-87
5	1	6	-58	-49	-76
6	3	6	-49	-57	-79
7	1	8	-62	-35	-72
8	3	8	-51	-45	-77
9	1	11	-63	-51	-71
10	3	11	-66	-46	-72
11	1	14.6	-55	-66	-51
12	3	14.6	-73	-67	-55
13	1	18	-66	-68	-44
14	3	18	-71	-64	-51
NULL	NULL	NULL	NULL	NULL	NULL

RSS Samples Angle 90 from Sony

ALEXK-PC\PROJEC...0 - dbo.FINGER2

id	x	y	AP1	AP2	AP3
1	1	1	-52	-65	-84
2	3	1	-45	-62	-83
3	1	3.5	-53	-65	-81
4	3	3.5	-50	-55	-82
5	1	6	-51	-48	-73
6	3	6	-60	-59	-80
7	1	8	-63	-32	-74
8	3	8	-54	-43	-77
9	1	11	-66	-47	-76
10	3	11	-69	-40	-73
11	1	14.6	-75	-66	-50
12	3	14.6	-61	-60	-50
13	1	18	-71	-65	-40
14	3	18	-66	-64	-48
NULL	NULL	NULL	NULL	NULL	NULL

RSS Samples Angle 120 from Sony

ALEXK-PC\PROJEC...20 - dbo.FINGER2

id	x	y	AP1	AP2	AP3
1	1	1	-51	-66	-85
2	3	1	-47	-59	-83
3	1	3.5	-50	-67	-82
4	3	3.5	-49	-57	-79
5	1	6	-47	-49	-74
6	3	6	-58	-57	-81
7	1	8	-64	-30	-78
8	3	8	-50	-48	-76
9	1	11	-68	-50	-74
10	3	11	-66	-39	-71
11	1	14.6	-74	-64	-52
12	3	14.6	-58	-61	-55
13	1	18	-73	-66	-40
14	3	18	-66	-64	-49
NULL	NULL	NULL	NULL	NULL	NULL

RSS Samples Angle 145 from Sony

ALEXK-PC\PROJEC...45 - dbo.FINGER2

id	x	y	AP1	AP2	AP3
1	1	1	-55	-66	-88
2	3	1	-45	-62	-86
3	1	3.5	-56	68	-82
4	3	3.5	-48	-59	-81
5	1	6	-52	-49	-72
6	3	6	-60	-65	-80
7	1	8	-62	-61	-78
8	3	8	-49	-52	-77
9	1	11	-69	-49	-75
10	3	11	-68	-42	-70
11	1	14.6	-75	-65	-54
12	3	14.6	-57	-62	-56
13	1	18	-73	-67	-41
14	3	18	-68	-66	-50
NULL	NULL	NULL	NULL	NULL	NULL

Figure 19: RSS angle readings

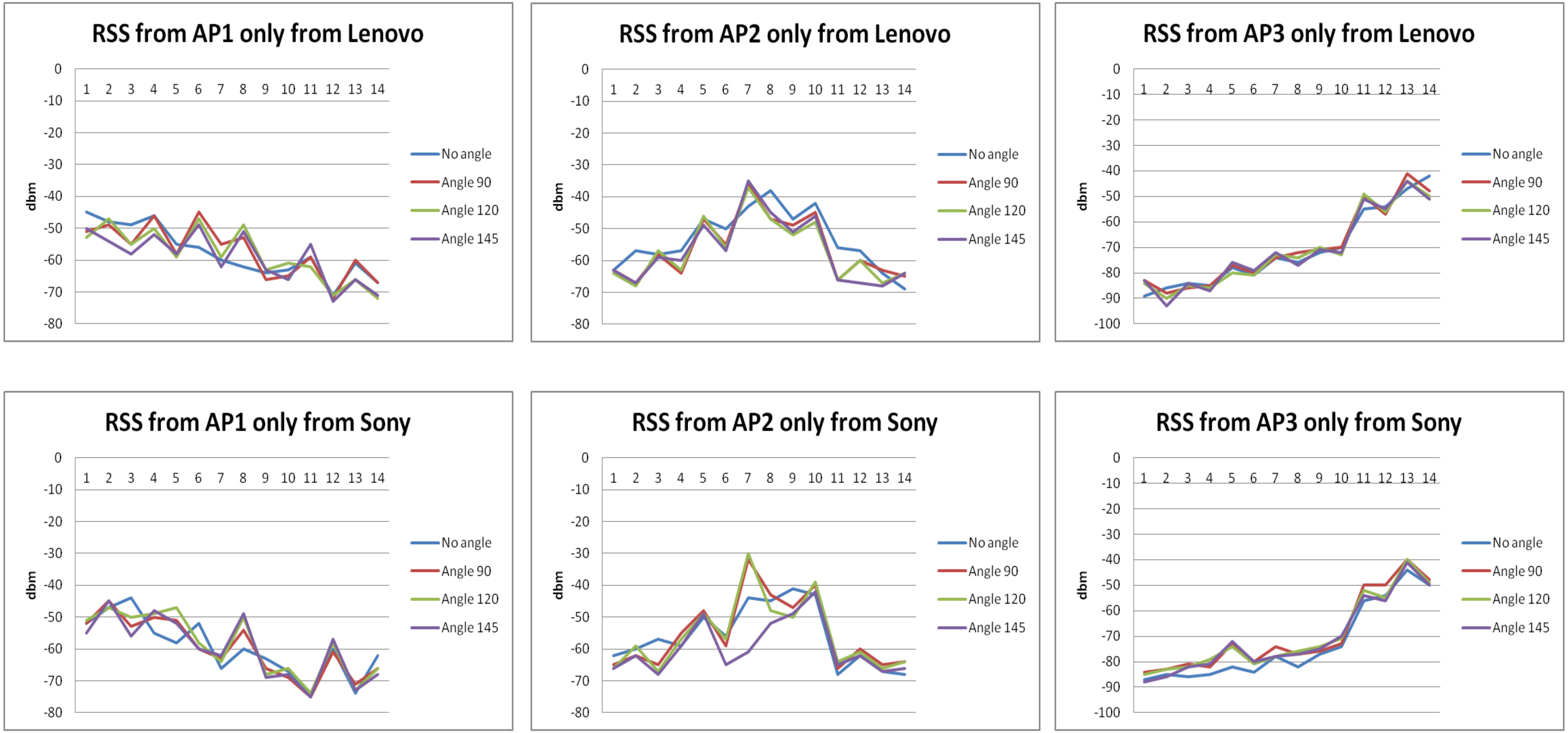

Figure 20: RSS readings from both laptops for all angles and no angle

Figure 19 just shows the new RSS readings for the angles databases, which in turn the tables show that the values in each cell are different for each reference point. For example the first sample with id 1 for angle 90 for the Lenovo laptop is (-51 -63 -83) and for the Sony (-52 -65 -84) which their deviation is small and has a minimum effect on the final estimated result. On the other in the same tables the sample with id 11 form the vectors (-59 -66 -50) and (-75 -66 -50). Despite that the two last values came out the same, the first value observe from AP1 has a difference of -26 dbm. This value can cause a significant deviation to the final estimated result due to the algorithm structure calculations. When the algorithm will average those vectors in order to create the final normalize RSS tables if in use was only the samples from the Lenovo laptop the normalize vector should look like (0 -7 9) and if in use was only the samples from the Sony laptop the normalize vector should look like (0 9 25). On the other hand if in use was the averaged RSS from both laptops the normalize vector should look like (0 1 17). This extreme example in the database states the different wireless factors that affect an RSS sample to its actual numerical value. Also it shows why it is important to use more than one client terminal to built the fingerprint database, because it helps to reduce the negative impact of the different environmental wireless factors and not. Furthermore this illustrates that the antenna gain for Sony is smaller than the one for the Lenovo.

Next another significant observation is that if we compare the same RSS vectors from each laptop for each angle in figure 20 the graphs show that deviation between the angles is not great but can cause different estimated results. So by taking into account the different angles RSS measurements can improve the final estimated result but not as much as taking into account RSS measurements from different clients. Of course the ideal is to take into account both cases but this is very time consuming.

Also in figure 20 the angle RSS samples are compared with the ones collected at section 4.3 which no angle was under consideration. This is done in order to show the RSS distribution over time. As said the trend of the RSS distributions across the angle different measurements does not change significantly but when compare with the RSS distribution at section 4.3 in almost all points the deviation is big enough and able to produce different results. It's worth mentioning that the database in section 4.3 was built on a different day than the latest ones. So a good practice can be to build a fingerprint database in which two and more terminals will be used and their samples will be collected on different time periods. The above observations may directly cause many traditional localization models to fail if they use the data collected at one time period, in one subarea or by one device for training and the data collected at another time period, in another subarea or by another device for testing. Finally there is no need to compare the values for each angle for both laptops because it is obvious from figure 19 that are different as shown earlier.

As mention earlier the final system uses the three different angle databases not only to show the relationship and the effect between the RSS signaling and the laptop angle but also to average the estimated location results produce by using separately each database and form a final one which is presented to the user on the map. All the results are saved in a txt file at local C directory as mentioned. The same reference points are used to show the estimated calculations locations points as before in the other sections. The results are summarized in table 7 at next page.

Point id	Real locations (m)		Angle 90 Estimated locations (m)		Angle 120 Estimated locations (m)		Angle 145 Estimated locations (m)		All angles Estimated locations (m)		Distance Error (m) 90	120	145	All angles
	x	y	x	y	x	y	x	y	x	y	*E*	*E*	*E*	*E*
1	3.10	5.00	2.33	6.67	2.33	6.67	1.67	5.83	2.11	6.39	1.84	1.84	1.65	1.71
2	2.10	10.00	1.67	8.33	1.67	9.33	1.67	9.33	1.67	9.00	1.72	0.80	0.80	1.09
3	0.40	16.60	2.33	15.73	1.67	16.87	2.33	16.87	2.11	16.49	2.12	1.30	1.95	1.71
4	2.50	13.00	2.33	12.20	2.33	15.73	2.33	13.33	2.33	13.76	0.82	2.74	0.37	0.78
5	4.00	9.00	2.33	6.67	2.33	6.67	1.67	5.83	2.11	6.39	2.87	2.87	3.93	3.22
6	1.00	7.00	2.33	5.83	2.33	6.67	2.33	5.83	2.33	6.11	1.77	1.37	1.77	1.60
7	3.16	0.30	1.67	2.67	1.67	2.67	1.67	1.83	1.67	2.39	2.80	2.80	2.14	2.57
Average Distance Error (m) for each angle case											**1.99**	**1.96**	**1.80**	**1.81**

Table 7: Estimated Results for less reference points (All angles databases)

What is interesting in this table is the relationship that derives when comparing the estimated results for the three different angle databases. Angle 90 and 120 have a close distance error rate compare with 1.80 m that the angle 145 has. The main reason of course is the large angle that the two laptops had during RSS sample measurement phase. Due to the antenna position iside the top plastic of the screen and to the wide angle the distance between the user and the client terminal laptop increases proportional in compare with the other angles. This limits the effect of the negative wireless factors such as multipathing, fading and the most important of all in this measurement phase the effect of user’s presence on RSS. Because the human’s body consists of 70% water and resonance frequency of water is at 2.4 GHz and the RSS is absorbed when the user obstructs or is relative close to the signal path and causes an extra attenuation. This extra attenuation is maximum significant to be present during the fingerprint database collection because if a user is not present then the values collected will not reflect the user presence in the area of interest.

Another point coming out of the previous table is that the estimated values produce from the final system which uses the average estimated locations from all angle databases do not improve the distance error rather doing exactly the opposite, the first two angles 90 and 120 contribute to the increase of the error rate and only angle 145 decreases it. This leads to the assumption that if the three databases were built using only angle 145 will probably decrease the distance error even more but probably with not a big difference.

Next in term of probabilities the following table 8 presents the precision accuracy of the distance error, of an estimated target to be physically located with in the range of 0-2 m or of 2-4 m from the estimated Cartesian coordinates on the map. The comparison is between this experimental final phase and the one described in section 4.3 but this time with the data we have estimated values with distance error less than 1m that should taken into account.

Experiment Map	Laptops	Fingerprint Database	Angle	Probability within in 0-1 meter	Probability within in 1-2 meter	Probability within 2-3 meters	Probability within 3-4 meters
Section 4.3-a	2	from2 laptops	random	0	4/7=57.2%	3/7=42.8%	0
Section 4.4	2	from2 laptops	90	1/7=14.2%	3/7=42.8%	3/7=42.8%	0
Section 4.4	2	from2 laptops	120	1/7=14.2%	3/7=42.8%	3/7=42.8%	0
Section 4.4	2	from2 laptops	145	2/7=28.5%	3/7=42.8%	1/7=14.2%	1/7=14.2%
Section 4.4	2	from2 laptops	all angles average	1/7=14.2%	4/7=57.2%	1/7=14.2%	1/7=14.2%

Table 8: Estimated Probabilities for final system

A closer look in the previous table reveals that actually angle 145 has the highest accuracy percentage in terms of estimated location precision because it estimates two results within 1 meter instead of the other angles which estimate only 1 result and 0 result from section 4.3 a database. What is interesting about angle 145 is also the worst result between 3-4 meters. This raise some suspicious because in table 7 angle 145 has the highest distance error for point 4 which estimates (1.67, 5.83). The x and y coordinate values have almost 1 m difference compare with the other results from the other databases. This is exactly the negatives effects of the wireless factors which are uncontrolled by humans. A possible solution to this is to manually replace the values of the RSS samples in the problematic database to match the closest values from the others. Then run the system again until a better result is estimated. Of course this is not an optimal solution because is a complicate and time expensive task that must be done with extreme precaution. Also what is important in table 8 is that the random database has all the estimated results between 1-3 m which is in the acceptance levels of accuracy of a wireless RSS positioning system. But why the other databases have estimated results with higher accuracy from the random angle database? The answer is in the question. The random angle database from two laptops has a random value for all its RSS samples collected during the fingerprint database and so it absorbs positive but also negative effects from the environment. So the relation between a random and a constant angle is that a constant angle fingerprint database can produce highest accurate results in terms of coordinate precision but also and the other way around, instead of a random angle database which its rests are always in the average acceptance accuracy levels. Finally from the average all angles database has the same distance error as angle 145 database and better from the other two. That means that in a future real physical implementation of this system angle 145 can be consider as the best alternative from the random angle database and from the all angle database scenario.

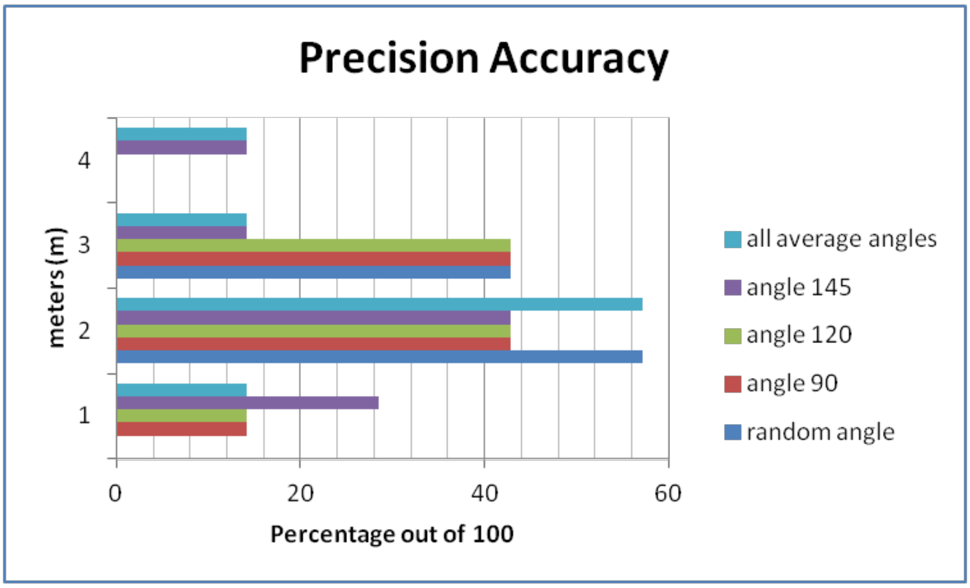

Figure 21: Final Precision Accuracy Percentages

Chapter 5 Conclusions and Future work

5.1 Conclusions and goals achieved

In the thesis, a brief description of the different kinds of positioning technologies was introduced. Next the new era of Location Based Services is mentioned and also a detailed report on the multiple different indoor wireless factors is presented and their impact on RSSI signaling. The system has been developed using the positioning technology called fingerprint, which is a pure RSSI dependant technology. The SNN (Search by Nearest Neighbor) algorithm has been chosen to be implemented in this system due to the relative easy implementation but most important due to the fact that these kinds of systems do not need any extra configuration and hardware to the designated area thus appoints them as a cost effective solution. Also another advantage of the SNN algorithm is that it produces fairly good results within an acceptances level of distance error. The primary goal of this thesis was to create an application that can estimate the location of a mobile node in terms of a Cartesian product in indoor environments with the innovation that positioning is taking place in the area of interest without the user have any idea that is been tracked down.. The challenge was to achieve a sub-room level accuracy of less than 3 meters. As a secondary goal was to develop the system by using open source tools on Windows network environment and also to be developed in such a way that the system will make use the existence wireless infrastructure. The second goal set appoints the system to be a cost effective solution for indoor wireless positioning because in order to be operational the only hardware needed it a minimum number of three access points that are able to run the specific firmware mentioned. The final goal of this thesis was to get a glimpse of the unstable, unpredictable world of indoor RSSI signaling. This final goal was achieved by conducting different experiments detailed mentioned in section 4 where those experiments were mainly base on the construction of the fingerprint database by changing and comparing the different laptop angles and their impact on the final estimated location results.

Through the observations on signal strength features, all the positioning experiments and results comparison the following conclusions can be derive:

1. First of all by comparing all estimated results in section 4, the section which has the highest distance error rate is section 4.2 were the fingerprint database were built by collecting RSS samples in many reference points close to each other. So is safe to assume that a fingerprint database of this kind will fail in any implementation. The correct first step when deciding to build a fingerprint database is to choose reference points in a grid manner way which they have at least a different of 3 meters between them in all directions. The consequence of this action is to have a scattered radio map that can reflect the RSS indoor changes on the actual values. In this thesis this was not possible due to the limited space but the reference points were quite apart from each other as possible.
2. A second conclusion derives from section 4.3 were two fingerprint databases were build. The one was build using only RSS sample from one laptop and the other from the average RSS values from two laptops but in both the angle of the laptop was random in all time. The comparison between them shows that if the algorithm uses the second database with the average RSS samples has less average distance error and hence estimates better results in terms of accuracy precision as shown in table 6 in section 4.3. So as a second step when building the fingerprint database is wise to use more than two mobile terminals RSS signals.
3. Based on the second conclusion that by increasing the number of mobile terminals during the fingerprint phase it is logically correct to assume that increasing the

number of access points in both offline and online phase will increase the system accuracy.

4. The final conclusion investigates the relationship and the impact between the different angles in which a laptop screen can be and how these angles affect the receiving RSS in terms of power and value. By comparing the estimated results not only between the three different angles and the average one derived from them but also with the results from the database built in section 4.3 is clear that database with RSS measurements only from the 145 angle has the minimum average distance error at 1.80 m. This number applies only for the current samples estimated but in general a rule that can be derived from section 4.4 is that if the database is built using a constant laptop angle the algorithm will produce higher accuracy. In this thesis it seems that angle 145 is the best scenario to go with it for future implementations. Also the different charts in section 4.4 show how much the RSS signals values change by slightly changing the angle of a laptop. This come to contribute to the negative unstable indoor wireless environment that pure RSS positioning systems rely on.
5. Finally the previous conclusions can be used as recommendations when building such a system but at the end they all come down to the future owner of the system. Meaning if the future owner chooses to use more than two mobile terminals in the offline phase , more access points and decide to investigate which angle produce more accurate results in the designated area then the system can be too expensive in terms of money and time consuming to be deploy.

5.2 Future work

The indoor wireless Positioning system developed, works well on to locate mobile devices which are temporarily static, and the positioning accuracy is less than three meters and sometimes even under two meters. There are several problems that still need to be further explored in order to improve the system positioning and tracking ability. They are listed as follow:

1. Examine other tools or built one from scratch that can replace Wiviz because most of the times when the system is in tracking mode Wiviz fail to find the client that is been tracked down and so tracking stops. The new tools will have the ability to automatically scan the area and send the results to the server when needed by the system without the use of intermediaries programs and thus reducing the tracking and positioning function and operation.
2. Almost all wireless devices are equipped with Bluetooth chips. A future scenario can be to examine the uses of both RSS and Bluetooth in order to achieve higher accuracy. Wireless access points can be equip with Bluetooth scanners and when a client is been tracked down the Bluetooth can be use to determine in which room is the user if the RSS system estimates that is close to the boundaries of two rooms.
3. Another crucial point that was not investigated in this thesis is the algorithm itself. This algorithm, has a running time of $O(Nd)$ where N is the cardinality of S meaning the number of elements in set S and d is the dimensionality of M (metric space). In order to reduce the running time of this algorithm with one solution is to compare the live RSS sample against the ones in the database and then the algorithm could divide

the samples in *k* value clusters and then apply the calculations only to the clusters that are only closest (best match) to the live RSS taken from the mobile terminal. With this approach the running time of the algorithm will be $O((N/k)\ d)$ but an extra time complexity will be added when comparing against all samples in order to do the clustering process. Another possible way to reduce the best match comparison is to use the Bluetooth scanners on the access points. Due to the fact that Bluetooth operates up until two meters if a client is in the Bluetooth range of an access point then the algorithm could pick up those samples which will have an identification id that are within that range and apply the calculations only to them.

References

1. Bensky Alan, *Wireless Positioning Technologies and Applications*, Boston, Artech House, Jan. 2008, ISBN-13: 978-1-59693-130-5.

2. Dik Lun, Lee Manli and Zhu Haibo Hu, "When Location-Based Services Meet Databases"; www.cs.ust.hk/~dlee/Papers/mobile/mis-invited-05.pdf

3. Diep Dao, Rizos Chris and Jinling Wang, "Location-Based Services: Technical and Business Issues"; www.gmat.unsw.edu.au/snap/publications/dao_etal2002a.pdf

4. B. Kolmel, "Location based services," in *Proceedings of Workshop Mobile Commerce*, 2003, pp. 88-101.

5. Varshavsky Alex, Pankratov Denis, Krumm John and Lara de Eyal, "Calibration-free Localization using Relative Distance Estimations" 2008, ;www.research.microsoft.com/ ~jckrumm/ Publications %20 2008/ calibree.pdf

6. M. Djuknic Goran and E. Richton Robert, "Geolocation and Assisted GPS", Feb.2001, Bell Laboratories; http://www.cens.ucla.edu/~mhr/cs219/location/djunkic01.pdf

7. Brethour, V., ''Ranging with Draft 2,'' IEEE P802.15 Working Group for Wireless Personal Area Networks (WPAN), Doc.IEEE 15-06-0242-00-004a, May 15, 2006

8. Marko Helén , Juha Latvala , Hannu Ikonen and Jarkko Niittylahti, "Using Calibration in RSSI- based Location Tracking System", CiteSeerX, March, 2005; http://130.203.133.150/viewdoc/summary?doi=10.1.1.161.3429

9. Grossmann, U.1 Gansemer and S.1 Suttorp, O. , "RSSI-based WLAN indoor positioning used within a digital museum guide" International Journal of Computing , 2008, Vol. 7, Issue 2, p. 66-72.

10. Zhen Fang, Zhan Zhao, Xunxue Cui, Daoqu Geng, Lidong Du and Cheng Pang, " Localization inWireless Sensor Networks with Known Coordinate Database ", Hindawi Publishing Corporation EURASIP Journal onWireless Communications and Networking, Volume 2010, Article ID 901283; http://www.hindawi.com/journals/wcn/2010/901283/

11. Kurt Derr and Milos Manic, "Wireless Indoor Location Estimation Based on Neural Network RSS Signature Recognition (LENSR)", *3rd IEEE Conference on Industrial Electronics and Applications*, 2008 Jun 01.

12. Quang Tran, Juki Wirawan Tantra, Chuan Heng Foh, Ah-Hwee Tan, Kin Choong Yow, "Wireless Indoor Positioning System with Enhanced Nearest Neighbors in Signal Space Algorithm", IEEE Xplore, 25-28 Sept. 2006; http://ieeexplore.ieee.org/ xpl/ freeabs.all . jsp?arnumber=4109754

13. Atreyi Bose and Chuan Heng Foh, "A practical path loss model for indoor WiFi positioning enhancement ", IEEE Xplore, 10-13 Dec. 2007; http://ieeexplore.ieee.org/ xpl/freeabs_all.jsp?arnumber=4449717

14. Yu-Tso Chen, Chi-Lu Yang, Yeim-Kuan Chang and Chih-Ping Chu, "A RSSI-based Algorithm for Indoor Localization Using ZigBee in Wireless Sensor Network", Jun 2009, http://www.csie.isu.edu.tw/homepage/ccchen/IJSEKE-2011.pdf.

15. Abdalkarim Awad, Thorsten Frunzke, and Falko Dressler, "Adaptive Distance Estimation and Localization in WSN using RSSI Measures ", IEEE Xplore, 29-31 Aug. 2007 ; http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4341511

16. Giovanni Zanca, Francesco Zorzi, Andrea Zanella and Michele Zorzi," Experimental comparison of RSSI-based localization algorithms for indoor wireless sensor networks", Apr 2008, http://www.techrepublic.com/whitepapers/experimental-comparison-of-rssi-based-localization-algorithms-for-indoor-wireless-sensor-networks/3718875

17. Ambili Thottam Parameswaran, Mohammad Iftekhar Husain and Shambhu Upadhyaya, "Is RSSI a Reliable Parameter in Sensor Localization Algorithms – An Experimental Study", 2009; www.cse.buffalo.edu/srds2009/F2DA/f2da09_RSSI_Parameswaran.pdf

18. Hirokazu Miura, Kazuhiko Hirano, Noriyuki Matsuda, Hirokazu Taki, Norihiro Abe and Satoshi Hori, "Indoor Localization for Mobile Node Based on RSSI", 2007**,** http://www .springerlink.com/content/b1544k768lp12364/

19. Jefrey Hightower and Gaetano Borriello, "Location Sensing Techniques", 2001; http:// portolano.cs.washington.edu/papers/UW-CSE-01-07-01.pdf

20. Feifei Guo, Chunkai Zhang, Min Wang and Xiaofei Xu, "RESEARCH OF INDOOR LOCATIONMETHOD BASED ON THE RFID TECHNOLOGY", Atlantis Press; www.atlantis-press.com/php/download_paper.php?id=1769

21. Jie Chen, "RSSI-based Indoor Mobile Localization in Wireless Sensor Network", International Journal of Digital Content Technology and its Applications,Volume 5, Number 7, July 2011

22. Erin-Ee-Lin Lau, Boon-Giin Lee, Seung-Chul Lee and Wan-Young Chung, International journal on smart sensing and intelligent systems, vol. 1, no. 2, June 2008

23. Uwe Grossmann, Markus Schauch and Syuzanna Hakobyan, "RSSI based WLAN Indoor Positioning with Personal Digital Assistants", IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 6-8 September 2007, Dortmund, Germany

24. Lu´ıs Felipe M. de Moraes and Bruno Astuto A. Nunes, "Calibration-free WLAN location system based on dynamic mapping of signal strength", 2006; http://www.techrepublic.com/whitepapers/calibration-free-wlan-location-system-based-on-dynamic-mapping-of-signal-strength/3675949

25. Eduardo Navarro, Benjamin Peuker and Michael Quan, "Wi-Fi Localization Using RSSI Fingerprinting", 2010, http://digitalcommons.calpoly.edu/cpesp/17/

26. R, Mardeni Othman and Shaifull Nizam, "Node Positioning in ZigBee Network Using Trilateration Method Based on the Received Signal Strength Indicator (RSSI)", European Journal of Scientific Research, 2010,ISSN 1450-216X Vol.46 No.1, pp.048-061

27. Luis Peneda, Abílio Azenha and Adriano Carvalho, “Indoors Localization Using Mobile Communications Radio Signal Strength”, InTech, February 2011, http://www. intechopen.com/articles/show/title/indoors-localization-using-mobile-communications-radio-signal-strength

Appendices

Notes:

In this thesis as mention earlier two free firmwares are installed on the routers due to their capability to run the Wiviz tool. DD-WRT is running Wiviz ver.1 and OpenWrt is running Wiviz ver.1. The core and the scanning capabilities for both tools are the same. The only differences between them is that version 2 of the program has more graphics and also gives more network details for clients and access points scanned that are unnecessary for this project. Although due to some major differences that the two versions have like the running time that the tool needs or the time to transfer the results from the routers locally two systems have been developed each one working respectively with DD-WRT and OpenWrt.

During the testing periods the system developed for running along side with DD-WRT presented much stability issues. For example when the user issue a command to scan the area of interest through the browser mode or while working in browser mode for much time many times the Wiviz tool suffered from crashes instances. Also Wiviz ver.1 takes less time to load and to scan and also less time to transfer the results from the router locally. Generally speaking the experiments with the setup of OpenWrt and Wiviz ver.1 proved to be more stable and faster than DD-WRT and Wiviz ver.2.

Installation Guide:

In order for the system to be operational the installation must be done as follow:

1. First download and install Microsoft SQL Express 2008 version on the server that is going to run the system. During installation configure the sever to accept only SQL Server Authentication (username, password) for security enforcement reasons and after the installation has finished create three different databases. The databases can be called anything but its best to be called angle90, angle120 and angle145 in order to reflect their purpose.
2. Make sure that three and more access points exist in the wireless infrastructure running DD-WRT with Wiviz ver.2 or OpenWrt with Wiviz ver.1. The access point should be password protected and the server should be cable of accessing them wired or wireless.
3. Then just install the setup executable and following the system sequence for proper operation. First build the fingerprint database and then run the positioning functions.
4. If the setup way of installation is not desirable then proceed from this step and below for a manually execution of the system. Steps 1 and 2 remain the same.
5. In the zip file there are two folders name Netcat and Putty. Copy and paste them in C directory.
6. Download the source code folder locally, run VB.NET with ADMINISTRATIVE PRIVILEGES on win7 and vista and run the program.
7. Inside the Netcat folder there is a subfolder name pic. Place the map of the area of the interest and name it map.jpg for example. This will help not load the area map each time the system runs. Be careful about the x and y axis of the map. The initial

point of the map (0, 0) must on the top left corner of your map. See figure13 at page 62.

8. If OpenWrt is chosen over DD-WRT then the administrator must run and login to each router with Putty manually at least one time before running the program because the SSH key generate by Putty must be added to the registry of the local server manually.
9. For both firmware's it's better to run Wiviz at least once for all routers from telnet or ssh in order to create the configuration file before running the system.
10. Also Netcat (nc) must be added to the exception list of Windows firewall and antivirus installed locally in order for the routers to be able to open a communication channel between the local host and them.
11. Then just run the system, enter the details and start using it.