TECHNICAL UNIVERSITY OF CRETE
ELECTRONIC AND COMPUTER ENGINEERING DEPARTMENT
TELECOMMUNICATIONS DIVISION

Community RF Sensing

by

Emmanouil Alibertis

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DIPLOMA DEGREE OF

ELECTRONIC AND COMPUTER ENGINEERING

October 2012

THESIS COMMITTEE

Assistant Professor Aggelos Bletsas, *Thesis Supervisor*
Professor Minos Garofalakis
Assistant Professor Michail G. Lagoudakis

Abstract

Cellular mobile telephony (GSM or newer UMTS) is currently used by over 4 billions users, indicating great success of the relevant technologies. The received signal power levels at each geographical region are very important since they define the quality of service. Thus, received signal strength (RSS) recording networks have emerged the last few years, such as those in the Hermes or Android's openSignalMaps projects. However, Hermes project deploys measuring stations at fixed locations only and records the whole RF band, while OpenSignalMaps does not include recordings of user transmission power levels or other important details.

This thesis develops community RF sensing using as sensors the mobile phones of users; cellular telephony coverage maps are created by user measurements with the iPhone (3G, 3Gs, 4G) platform. A community geographical information system (GIS) is implemented, consisting of the MySignals iPhone application running at each participating user, a central MySQL database (DB) and a website that displays the acquired coverage maps. A real world evaluation was performed with seven iPhone users for the city of Chania. Over 40000 RSS measurements have been collected within 3 weeks in an automated and user-transparent way. A time/space analysis was performed demonstrating the RSS variance over time and discovering particular areas with very poor signal. Finally, an introduction to cell towers position discovery was also considered, by careful application of particle filtering. The system is designed to support a large number of user-sensors and could assist in city-wide evaluations of existing cellular telephony network deployments.

Thesis Supervisor: Assistant Professor Aggelos Bletsas

Acknowledgements

There are so many people who supported and encouraged me at all aspects throughout this work and during the writing of this thesis and i want to thank them all from the bottom of my heart. Everybody helped me some way for completing this thesis:

Firsty, I would like to express my gradidute to Dr. Aggelos Bletsas, for the assignment of this thesis and his encouregment, support and guidelines during the implementation and writing of this thesis. He is a big source of motivation for hard work and for implementing as much as possible real world telecommunications and software applications. Also his philosophy, that an engineer must combine theory with real world implementations from all the electronic and computer engineering sectors, has inspired me.

My little sister, "Sofoula" (yeah, she is older but it does not matter). She supported me in all possible ways in writing of this thesis and preparing the presentation of this work. Thank you "Sofoula" for your vital help, support and mostly for calming me down.

Next, my best friends, Nikos Kofinas (aka. Kofi) and Nikos Pavlakis! I was always chatting with them all of my problems in the implementation of this project, which was very helpful for me! Guys you are really great company, thank you for everything!

D. Iliou and Nikos Pavlakis (yes he earned a second mention) for their important corrections!

To sum up, i would like to thanks all my friends here in Chania for the six amazing years that we have spent here: N. Kofinas, N. Pavlakis. E. Soulas, I. Perros, G. Liagouras, G. Krokos, K. Tsichlis, V.Soultis and J. Iliou.

Of course MySignals beta testers (K. Tsichlis, G. Krokos, E. Kampinakis, J. Kimionis, Thodoris, A. Varouranakis, J. Iliou) who without them i could

not evaluate in practice my work! I really thank you guys for draining your battery in order to collect measurements and testing my work!

Finally, i would like to thanks my parents for their deepest love and support in all stages of my life...

Table of Contents

List of Figures

List of Tables

List of Abbreviations

GSM	Global System for Mobile
GPRS	General Packet Radio Service
UMTS	Universal Mobile Telecommunications System
2G	*Second* Generation of Cellular Telephony etc
BTS	Base Transceiver Station (*aka Cell Tower Site*)
RSS	Received Signal Strength
RF	Radio Frequency
ICNIRP	International Commission on Non-Ionizing Radiation Protection
RAT	Radio Access Technology
QoS	Quality of Service
E/M	Electromagnetic
RSSI	Received Signal Strength Indicator
Rx	Receive
Tx	Transmit
GIS	Geographical Information System
SDK	Software Development Kit
API	Application Programming Interface
GUI	Graphical User Interface
MS	Mobile Station
BSC	Base Station Controller
MSC	Mobile Switching Centre
LAC	Location Area Code
UTRAN	Universal Terrestrial Radio Access Network
AMPS	Advanced Mobile Phone System
FDMA	Frequency Division Multiple Access
D-AMPS	AMPS digital evolution

ETSI	European Telecommunications Standards Institute
TDMA	Time Division Multiple Access
SMS	Short Message Service
EDGE	Enhanced Data-rates for Global Evolution
ARFCN	Absolute Radio Frequency Channel Number
MSK	Minimum Shift Keying
GMSK	Gaussian Minimum-Shift Keying (*GSM Modulation*)
PSK	Phase Shift Keying
IS-95	Interim Standard 95
CDMA	Code Division Multiple Access
DSSS	Direct-Sequence Spread Spectrum
3GPP	3rd Generation Partnership Project
IMT-2000	Internet Mobile Communication 2000
W-CDMA	Wideband Code Division Multiple Access (*UMTS Modulation*)
iOS	iPhone Operating System
CGI	Cell Global Identifier
ASU	Arbitrary Strength Unit
BCCH	Broadcast Control CHannel
MCC	Mobile Country Code
MNC	Mobile Network Code
IDE	Integrated Development Environment
JSON	JavaScript Object Notation
PLMN	Public Land Mobile Network
BSS	Base Station Subsystem
GMSC	Gateway Mobile Switching Centre
NSS	Network Switching Subsystem
BSIC	Base Station Identity Code
RR	Radio Resource
TXPWR	Transmit Power

IDE	Integrated Development Enviroment
FIFO	First In First Out
MVC	Model View Controller
KVO	Key Value Observing
LAI	Location Area Identity
PFs	Particle Filters
DBN	Dynamic Bayesian Network
PDF	Probability Density Function

Chapter 1

Introduction

1.1 Domain and Motivation

1.1.1 Everyone uses a mobile phone, only a few understand the Transmit Power Problem

The cell phone was invented in 1991 when the GSM (Global System for Mobile) was introduced in Europe providing the first digital mobile telecommunication network [1]. Since then the mobile phone penetration rate [i] was increased rapidly. According to [2] there are approximately six billion mobile phones worldwide. However, the actual number of cellular telephony subscribers is estimated roughly to 4.1 billion because many subscribers posses more than one cell phone. This data, without doubt, demonstrate that mobile cellular telephony represents the most successful technological product ever made.

Furthermore the last few years the capabilities and the offering features of mobiles phones have increased dramatically resulting in their evolution to smartphones. At the same time mobile cellular networks have been upgraded to GPRS (2.5G) or UMTS(3G) since 2000, in order to provide mobile Internet access. Smartphones are not only used for phone calls, as the first "dumb" cell phones, but also for mobile computing, Internet surfing, listening to music, reading news, entertainment and more. Typically a smartphone is a fully equipped hand-held computer device with a touchscreen. Therefore the "modern" cell phone plays essential role in any aspect of every day life providing the personal digital assistant and communicator which everybody

[i] Mobile phone penetration rate is a term generally used to describe the number of active mobile phone numbers (usually as a percentage) within a specific population. [3]

Figure 1.1: Various generations of mobile phones.

has. In Figure 1.1, representative cell phones and smartphones are shown.

In Greece, the mobile penetration rate is 139% which is translated into 15.25 million subscriptions [4]. Although almost everyone in Greece owns a cell phone, only a minority understands the basic parameters of mobile phones operation. It is a common phenomenon for residents to complain about the "enormous" electromagnetic radiation emitted from cellular telephony antennas. In addition, many people believe that Cell Towers cause cancer. At the same time these users make a phone call without using a bluetooth handset or a hands-free and therefore the mobile phone transmits

Figure 1.2: BTS site in town, Tzanakaki Str, Chania Crete, Greece (Source: www.eeae.gr)

electromagnetic waves exactly next to their head. At this point, it must be underlined that even close to a Base Station Transceiver (BTS) -that is (i.e.), a Cell Tower Antenna- the received power of electromagnetic waves from the base station is millions of times smaller than the power of the transmitted signal from the mobile phone. Besides, the electromagnetic waves attenuate proportionally to the square of distance between transmitter and receiver. In Figure 1.2 a typical BTS example installed inside a town is shown.

A simple arithmetic example indicates the truth. Even close to a Cell Towe, for example (e.g.), at 50m, the received signal strength (RSS) is around -50dBm [i]. The mobile phone usually transmits around 30 dBm or even higher if a Cell Tower cannot be easily reached. Most importantly, the difference of 70 dBm means that mobile phone transmits seven million times higher power than the received signal from the Cell Tower Antenna. Definitely the

[i] $y(dBm) = 10\log_{10}(z/1mW)$

possible issues in human health from Radio Frequency (RF) radiation are due to mobile phones, not to the Cell Tower Antennas. Consequently, if the Cell Tower's Network become more dense, the transmission power of the mobile phones will be lower, because it is easier to reach a Cell Tower when the distance becomes shorter. Hence possible effects in human's health will be minimized. However, this assumption is valid only if the emitted electromagnetic radiation from a BTS remains under the safety limits. These limits are defined by the European Commision Recommendation 1999/519/EC, the Hellenic Republic Law no. 3431/2006 and 4070/2012 reference levels. Further information about non ionizing Radio Frequency [i] exposure and protection can be found in ICNIRP [ii] Review [5]. The observance of safety limits in Greece is operated by the Greek Atomic Energy Commission (GAEC) [6].

A phone call can be served and mobile Internet can be accessed only if the RSS is above a certain level. This level is dependent on Radio Access Technology (RAT) and the QoS (Quality of Service) requirements. In general, for any type of network, if the RSS is higher than -100dBm the mobile network can be accessed satisfactorily from the cell phone. Therefore the cellular network coverage and performance in a particular region are determined from the RSS in this region. In order to achieve better RSS, the Cellular Tower's network should become more dense. Subsequently, this improvement of RSS would result in much better mobile services and lower emitted power from mobile phones as mentioned above. Unfortunately users, as it is has already been discussed, cannot understand how important it is to have good RSS for both their health and for the quality of mobile services. This fact was a very strong source of motivation for this thesis.

1.1.2 Hermes, Signal's Quality Recording Network

The RSS from a mobile cellular network -i.e., received signal power- in a fixed location may differ from time to time. It may be affected by scattering, reflections, thermal noise in electronics, changes in the environment

[i] Non-ionizing Electromagnetic Radiation extends from 1 Hz to 300GHz [5]
[ii] International Commission on Non-Ionizing Radiation Protection

reader.png

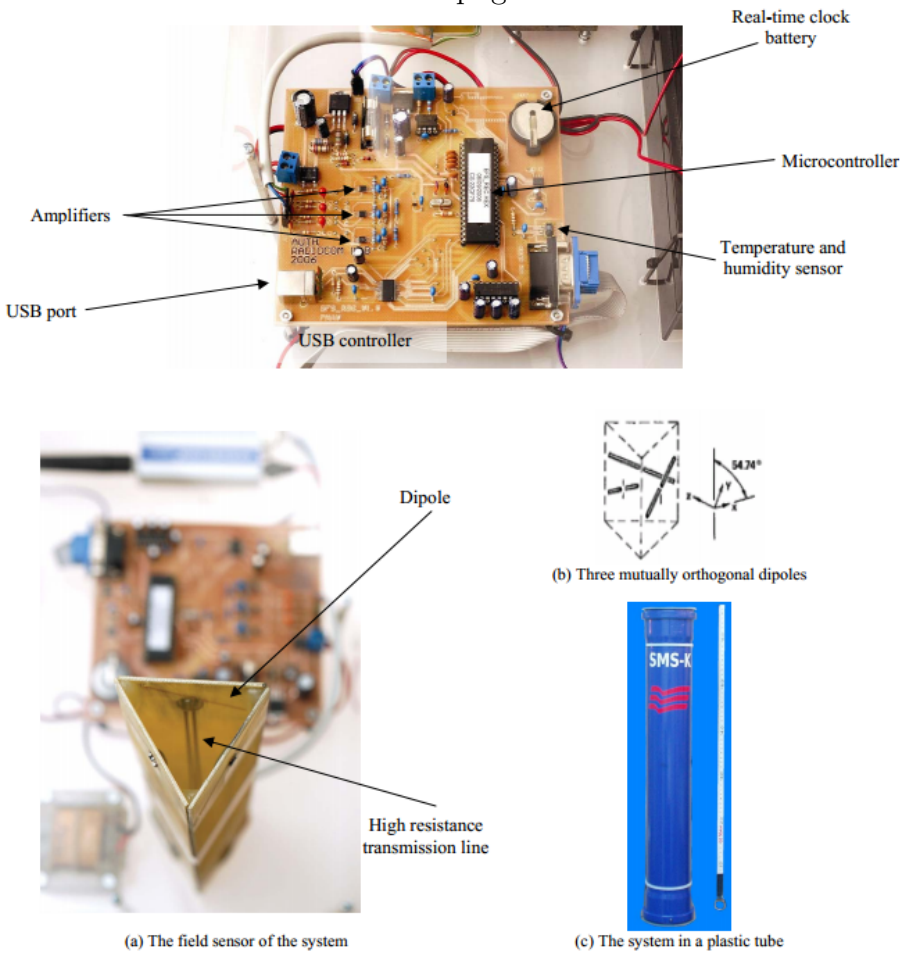

Figure 1.3: A scientific,wide band RF Reader, called SMS-K [7]

or, additionally, by BTS's trasnmitted power which is not constant (BTS transmitted power is dependent on network's status). Therefore the received signal strength cannot be modelled (estimated) satisfactorily.

On the other hand, the cellular mobile telephony coverage -i.e., the RSS level per region- is very important parameter which any carrier and user would like to know, for the following reasons:

- The best network carrier for the user can be chosen.
- The cellular network coverage, performance and range can be deter-

mined.

- Service's evaluation per region can be done. If e.g. mobile Internet is needed by users, the signal's quality would be checked at workplace or home.
- Specific regions with poor signal can be discovered. This data is vital for network carriers in order to do a better network planning and probably add new Cell Towers.
- Network upgrades can be scheduled. For example, if a detailed mobile coverage map is available, network carrier can determine where 2G signal is available but 3G does not.

Based on the reasons discussed above, RSS cannot be known a priori for a specific area unless it is measured with a scientific RF reader/analyser [7], [8], [9] (example in Figure 1.3). In other words the cellular network's RSS is determined only experimentally. Moreover safety limits for the non ionizing RF radiation emitted by BTS must be applied, thus a recording network structure for RSS measuring, is necessary.

Hermes project [10], [11], which is operated by the National Technical University of Athens (NTUA) and the Aristotle University of Thessaloniki (AUTH), implements an innovative system for the continuous monitoring of the non-ionizing electromagnetic (E/M) radiation at radio frequencies emitted to the environment by various sources, as previously mentioned, such as radio and television station transmitting antennas, mobile telephony antennas, radars etc. Hermes project has many fixed measuring stations which observe E/M radiation levels at radio frequencies. Examples of such measuring stations are shown in Figure 1.5. Also a car, called Hermes Mobile (see Figure 1.4), has appropriate equipment and readers which measures E/M radiation levels while driving (on the streets).

Data for the signal quality of cellular telephony can be provided by Hermes project only for some specific measuring stations at fixed locations. Also

Figure 1.4: Hermes Mobile car (Source: hermes.physics.auth.gr)

Figure 1.5: Hermes Project, measuring stations of non ionizing RF spectrum (Source: www.hermes-program.gr)

a single wardriving car [i] cannot cover the whole country. In addition, Hermes stations measure E/M radiation levels for a large range of non ionizing RF Spectrum. Considering that the same cellular Frequency Band is used by many companies, rss per network carrier cannot be obtained. Hence Hermes Project is not capable enough to give detailed RSS measurements, for constructing a mobile coverage map, neither covering whole geographical areas.

This thesis concentrates on providing a different and smarter way to measure cellular network signal quality per region, network type and network carrier. In contrast to Hermes project, this thesis monitors only the cellular

[i] A car which is equipped with RSS reader and collects rss measurements while driving. Thus rss stamps for the streets of a town can be consolidated

telephony Frequency Bands. A mobile coverage map can be constructed with deeper resolution, scalability and flexibility for RSS readings by user mobiles themselves.

1.1.3 Exploit Smartphone Capabilities of recording Signal Quality

How can a RSS-reading network be implemented? The answer is extremely simple. The RSS readings can be obtained from the mobile phone itself, since the mobile phone calculates an estimation of the RSS. This is called Receive Signal Strength *Indicator* (RSSI) and it is implemented by the hardware of the mobile. More specifically, RSSI is an estimation of the actual received signal power, whose calculation, as mentioned above, may be affected by several parameters such as thermal noise. Therefore, since many Cell Towers are usually available in a region, RSSI is used by the cell phone in order to select the best available. Also, RSSI is being displayed intuitively on the mobiles as the well known five bars and indicates the quality of the mobile services to the users.

The evolution of the cell phone to a fully equipped handheld computer device gives the opportunity to create an RF Sensing Community -i.e. a community of mobile phones which records RSSIs relative to the location where they are observed. Smartphones are equipped with GPS (Geographical Position System), high capacity flash disks and powerful SDKs(Software Development Kits). In addition, various sensors such as accelerometers, gyroscopes, proximity sensors etc. are built-in in smarthphones. All this stuff is packed into excellent mobile operating Systems such as Google's Android and Apple's iOS. Great opportunities for application development are provided by the combination of the above software and hardware. This thesis exploits all these capabilities and features of smartphones for creating a Community of RF Sensing at cellular telephony frequency bands using user mobiles themselves, instead of using a wideband RF reader such as the SMS-K in Figure 1.3, which is installed only in fixed locations.

1.2 Thesis Purpose

1.2.1 Users record signal quality and Mobile Network's Info by region

An RSS recording platform by users themselves, is developed and introduced by this thesis. The main objective of this work is to collect RSS readings to the respective coordinates where they are observed. Apart from RSS readings, cellular network information (such as network type, carrier frequency, identification codes for Cell Towers, neighbouring Cell Towers info, Mobile Carrier Name and many others), is also collected.

A real world Geographical Information System is implemented as part of this thesis. The software platform consists of an iPhone Application [i], a central web server with a database and a web site for displaying mobile coverage. The iPhone App, which is named "MySignals" reads and saves:

- The Received (Rx) power -i.e., RSSI.
- The transmitted (Tx) power.
- Cellular network information (eg. carrier frequency etc).
- The location of the iPhone.

All this data is forwarded to a central server and is saved in a MySQL Database. Finally the mobile coverage is displayed to a Geographical Information System (GIS). More specifically mobile coverage is the intuitive result of collected RSSI data. Mobile coverage is displayed through a heatmap. Thus the cellular network rss, information and mobile coverage per geographical region, can be monitored by the users themselves.

1.2.2 Why the iPhone has been chosen

Apple's iPhone was chosen as the platform to implement this project for several reasons. First of all, the iPhone is the most popular smartphone in

[i] Also known as (aka) "App"

the world [i]. Iphone users are always excited with their new device [ii] to the point of addiction [12]. Also, iPhone's usage satisfaction rate is extremely high [13]. Many of the iPhone users are electronic and computer engineers, or maintain a similar degree (e.g. Computer Science or Technical University departments). Therefore the iPhone App would be used more easily by this user category. The adoption of the application is essential in order to collect as many RSS readings and cellular network data as possible.

Secondly, iPhone's official SDK and APIs (Application Programming Interfaces) do not provide access to RSSI neither to cellular network information (which is necessary for creating the coverage maps). Those features are completely locked and hidden in iPhone's platform. Definitely, bypassing Apple's software locks and restrictions and creating an application that did not exist (then), was a great challenge. In general, Apple's policy is very strict. Only applications from Apple's App Store are allowed to be installed on the iPhone. Many applications are rejected by Apple for using private APIs-i.e, APIs available only to Apple and not to other developers.

To the best of our knowledge, this thesis provides the first community RF sensing in iPhone platform, for creating mobile coverage maps by users themselves. During the development of this thesis, the Android application OpenSignalMaps was released, a project which is very close to what was considered to be MySignals. It was a great challenge to create such an important platform (as the development of mobile coverage maps by users themselves) for iPhone, the best and most popular smartphone in the world.

1.3 Thesis Contribution

This thesis contributes to several aspects of the Telecommunication field and cellular mobile networks as it introduces an Informational platform for the users. It must be underlined that both an engineering tool and scientific applications are combined in this thesis.

[i] Approximately 250 million iPhones have been sold since 2007 according to Apple's financial reports.

[ii] Over 2 millions pre-orders in 24 hours for iPhone 5 [14]

1.3.1 A Scientific, Engineering and Research Tool

The whole software platform is a complete monitoring and observing tool for Cellular Network signal reception, quality and coverage. All these parameters of cellular mobile networks can be observed by network carriers or telecommunication engineers. MySignals App can be used not only by users (e.g. choose the best available carrier as mentioned) but also by cellular network and telecommunication engineers. Technical information and details (e.g. serving cell, neighbouring cells etc) for Cellular network can be obtained and monitored by the App. Therefore, MySignals can be used by engineers for network maintenance and for analysing network behaviour. Additionally, collected data from this project can be used for extended research applications such as developing localization algorithms for Cell Tower Antennas, mobile phone localization without the use of the gps, analysing RSS performance over space and time, algorithms for frequency allocation to BTS and much more.

1.3.2 Social, Informational and Educational Tool

Smartphones, mobile phones and Cellular Telephony constitute nowadays an essential component of everyday life and business. In our society mobile phone and smartphone usage has become a lifestyle, thus the understanding of cellular telephonys basic concepts is very important. Therefore, every individual should understand the need of a more dense Cell Tower Network and this shapes the social contribution of this thesis.

Furthermore, as it is discussed, MySignals introduces an Informational platform for cellular telephony. The best network carrier in user's region can be chosen and poor signal regions can be discovered. The educational contribution is focused on explaining the basic cellular telephony parameters, information and concepts inside the iPhone App.

1.4 Related Work

Several solutions for mobile coverage maps and cellular networks monitoring platforms have been developed since smartphones were introduced on the market.

Signal (iPhone App, Cydia Store)
The Signal App [16] was released in August 2010 at Cydia Store, while this thesis was being considered for implementation. Cydia Store is an alternative to Apple's App Store and consists of applications that have been rejected by the App Store. Jailbreaking [i] an iPhone is a prerequisite for accessing the Cydia Store.

Iphone's RSSI, cellular network information and details are provided by Signal. Also Cell Towers are displayed to their estimated position which is provided by a hidden Google API. Signal has been developed by iPhone hacker, Dev Team member [ii], planetbeing (Yiduo David Wang) [15].

Signal App is a paid application at Cydia Store, hence the source code is not publicly available. Also it has a very poor GUI (Graphical User Interface) without a FAQ [iii] screen or any explanation. It is an engineering oriented App. No data and RSS measurements are collected by Signal and the concept of building a mobile coverage map does not exist. Signal App is just an iPhone application and not a complete geographical information system as opposed to MySignals.

OpenSignalMaps (Android Market)
OpenSignalMaps for Android [17] smartphones was released in December 2010 while this work was under development. Since then a lot of features have been added to OpenSignalMaps App and this App belongs to the most popular applications of the Android Store. OpenSignalMaps is very close to

[i] Jailbreak is a procedure to install software that is not allowed by Apple. Jailbreaking methods use software or hardware security issues to bypass Apple's software protection. Then Cydia Store is installed and users have access to thousands of applications and tweaks which are not available in the App Store.
[ii] Dev Team is a hackers community for developing unlocks and jailbreaks for iPhone.
[iii] Frequenty Asked Questions

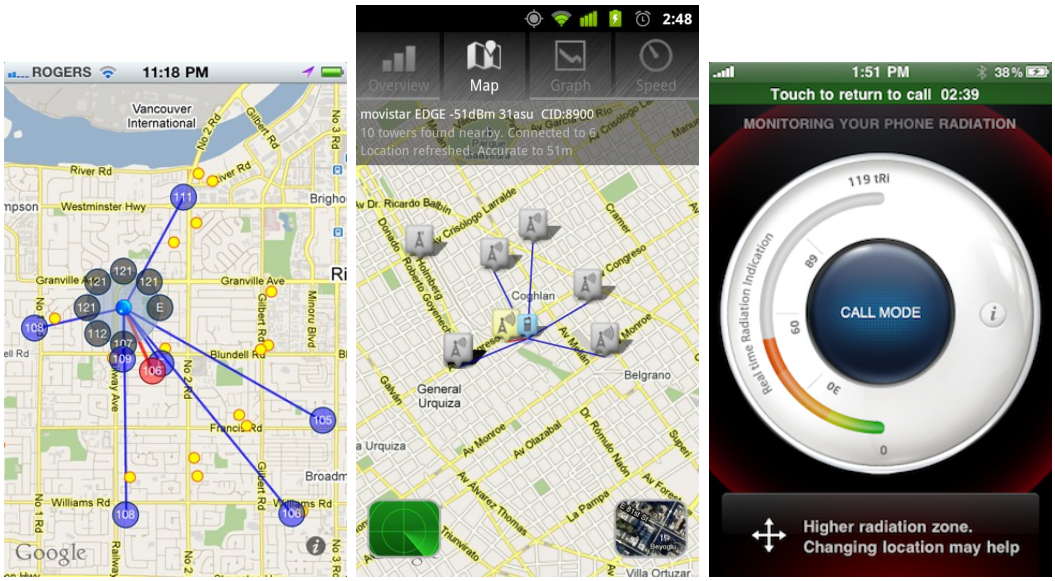

Figure 1.6: i) Signal for iPhone ii) OpenSignalMaps iii) iPhone's Tawkon (Source:redmondpie.com, 1mobile.com, techcrunch.com)

what was considered to be MySignals project. It consists of an Android App which records signal quality and a website which displays a worldwide mobile coverage map which is built by collected RSS from android users. Also, cellular network information and internet connectivity data are displayed on the App. This project has not been ported to the iPhone platform yet. Probably this attempt has been abandoned because of Apple's restrictions.

MySignals has the strong advantage that iPhone is the best smartphone in the world opposing to Android which is fragmented into several smartphones. Also, Android's APIs for RSSI and cellular network info are publicly available to developers as opposed to iPhone APIs. Moreover transmit power data and detailed cellular description (e.g. carrier frequency, RSSI from neighbouring cells etc) are collected in contrast to OpenSignalMaps. Apart from this, MySignals introduces a more detailed coverage map and in contrast to OpenSignalMaps, educational and technical information is been available through the MySignals App.

Other work

Cellumap [18] is another mobile coverage map platform. Cellumap has an extremely simple implementation and is available for Android, Symbian and Blackberry. Certainly, OpenSignalMaps is a much better application than Cellumap. Moreover Cellumap has not been updated since January 2011.

Tawkon app was released for iPhone Cydia store in April 2011 and is also available in Android Market [19]. The aim of Tawkon application is to calculate the emitted radiation level that the user absorbs. In order to achieve that, Tawkon tries to predict iPhone's position relative to the user's body. Definitely it is not oriented to the principles of MySignals App.

Finally, a project called "location-estimation-trials" exists on Android platform [20]. This project aims to evaluate collected RSS data per geographical area.

1.5 Thesis Outline

Chapter 2 describes the basic concepts, principles and structure of Cellular Telephony as well as the basic iPhone software structure and iOS SDK, providing basic background information for this thesis. In Chapter 3 we describe in detail our design and implementation for the whole real world software platform MySignals and the cooperation of the sub-components (iPhone App, Web Server Database and Heatmap). In Chapter 4 the operation of the system with seven real iPhone users is presented and evaluated. Over 35000 measurements (RSSI and their relative cellular network details) have been collected for over three weeks. Also, an analysis on both time and space for the collected measurements has been done. Additionally, a first approach for research application with the collected data is attempted. More specifically, a discovering Cell Tower position scenario using Particle Filters on the collected RSSIs, is considered. In Chapter 5 we summarize the results of this thesis discussing at the same time for future additions and improvements for the whole project. Several directions can be followed for the further development of MySignals as a real world platform. Finally, future research directions, for discovering and Localization scenarios of Cell Tower Positions

using Probabilistic Methods such as Particle Filters, are discussed.

Chapter 2

Introduction to Mobile Telephony

Without a doubt, cellular telephony networks are the most complicated technological structures in the world. Cellular telephony networks and standards (such as GSM, UMTS etc) are described by thousands of specification pages. Hundred of software modules, complicated algorithms, hardware and telecommunication devices, complex protocols, digital signal processing algorithms and various equipment are cooperating in order to make a phone call or to use mobile Internet. That demonstrates that cellular mobile networks and mobile phones are a result of technological convergence. In this chapter basic concepts, structure and principles of cellular mobile telephony are discussed briefly in order to assimilate the domain problem. Basic principles of mobile networks are necessary to understand how cooperative mobile coverage maps can be constructed, as well as to determine which mobile's info is necessary for this thesis.

2.1 Overview and Principles of Cellular Telephony

Cellular telephony is designed to provide wireless communication between a mobile station (MS) and the rest telephony network (another MS or a stationary phone). Internet naturally, has been incorporated by cellular telephony the last few years. In order to achieve communication between MS and the rest telephony network, a radio communication link must me established between the MS and one land unit. This land unit is usually called BTS or Cell Tower. The phone call or the mobile's relatively Internet data will be

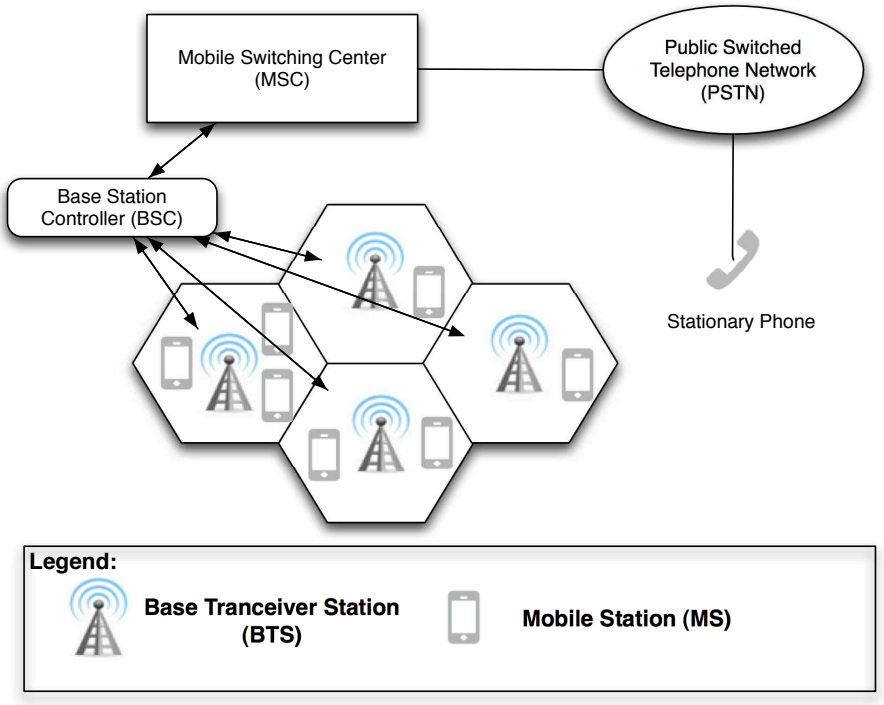

Figure 2.1: A typical Cellular System.

forwarded by BTS to the rest telephony network. The network carrier (or in other words the service provider) must be able to communicate, locate and track the MS. To make this tracking possible, each cellular service area is divided into small regions called *cells*.

In Figure 2.1 the general architecture of a cellular telephony system is demonstrated. The cells are the basic structural unit of mobile telephony. Each cell is served by a BTS and has a unique identifier, cell-id. It is a common practice a BTS -i.e., a Cell Tower- to have several antennas for serving different RATs (e.g. a Cell Tower can combine antennas for both 2G and 3G networks) or even serving more than one cell for the same RAT, splitting an area into sectors and serve each area with a directional antenna (see Figure 2.2) . That indicates that several cell-ids may be served from equipment (antennas) which is installed in the same physical location -i.e. a tower (examples in Figure 2.2 and 1.2).

It is clear that cell size is not constant. Generally the cell size is increasing and decreasing depending on many parameters during the day, such as transmitted power from BTS. The definition of Cell size by engineers is based on traffic demands and the particular geographic area where BTS is established. For example, in rural areas where network load is lighter than a town, a cell may have size of 10Km. In contrast, in urban areas the traffic is higher so the cells are more dense. For example, in a town, the cells have an average size less than 1Km or sometimes picocells with range of a few hundred meters. A particular area may be served from several cells -i.e., several cell-ids are observed by a cell phone. Th e cell-ids which co-exists may serve different frequency bands for the same carrier and by this way the desirable network capacity is achieved. Also cell range is overlapped in many locations by each other in order to ensure that mobile services would be always available.

The BTSs in a particular area are organized into clusters which are called Base Station Controllers (BSCs). Each BTS, whose only function is to transmit and receive data, has a network link with the corresponding BSC, which forwards all network traffic. In other words only physical and mac layer is implemented by a BTS. All the other processes such as frequency allocation, charging, cell handoffs, routing, etc happen on the upper level of BSCs and Mobile Switching Centers (MSCs). As expected, many BSCs are organized into a MSC, which is responsible for the communication with the rest telephony (both mobile and landline) network. MSCs are the heart of the cellular telephony network and handle multiple BSCs, call setup, call routing, handoffs [i] and interfaces with other MSCs. Each MSC it is distinguished from other MSCs with a unique identifier, Location Area Code (LAC).

Another fundamental principle of cellular telephony is the frequency reuse. In general the same frequencies cannot be used by neighbouring cells because it may create interference. However, the available frequency channels (sub-Chapter 2.3.3, 2.4.3) are limited. For this reason, neighbouring cells would not use the same frequencies. In the same time, splitting a cell to sectors with different frequencies, by using directional antennas offers higher capac-

[i] If the receiving signal from a BTS become weak, then the mobile seeks a new cell that can better accommodate the communication. This process is called handoff.

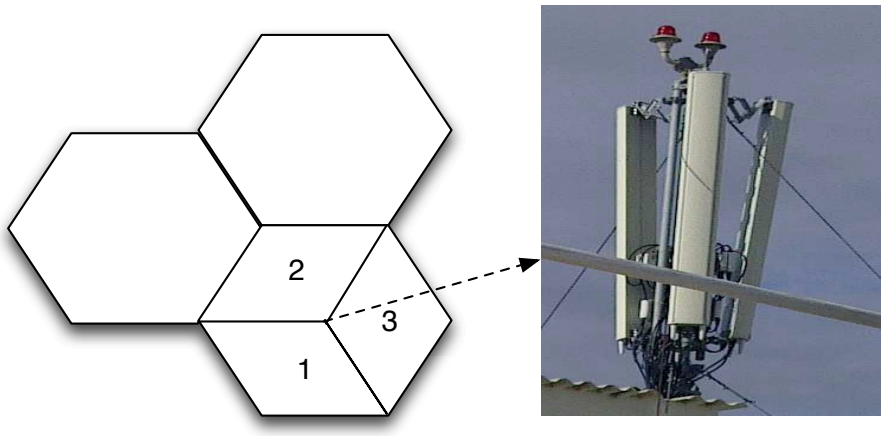

Figure 2.2: A BTS site in a town. Three directional antennas are used for splitting the cell to three sectors. (BTS picture from: www.eeae.gr)

ity. This pattern is used almost everywhere in cellular telephony networks, thus the network equipment in a specific location usually offers many cell-ids as it is explained above. An example is shown in Figure 2.2.

This design pattern and basic logic of cellular telephony applies both on GSM/GPRS/EDGE (2G/2.5G/2.75G) networks and on UMTS (3G) networks although some minor differences exist. The 3G network is also named UTRAN, UMTS Terrestrial Radio Access Network. UTRAN and GSM networks infrastructure shares the same physical location. Network carriers always install equipment and antennas in the same location and cabin for practical reasons. In upper levels of mobile networks the traffic from two networks is consolidated. A comprehensive presentation of GSM and UTRAN (3G) networks details can be found on [21].

2.2 The First Steps of Cellular Telephony

AMPS (Advanced Mobile Phone System) was the first analog cellular telephony system and was introduced (1st generation: 1G) in North America in early 80s [22]. AMPS was operated in ISM 800-MHz band using FDMA,

Frequency Division Multiple Access, for separating this band into channels. The AMPS was never adopted by the rest of the world. Especially with the introduction of GSM in the early 90s AMPS and D-Amps, which was Amps digital evolution, disappeared. Further details are outside the scope of this thesis.

2.3 GSM (2G) - GPRS (2.5G)

GSM was developed by European Telecommunications Standards Institute (ETSI) and released in Europe in 1992 and has adopted. By the year 2010 GSM surpassed 5 billion mobile connections [1]. In [1] can also be found analytical history and timeline of GSM standard. The GSM standard is detailed described and documented in GSM specification [26]. GSM belongs to second generation of cellular telephony (2G). Although originally designed for operation in 900 MHz band [1] it was soon adapted for 1800MHz. The introduction of GSM into North America and the rest of the world meant further adaptation to the 800MHz and 1900MHz bands [23]. Our discussion is focused primarily on Europe, both for 2G and 3G.

2.3.1 Offering Services

GSM was initially designed for voice telephony. Also short messages services (SMS) and circuit-switched data connection up to 9600 bits/sec was available in the initial standard. However, with the passage of time the data rate became insufficient. Also packet-switched applications such as always-on internet access was not included in initially standard. For this reason GSM Phase 2+ was introduced in the early 2000s. GSM phase 2+ was an improved version of initially GSM and included GPRS (General Packet Radio Service) for higher speed, packet-swithced Application such as mobile Internet. Meanwhile, investigations had been continuing with a view to increasing the intrinsic bit rate of the GSM technology via novel modulation techniques. This resulted in Enhanced Data-rates for Global Evolution (EDGE), which offers an almost three-fold data rate increase in the same bandwidth.

The combination of GPRS/EDGE, based on GSM infrastructure, brings system capabilities into the range covered by the International Telecommunication Unions IMT-2000 (third generation), see sub-Chapter 2.4, concept, and some manufacturers and network operators consider the EDGE networks to offer third generation services [23].

EDGE technology has average rate 400Kbits/sec and peak rate of 1 mbit/sec. Because GSM standard has reached performance limits since EDGE introduction, UMTS standard was developed for offering higher data rates and next generation services for UTRAN.

2.3.2 Physical Layer - Mac Layer

GSM is a digital cellular phone system combining TDMA and FDMA. Two bands (GSM-900, GSM-1800) are used by GSM in Europe. Each band is divided into 200KHz channels which are separated by guard bands. These channels are indexed with a unique identifier, ARFCN (Absolute Radio Frequency Channel Number). Subsequently, every channel is divided into 8 slots and it can be used with TDMA by equivalent number of users. Thus, a frequency channel is shared with TDMA by 8 users.

GSM signals are modulated using GMSK, Gaussian filtered MSK, (a form of Minimum Shif Keying, MSK). It has advantages of being able to carry digital modulation while still using the spectrum efficiently [24]. One of the problems with other forms of Phase Shift Keying (PSK) is that the sidebands extend outwards from the main carrier and these can cause interference to other radio communications systems using nearby channels. Thus, GMSK ensures the appropriate frequency usage without interfering the neighbour channels.

There is plenty of information to discuss for GSM Physical and MAC Layer but unfortunately are out of scope of this thesis. Further details can be found in ETSI GSM specification documents [26] and in bibliography [24], [25], [27].

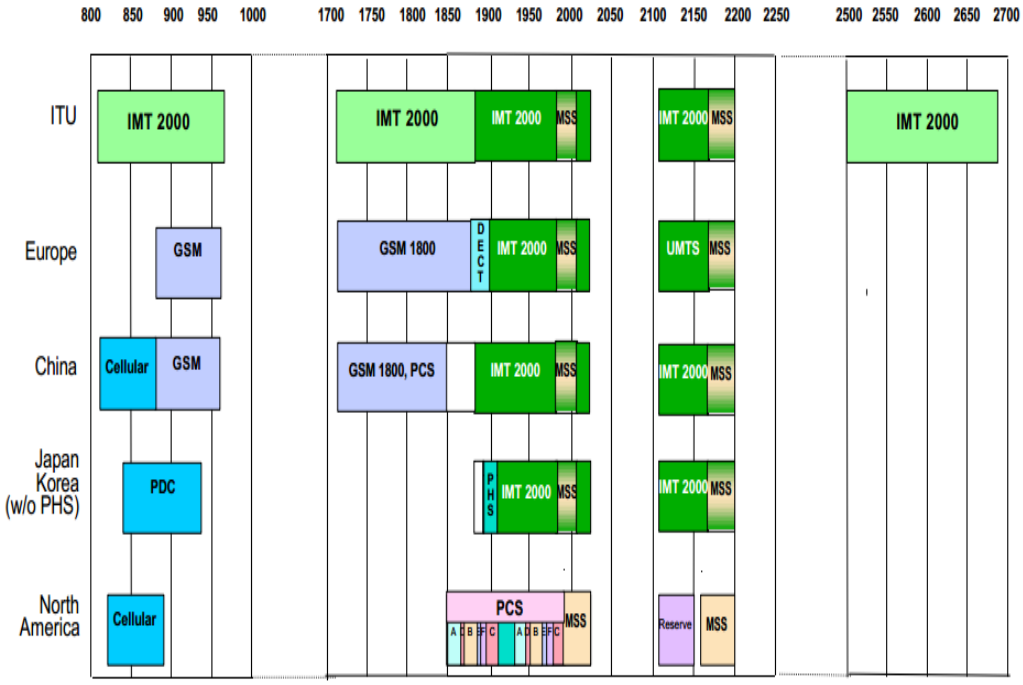

Figure 2.3: A short presentation of the mobile telephony bands all over the world. Source and details available on [28]

2.3.3 Frequency Bands

As it has been mentioned, GSM-800 and GSM-1800 bands are used in Europe. In Figure 2.3 the existing mobile telephony bands are presented. IS-95 (Interim Standard 95) is one of the dominant second-generation standards in North America and it is based on CDMA (Code Division Multiple Access) and DSSS (Direct-Sequence Spread Spectrum) [22]. CDMA uses a completely different approach to offer mobile services than GSM. All users access the same wideband channel (5MHz), signals multiplexed and the mobile and BTSs can separate the desirable signal by multiplying the signal with an appropriate code. It must be underlined that ETSI has adopted CDMA for building the 3G UMTS -Chapter 2.4- in Europe, since usage of CDMA achieves high data rates.

On Table 2.1 the separation of GSM bands in Europe and the respectively

GSM Ver.	Band	Uplink(MHz)	Downlink(MHz)	Channel Num
P-GSM-900	900	890-915	935-960	1-124
E-GSM-900	900	880-915	925-960	975-1023, 0-124
R-GSM-900	900	876-915	921-960	975-1023, 0-124
GSM-1800	1800	1710.2-1784.8	1805.2-1879.8	512-885
GSM-1800 is also called DCS-1800				
GSM-900	45MHz spacing between Uplink and Downlink			
GSM-1800	95MHz spacing between Uplink and Downlink			

Table 2.1: GSM Bands in Europe and their respective ARFCNs.

ARFCN are shown. Converting ARFCN to the relative absolute frequency value is defined on GSM specification [29]. Conversion types, which are included in MySignals Implementation, are quoted in Chapter **??** .

2.4 UMTS (3G)

The next generation networks (3G and the passage to 4G) are standardized and developed by 3rd Generation Partnership Project (3GPP), which is created by all the major telecommunications standard development organizations. Further details can be found on the 3GPP web site [31] .

2.4.1 Offering Services

A blueprint which is called Internet Mobile Communication 2000 (IMT-2000) defines some criteria for third generation technology [22]:

- Voice quality comparable to that of existing public telephony network.
- Data rate of 144 Kbps for access in a moving vehicle car, 384 kbps for access when the user walks (pedestrians), and 2 Mbps for the stationary user.
- Support for packet -switched and circuit-switched data services
- Interface to Internet, multimedia services such as video conference etc.

2.4.2 Physical Layer - Mac Layer

In Europe the standard which is used for creating UTRAN 3G networks, is UMTS. It was developed by 3GPP/ETSI. UMTS uses a CDMA modification named wideband-CDMA (W-CDMA). All the users access the same 5MHz channel, signal are multiplexed with each other and the signal's separation for each terminal is achieved by multiplying "mixed signal" with an appropriate code. Further details are out of the scope of this thesis.

2.4.3 Frequency Bands

Channel number is straightforward at 3G systems. Each channel has 5MHz bandwidth. Thus, UTRA (UMTS Terrestrial Radio Access) ARFCN is: $UARFCN = AbsoluteFrequencyMHz/5$.

UMTS	**Band**	**Uplink(MHz)**	**Downlink(MHz)**	**Channel Num**
IMT	2100	1920-1980	2110-2170	10562-10838
180MHz spacing between Uplink and Downlink				

Table 2.2: UMTS Bands in Europe and their respective ARFCNs.

2.5 LTE 4G (Under Development)

2.5.1 Objectives Defined

The fourth generation of cellular telephony is expected to be a complete evolution in wireless communications. Some of the objective defined by the 4G working group are as follows [22]:

1. A spectrally efficient system and high network capacity.
2. Data rate of 100 Mbit/sec for access in a moving car and 1 Gbit/sec for stationary users.
3. Data rate of at least 100 Mbit/s between any two points in the world.
4. Smooth handoff across heterogeneous network.

5. High quality of service for next generation multimedia support.

6. All IP, packet-switched network, support IPv6.

LTE is the latest standard in the mobile network technology tree. It is based on the GSM/EDGE and UMTS/HSPA network technologies increasing the capacity and speed, using a different radio interface with core network improvements [34], [35].

LTE in Greece will be offed by Cosmote [32] and Vodafone [33] probably in 2013.

2.6 Principles for Constructing Cellular Telephony Coverage Maps

A cell phone can use one of two networks each moment (2G or 3G). Hence we must distinguish the RSSI source that will be collected by our users. Cell Global Identity (CGI) is a unique worldwide identifier for each BTS, either 2G or 3G, in the world. It consists of: [MCC, MNC, LAC, cell-id]. MCC is Mobile Country Code and MNC is Mobile Network Code. Typically LAC is assigned to MSC or the UTRAN B-nodes (matches the GSM MSC in UTRAN) and is always different between 2G and 3G. For example, Cosmote at Chania has LAC equal to 312 for GSM and LAC equal to 1602 for UTRAN (3G). Hence, cellular network structure itself indicates the way to save RSSI data for craeting a mobile coverage map. RSSI must be interconnected with CGI (cell-id, LAC, MNC (network carrier), country (MCC)). This can determine the source of the RSSI and provide enough information for constructing the mobile coverage maps since at any case our information can be matched to the basic logic of cellular Telephony.

2.7 iPhone

Without a doubt, iPhone release in 2007 has changed the whole mobile phones industry. Over 250 million iPhones have been sold since 2007. One

Figure 2.4: The last three generations of iPhone (Source: Apple)

can observe that the whole mobile industry has adopted the iPhone patterns, philosophy and design. All the modern smartphones have a full phone-size capacitive [i] touchscreen and a multitouch technology which was first introduced by iPhone. Also, all the mobile operating systems, such as Android, Windows Phone OS, Symbian etc, have their own "App Stores" which was also firstly introduced by Apple in 2008 as part of iPhone 3G and iPhone OS 2. Iphone's operating system, iOS [ii] is considered by the overwhelming majority of the users as one of the best mobile operating system. Nowadays, iOS is also the mobile operating system for other Apple's mobile devices, the iPod Touch and the tablet iPad. In Figures 2.4 and 2.5 iPhone models are presented.

[i] Capacitive touchscreen works based on coupling effect of human body. They are much more accurate than resistance screens. The usage of resistance touchscreens it was not usable.

[ii] The iPhone's operating system has been renamed to "iOS" since version 4 which released in 2010. Until then was named "iPhone OS"

Figure 2.5: iPhone 3G/3GS, used for developing MySignals (Source: Apple)

2.7.1 Architecture and Software Development kit

A SDK was provided to developers by Apple in order to be able to create their applications for iPhone and release them in App Store. App Store is available for every iPhone, so even a single developer could use the iPhone SDK to build an application and release it directly to the App Store, accessing that way the whole iPhone users pool.

The iOS SDK offers many iPhone's features and capabilities for Application Development. A fully reference to iOS Developer Library is available online on [36]. The programming language for iOS environment is Objective C [37]. Below, some of the main characteristics of Objective C are shown:

- Object Oriented programming language. It is a small but powerful set of extensions in ANSI C language.
- Superset of C/C++: C/C++ code can be compiled inside Objective c
- Memory management [38]: Garbage Collector (Available only in Mac OS X), Reference Counting Environment (used in iOS).
- Powerful runtime environment: Dynamic typing and binding, message

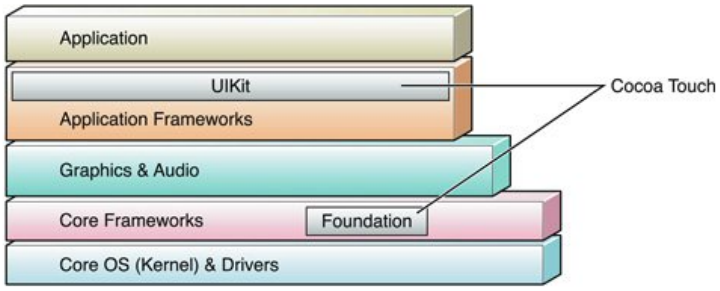

Figure 2.6: Detailed iOS Architecture (source: Apple)

syntax etc.

In Figure 2.6 and 2.7 the main iOS architecture is presented. Cocoa Touch APIs encapsulates the hardware capabilities and programming environment that are offered to developers. In Figure is shown the software services and elements that are provided by Cocoa Touch. Further details and APIs documentation are available online [36].

However, many Core Services and APIs as well as direct access to hardware and system utilities are denied and locked by iOS. For example, Core Telephony Framework which belongs to Core Services has the most of each APIs private -i.e., function headers are not available in public documentation, only Apple knows them. This restriction applies to many of the iOS APIs. CoreTelephony framework provides APIs to iPhone RSSI, cell-id, LAC, network carrier etc. Moreover access to the file's system outside local application's directory is not permitted by iOS.

Another restriction and downside is that you are not able of deploying applications on iPhone's hardware, unless you pay 99$ for the developer program. This strict policy was always a main characteristic of Apple. Apple considers that nobody should have full access to iPhone software or hardware. The main reason of course is to discourage piracy (Apple has a 30% commission in every App that is been sold from App Store). Also it is considered by Apple that nobody should have full access to iPhone software and hardware because it would break the "user experience" which they have created.

Applications development for iPhone is available only through the Apple's IDE (Integrated Development Environment) XCode. XCode runs only in operating system Mac OS X for Macintosh computers. Macintosh are equipped with Intel's processors so their architecture is very similar to PCs. Theoretically Mac OS X should run on a PC. Unfortunately, Mac OS X porting to PCs is extremely difficult since operating system kernel checks a lot of hardware parameters to ensure that the hardware which is installed on, is an official Macintosh computer. For example, when this thesis implementation had started, an attempt to install "hackintosh" on a Intel based PC was made. After a lot of effort, Mac OS X was installed on PC, but the PC was crashing after some minutes of operation.

Figure 2.7: Detailed iOS Architecture (source: CS193P lectures, Stanford University)

Chapter 3

Implementation: A Community Geographical Information System

3.1 Software Architecture

3.1.1 Software Components Overview

The basic software components and the general system architecture which are implemented in this thesis as well as the data flow, are shown in Figure 3.1. The software platform (GIS) consists of three parts. The first one is the MySignals Application for iPhone. Measurements which contain RSSI -i.e., the signal quality-, the serving cell tower, the network type (RAT), the neighbouring cells and a lot more technical info for the mobile network are observed by MySignals App. These measurements are saved locally in iPhone and more specifically to a SQLite database. At regular time intervals, assuming that Internet connection is available, all these measurements are packetized using JSON [i] (JavaScript Object Notation) format and they are sent to a central web server through HTTP protocol. At the central web server, which is the second part of our software platform, the measurements are unpacked and saved permanently to a MySQL database. The third part of our Community GIS is a mobile coverage map, which is the result of displaying the collected RSSI data to their corresponding location. Mobile coverage map is implemented using a heatmap engine. Each RSSI measurement is displayed using a color code which is dependent by RSSI

[i] JSON is a lightweight data-interchange format, commonly used by web services.

level. Cooperative mobile coverage map by iPhone users, is hosted in the website http://www.mysignals.gr/heatmapPage/heatmapPage.html [ii].

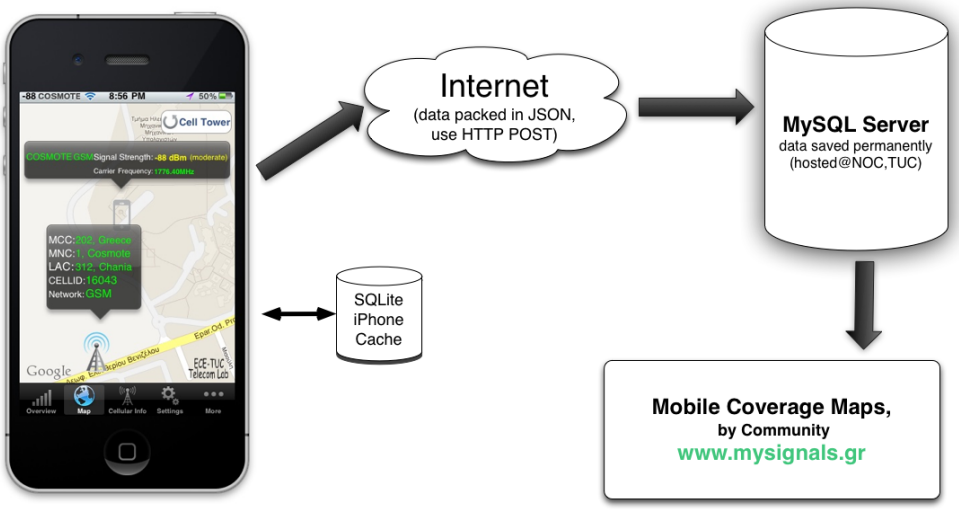

Figure 3.1: Community GIS: Thesis Software Components Overview.

3.2 MySignals: iPhone

3.2.1 Prerequisites and Background

Unfortunately an iPhone development course is not offered neither by ECE at TUC nor by any other university in Greece. A free development course is available online (videos, lectures and assignments for practice) from Stanford University at iTunes U [39]. The course offers a very good introduction to iPhone programming world, since basic principles of iPhone development such as objective c, useful APIs, common iPhone programming patterns and more, are explained. Also, many examples are provided during the lessons. In order to be familiar with iPhone programming, this course was followed up at the beginning of this thesis.

[ii] Web Browser supporting HTML 5 is required.

3.2.1.1 Field Test Mode

Field Test Mode is a software application which is usually pre-installed on the majority of mobile phones and provides the users cellular network information, technical details and parameters related to the transmission and reception, such as the following:

- Received Signal Strength Indicator (RSSI), transmit power and operating frequency (ARFCN).
- PLMN (Public Land Mobile Network) codes: MCC, MNC, LAC, cell-ID
- Neighbouring cell list parameters.
- Many more mobile phone and communication protocol details which are discussed on sub-Chapter 3.2.2.2.

On Table 3.2 a detailed description of all Field Test Mode parameters in iPhone is presented. Field Test variables are either calculated and known by the mobile phone itself (e.g. RSS or connected cell-ID) or known by "control signals", the BCCH (Broadcast Control Channel) which is transmitted by every BTS. BCCH carries a repeating pattern of system information messages that describe the identity, configuration and available features of BTS [41]. Field Test Mode is used by engineers for verifying the operation of the network while upgrades or modifications are applied on the mobile network's equipment.

Field Test Mode is available on iPhone just by dialling *3001#12345#*. By doing this, the Field Test App is appeared immediately on iPhone's screen. In Figure 3.2 screen-shots from Field Test App running on iPhone 3GS, are shown. The existence of Field Test App by default in iPhone, indicates that all the cellular network details and info which are necessary for creating MySignals App are available on iOS APIs. These APIs unfortunately, as it has been mentioned before, are not included in the official documentation of iOS SDK -i.e., these APIs are called private since are only accessed by Apple [40]. Discovering a way to access through our code the

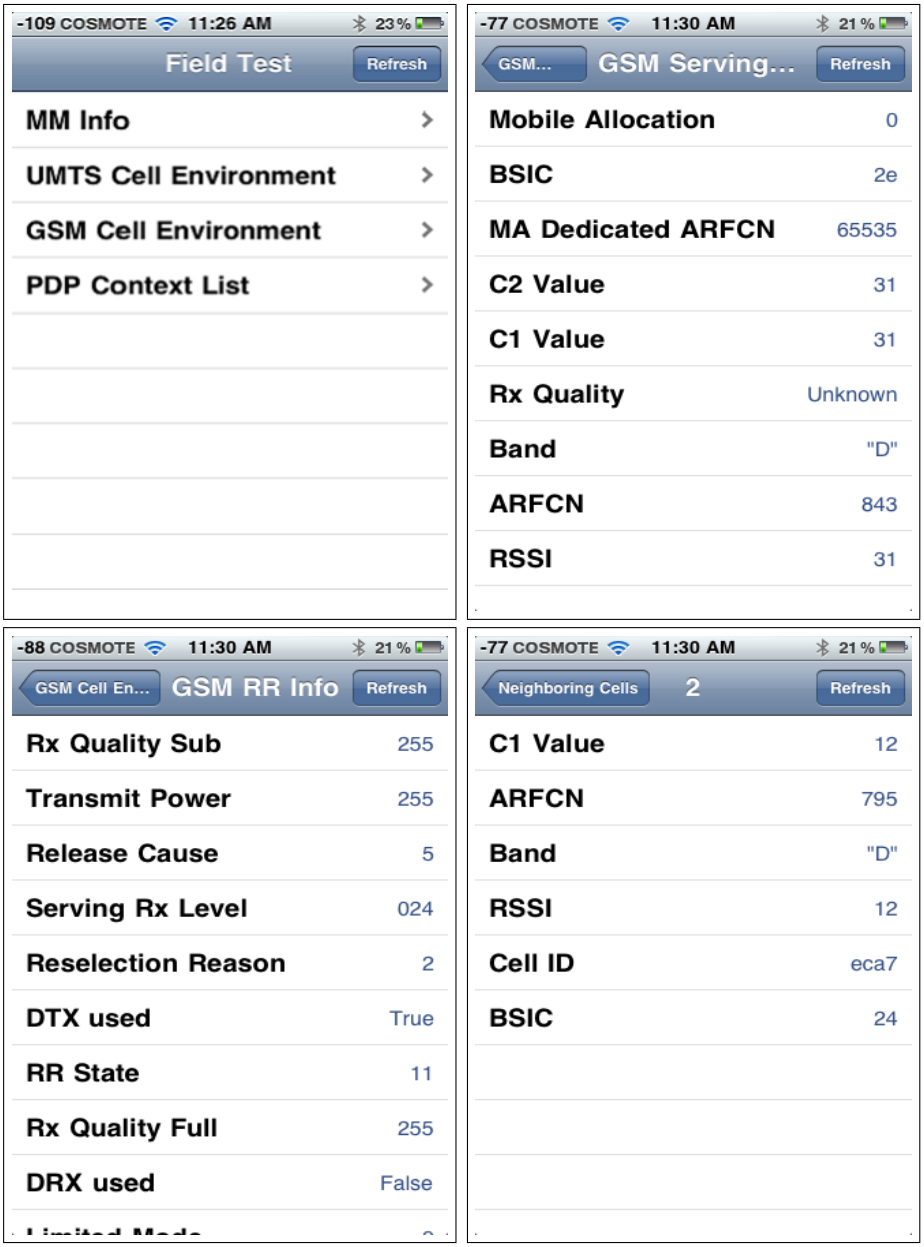

Figure 3.2: Field Test App running on iPhone 3GS with iOS 4.2.1. Field Test is available in all iOS versions.

information provided by Field Test Mode -i.e., read Field Test variables from MySignals App - was the most time consuming part of this thesis, since an official documentation does not exist and a lot of iOS restrictions had to be bypassed.

3.2.1.2 Received Signal Strength Indicator

The RSSI calculation is vital for every phone, since an indication for signal's quality -i.e., the well known five bars- is shown by every mobile. Also, RSSI is used by cell phone for choosing the best available BTS. The RSSI calculation takes place in the mobile's hardware. More specifically, the RSSI calculation is performed by GSM/UMTS modem's module in iPhone, which is responsible for all the mobile communications.

3.2.2 Bypassing Apple's Restrictions for accessing Field Test

3.2.2.1 Deploying Apps Without the official (paid) certificate

As it is has been already discussed, the officially development environment requires a paid Developer certificate in order to deploy and test compiled Apps on iPhone hardware. Otherwise, the compiled Apps are only allowed to run in iPhone Simulator on XCode environment. The great downside of the iOS Simulator is that it does not support any hardware features such as GPS or APIs to CoreTelephony framework, since these features do not exist in Simulator. They are only implemented in hardware. The iOS Simulator linker cannot even build an executable, if that contains hardware function calls to iPhone. This leads us to the necessity to bypass this restriction of iPhone SDK in order to be able to complete our work.

Jailbreaking [i] the iPhone was the first step. In a jailbroken iPhone a full access to the file system is granted and tools from Cydia Store, which are very useful for the development of MySignals, can be installed on iPhone.

MySignals App was initially developed in iPhone 3GS model with iOS 4.2.1. The greenpoison jailbreak was applied. Since Apple fixes the iOS and iPhone's hardware bugs, which allows the jailbreaking at every generation of iPhone and iOS, a new Jailbreak method comes on public based on other software or hardware bugs (they are called exploits in hacker's world).

[i] jailbreak is legal [42] with the term that no piracy occurs. Apple of course removes the warranty if a jailbreak software is detected in iPhone service.

A code-sign certificate and a provisioning profile (99$/year) by Apple are needed for deploying compiled Apps from XCode to iPhone [43]. Firstly a fake code-sign was created by following an online guide [44]. These settings were applied on XCode build Preferences. Secondly, the provision profile restriction was hacked [45]. Provision profile marks and signs your application in order to be recognized by iOS runtime environment and to be allowed to be executed. If the iOS detects an application without all the necessary digital identification entities provided by provisioning profile, the application will be banished and "killed". Thanks to Jailbreaking Community, there are several steps to hack this restriction and sign appropriately the executable App. A custom program which is called ldid makes all the "dirty" work, creating an executable that can be recognized by iOS runtime environment. All the steps of this method (that is available online) are applied, and XCode settings files are modified appropriately in order to bypass all these restrictions. Unfortunately the hacking method that deploys the App bypassing the confines of the official SDK, is completely custom and maybe subjected to changes in the future since Apple improves iOS security.

The above steps firstly were tested with a sample App in order to realise that iOS paid provision profiling was bypassed. There are two ways to deploy the customised App to an always jailbroken iPhone:

1. Install OpenSSH from Cydia Store. That gives a full access to iPhone's file System. Then the compiled App as it was described above can be copied in Applications Folder using a program like FIleZilla. From SSH terminal connection to iPhone, admin rights must be granted to our App in order to run in the iPhone.

2. Install through iTunes by drag and drop the App folder to the Apps in iTunes and sync iPhone-iTunes. The necessary prerequisite is to modify appropriately, the running daemon of iOS which checks if an Application is official and comes from App Store. From an SSH terminal connection to iPhone we just apply the command *"touch /var/mobile/tdmtanf"* in iPhone terminal.

The ssh communication to iPhone device is achieved though TCP/IP

protocol, using the Wi-Fi connectivity of the iPhone.

3.2.2.2 Access iPhone's Field Test Baseband (AT commands)

Considering what was discussed in sub-Chapter 3.2.1.1, the main goal was to access some way, through a code, the Field Test variables. Private APIs are hidden and not available from official documentation, but fortunately they can be discovered using reverse engineering techniques. Reverse engineering private APIs is a state of the art field and requires extremely good knowledge of assembly, compilers, details about linking and a lot more. From executable files, methods and functions, symbols can be extracted using programs such as otool [46]. Subsequently, using a debugger the hacker tries to find out how this method works and what are the arguments of the functions.

Private APIs headers for Field Test were firstly reversed engineered by hacker Geohot [47] in 2007. These headers [49] were the only available material online for getting through Core Telephony framework RSSI, PLMN codes (MCC, MNC, LAC, cell-id) and neighbouring cells info. The usage of these functions lead the iPhone to crash. Probably, the iOS CoreTelephony framework APIs has been updated since then.

No other examples of reading RSSI and Field Test info from iPhone were available on-line, so a completely different approach was considered. The key aspect of this consideration is that every single GSM/UMTS module in the world can be controlled and submit a query (e.g. ask for RSSI and cellular info) to it using AT Commands through serial line (UART) interface [48]. This is also applied on iPhone architecture which is presented in Figure 3.3. All the mobile communications of iPhone are controlled by an independent GSM/UMTS module (also known as modem or baseband) which is connected through a serial line (UART) interface to the iOS environment. This serial line (UART) is available from iOS as a communication socket, outside official SDK. Typically control of a GSM/UMTS module is performed by Phone App, which is also named "CommCenter", using AT commands. For example, "AT+CMGS" command submits an SMS etc. The modem responds to the commands or queries, which are also sent to the CommCenter through the

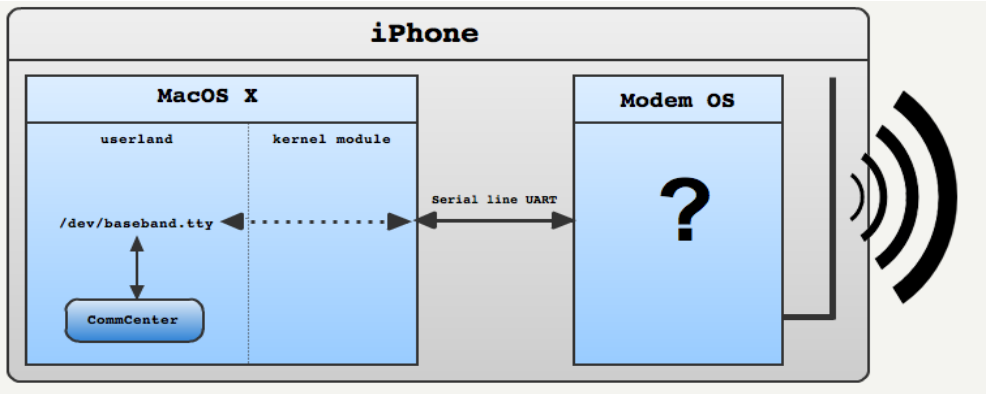

Figure 3.3: Connection between iOS and GSM/UMTS modem of iphone

serial line interface.

Thanks to Jailbreaking community, a software library for sending AT Commands to the iPhone's baseband and read the corresponding responses, is available online as the "iPhone-SMS project" [50]. This library has been used for several projects and tweeks on Cydia Store, such as the iPhone SMS delivery report which uses AT commands to add SMS delivery reports on iPhone's message App and of course for sending SMS outside the official iPhone App. In addition, minicom tool, available on Cydia Store, uses this library and offers a terminal for querying AT Commands to iPhone which was extremely useful for debugging. The functions for communicating with baseband modem through the serial UART are explained in Table 3.1.

Although everybody has used this library for SMS functionality, this thesis exploits these functions for reading RSSI and the whole cellular info -i.e., to read all these variables of the Field Test Mode. In order to retrieve all the necessary Field Test Info for building MySignals App two AT commands were discovered and used:

1. "AT+CSQ": The RSSI is returned in ASU (Arbitrary Strength Unit) format by posting this command.

2. "AT+CGED=0": This command returns a complete cell environment description.

Function	Description
InitConn()	Open the connection (socket) to iPhone's baseband.
sendAt()	Submit "AT" command to baseband and waits "OK" in order to confirm that the connection to the baseband is alive.
SendCmd()	Submits a programmer defined AT Command.
ReadResp()	Blocks and waits baseband to respond.
CloseConn()	Close the connection to iPhone's baseband

Table 3.1: Functions for submitting AT Commands to iPhone's Baseband and getting back the appropriate responses.

No documentation is available for the models of modem modules which have been used by Apple for constructing iPhone. The only available material is specification sheets with a brief technical description of the modems [51]. Discovering the above commands was achieved by investigating AT Commands manuals of other GSM/UMTS modules [52] and the 3GPP, ETSI, specificiation sheet for AT Commands [53] since all the modems have similar format of AT Commands.

ASU or "Arbitrary Strength Unit" is an integer value proportional to the received signal strength measured by the mobile phone. ASU is commonly used by GSM/UMTS modems for RSSI representation. The conversion formulas from ASU to dBm are given in the Table 3.5.

The steps for querying baseband are:

1. Open socket to modem using *InitConn()*.
2. Test that the connection is alive by sending "AT" and wait for "OK" in the function *ReadResp*.
3. Submit to the socket the appropriate AT Command ("AT+CSQ" or "AT+CGED=0").
4. Block and wait for answer in the function *ReadResp()*.
5. Close modem's socket.

Since the baseband may delay several seconds to respond, the function *ReadResp()* blocks for the corresponding time interval. If the querying of

the baseband occurs inside Main Thread then the whole application will be "frozen"-blocked during this time interval, because the Main Thread is responsible for the GUI handling. Usually the delay time varies between 1 and 2 seconds. Nevertheless, sometimes the baseband delays reach several dozens of seconds or even a minute. In general, a large delay occurs when the baseband is busy (e.g. an active phone call) or if the signal reception is poor or sometimes when the phone is in Airplane mode. Blocking the whole App for several seconds cannot be an acceptable solution because it interferes with the user's interactive experience. Thus, the procedure for querying baseband for the Field Test variables is performed on a background NSThread [i] and users can manipulate MySignals while it is reading the RSSI and the other Field Test data, since Main Thread is "free".

The responses from baseband are in plain text format (see Appendix 1 for examples). In order to extract all the Field Test information in separated variables, an appropriate text editing was applied to the received answer, using NSString text editing methods [ii]. For example, the RSSI ASU value was extracted from the plain text answer with two steps: Firstly the "+CSQ:" position was discovered inside answer and afterwards the ASU value which follows "+CSQ" was read. This approach was used for extracting all the field test parameters from the text stream -i.e., the answer from the baseband- which is quoted in Appendix 1.

The Field Test parameters are presented on Table 3.2. Many Field Test parameters which are extracted are not in human readable format -i.e., are encoded. The disambiguation of all this mobile's technical information was done using a relative At Commands manual [52], the official GSM specifications sheets [29], [41] and the [27] which summarizes all the GSM technology. The data interpretation of the Field Fest data and the saving procedure of the measurements -i.e., pair of RSSI with the corresponding cellular network details- are discussed in sub-Chapters 3.2.3.1, 3.2.3.2.

The approach discussed in this section, applies on iPhone 3G/iPhone 3GS

[i] NSThread is the POSIX Thread implementation provided by Core Foundation.

[ii] NSString is the collection of methods and logic for handling and editing strings, provided by Core Foundation

Mobile's Network Information	
RAT	Radio Access Technology (GSM or UMTS)
Band	The Frequency band that mobile operates (see table 2.1, 2.2), e.g. GSM-900 etc.
MCC	Mobile Country Code. A unique identifier is assigned to each country.
MNC	Mobile Network Code. A unique identifier is assigned to each network carrier.
LAC	Location Area Code. A unique identifier is assigned to a specific region (LAC identifies MSC).
Serving Cell Tower (BTS)	
PLMN codes	Public Land-Mobile Network Code (MCC, MNC, LAC)
cell-ID	The unique identifier of the serving
CGI	Cell Global Identity is composed of PLMN codes and cell-ID.
Mobile's Receiving And Transmitting Parameters	
RSSI	Received Signal Strength Indicator in ASU, calculated on modem's hardware
Transmit Power (*Tx pwr*)	Transmitted Power Level encoded in [55].
ARFCN	Absolute Radio-Frequency Radio Channel. The channel indicates the *absolute downlink and uplink carrier frequency* of the mobile [29].
GSM Network, operating details and parameters.	
BSIC	Base Station Identity Code. It is needed because it is possible that mobile stations receive the BCCH of more than one BTS on the same frequency.
C1	Cell Selection Criterion.
C2	Cell reselection Criterion.

Table 3.2: Synopsis of Field Test Information extracted by MySignals using AT Commands.

and iPhone 4 with some minor changes summarized on Table 3.4. All the above models have similar modems, manufactured by Infeneon. Qualcom modems have been adopted by Apple since iPhone 4S in order to achieve

Provided Info for a neighbouring GSM Cell (6 cells available)	
cell-ID	The identifier of the neighbouring cell.
Band	The Frequency band that mobile operates(see table 2.1, 2.2), e.g. GSM-900 etc.
ARFCN	Absolute Radio-Frequency Radio Channel, is the channel in which this cell is operated.
RSSI	The Received Signal Strength Indicator from this cell.
C1	Cell Selection Criteria.
BSIC	Base Station Identity Code.
Provided Info for a neighbouring UMTS Cell	
Cell	Cell type.
SC	Scrambling Code.
RSCP	Received Signal Code Power.
ECN0	The received energy per chip (Ec) of the pilot channel divided by the total noise power density
DLF	Downlink Frequency Channel Number.
RV	Ranking Value

Table 3.3: Synopsis of Field Test Information extracted by MySignals using AT Commands, Part 2, neighboring cell lists, depending on Network Type Case.

better performances. Unfortunately, nobody has achieved to submit through custom code, AT Commands to iPhone 4S, until now. Probably the communication pattern has completely changed and Apple introduced another approach for the communication with the baseband. For example, the iPhone SMS delivery project which has been mentioned previously, has been abandoned by his creator [54], since he could not determine the modems's communication mechanism. No one else from the Jailbreak scene has achieved this until now. All the above details, the accessing method to baseband and the supported iPhone models by MySignals are summarized on Table 3.4.

3.2.2.3 Access iPhone's Field Test through private APIs

Although the initial approach using private APIs of CoreTelephony framework failed, a working API of CoreTephony was discovered during the development of this thesis. Thanks to Jailbreaking Community, the CoreTele-

phony Notification Center was reversed engineered. The CoreTelephony Notification Center posts software notifications -i.e., software runtime messages for intercommunication- to every runtime object which is registered to observe it. The following are included in the notification message:

1. RSSI value: Matches the value of RSSI which is displayed in upper left corner of the screen.
2. Cell-ID.
3. LAC.

Every time an update of these values occurs, a function automatically is called and the above data are supplied through a NSDictionary. NSDictionary is data structure which contains values for given keys -i.e., the key is the "RSSI", the value is the arithmetic value in dBm. The RSSI value provided by this method, seems to be an average of mobile phone's RSSI provided by "AT+CSQ" command. The RSSI values which are read using AT Commands change rapidly, even with a time difference of 1 second. On the other hand, RSSI value from private APIs changes very slowly. All the above observations were extracted experimentally.

As it has been mentioned on Table 3.4, submitting AT Command through code is not supported currently by iPhone 4S. The current method will be considered in the future as a solution for porting MySignals in iPhone 4S. As it has been already discussed, for building the mobile coverage maps we need: RSSI, cellID, LAC, MNC, MCC and network type. The first three are provided through CoreTelephony private Callbacks. The MNC and network type are accessible from the public APIs of CoreTelephony (since version iOS 4.0). Hence the private callbacks methods constitute a very good alternative in the case the new baseband of iPhone 4S cannot be hacked for supporting AT Commands.

	iPhone 3G	**iPhone 3GS**	**iPhone 4**	**iPhone 4S**
Baseband Chip	Infineon X-Gold 608	Infineon X-Gold 608	Infineon X-Gold 618	Qualcom MDM6610
Supported RAT	GSM/EDGE (850,900,1800,1900MHz) UMTS/HSDPA/HSUPA(4S) (850,900,1900,2100 MHz) CDMA EV-D0 (1800,1900 MHz), seperated iPhone 4/4s, *versions are not available* in Europe			
Supported iOS	4.0 - 4.2.1	4.0 - 5.1.1		5.0.1 - 5.1.1
Field Test Mode (AT Commands)	**SUPPORTED** iPhone 4 socket port requires admin rights after a hardware reboot			*Not Supported*
CoreTelephony Private Callbacks	i)RSSI ii)cell-ID iii)MNC, MCC, LAC iv)RAT **supported**, iPhone 4S is currently under development			
Notes (socket etc.)	/dev/tty.debug		/dev/dlci.spi -baseband. extra_0	*Not Supported*

Table 3.4: Supported iPhone models by MySignals and Synopsis of accessing cellular info methods. IPhone 5 released on September 2012 and has not been jailbroken yet.

3.2.3 Application Functionality

3.2.3.1 Data Interpretation Library

Many of the extracted Field Test Values are encoded. Therefore, a software data interpretation library was implemented as part of MySignals App, in order to convert all the following values into a human readable format:

- RSSI is encoded in ASU format as it has been previously pointed. The conversion formulas from ASU to RSSI in dBm are shown on Table 3.5. These formulas are defined in [52], [56] and were validated experimentally, comparing RSSI from AT Commands with the RSSI provided by iOS.

- ARFCN encodes the carrier frequency for uplink -i.e., the frequency channel where mobile transmits data to the BTS- and the downlink -i.e., BTS transmits data to mobile. The centre of the absolute carrier frequency is calculated by the formulas on Table 3.6.

- MNC is paired with each network carrier everywhere in the world. The Table 3.7 includes the pairing of the greek network carriers to their respective MNC, which is implemented at MySignals App.

- The transmitted power of a Mobile phone is controlled and defined by BTS. BTS sends a special message to the mobile called "power control level". For example, power control "0" means that the mobile can transmit 30 dBm with 3 dBm tolerance. The Field Test Mode provides the mobile's transmitted power encoded in "power control level". Power Control levels are defined in detail in GSM specification [55] and were implemented in Interpretation Library according to the referenced document.

ASU	**GSM Networks**	**UMTS Networks**
Range	$0 \ldots 31$	$-5 \ldots 91$
RSSI formula	$RSSI(dBm) = 2ASU - 113$	$RSSI(dBm) = ASU - 116$
Unknown - not detectable	99	255
Notes	ASU encodes RSSI	ASU encodes RSCP which matches RSSI in UMTS.

Table 3.5: Conversion Formulas from ASU to RSSI in dBm.

	Uplink Frequency (MHz)	**Downlink Frequency (MHz)**
PGSM-900	$f_{UP} = 890 + 0.2\text{ARFCN}$	$f_{DL} = f_{UP} + 45.0$
EGSM-900	$f_{UP} = 890 + 0.2(\text{ARFCN} - 1024)$	$f_{DL} = f_{UP} + 45.0$
GSM-1800	$f_{UP} = 1710 + 0.2(\text{ARFCN} - 511)$	$f_{DL} = f_{UP} + 95.0$
UMTS-2100	$f_{UP} = \text{UARFCN}/5$	$f_{DL} = f_{UP} + 190.0$

Table 3.6: Conversion Formulas from ARFCN to absolute carrier frequency

3.2.3.2 Measurements Saver Subsystem: SQLite Schema

The basic purpose of this thesis is to collect to a cental database RSS measurements with their relative location and cellular environment (network

Network Carrier	MNC
Cosmote	1
Vodafone	5
Wind	9
Q-Wind	10

Table 3.7: Greek Mobile Network Carrier Codes (MNCs)

type, network carrier etc.). These measurements definitely must be firstly cached locally, at a persistence store [i] in the iPhone, for several reasons:

- It is not effective to keep hundread or even thousand of records in main memory (RAM). The performance will be slow and if e.g. iPhone crashes, all the measurements will be lost.
- Internet access for uploading data is not always available.
- It is not effective to submit individual measurements to the web server.

IPhone SDK offers a Cocoa API for saving efficiently data on the iPhone's disk using SQLite database. The library is called Core Data and is an object graph wrapper and management system for an SQLite database. In Figure 3.4 the basic architecture of the Core Data is described. The programmer can define Entities with their attributes and their relationships between them using a graphic tool. The Core Data's model is very close to the classic relational model which is used by relational database systems. At the runtime, the programmer can create objects from each entity and define the relationships between them, creating this way an object graph. The object graph is maintained appropriately from Core Data runtime system. When the programmer asks for saving data, the Core Data serializes all the entities and saves them to a SQLite database file on iPhone's filesystem. SQLite and its wrapper, Core Data, have many advantages:

- Complete SQL database in an ordinary file.

[i] Typically persisent store is a hard disk. The data are saved permantly even the disk is outside of electric power supply.

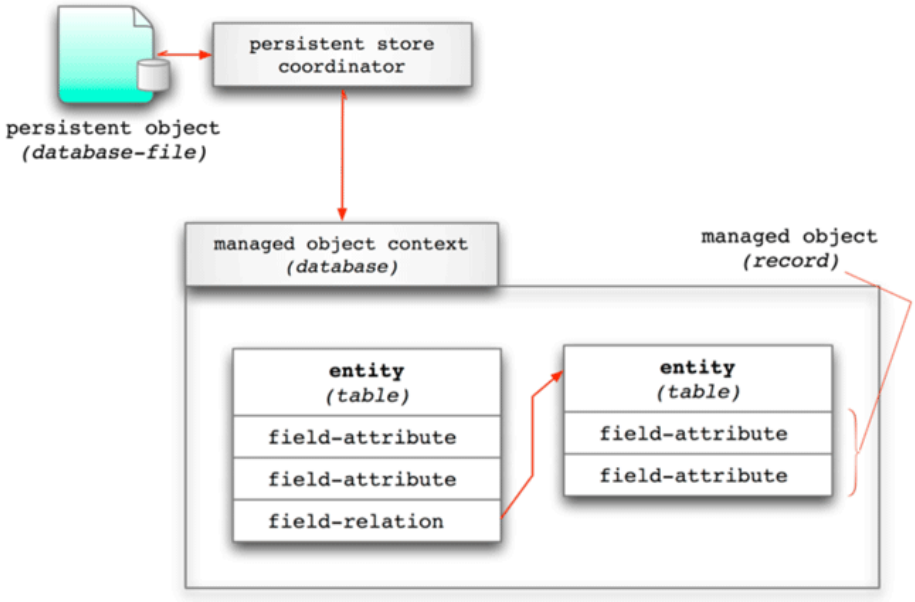

Figure 3.4: Core Data software Architecture (Source: www.drdobbs.com)

- Simple, compact, fast, reliable.
- Included on the iPhone platform, no server.
- Great for embedded devices.
- The programmer can use easily the saved data in DB, as objects in runtime.
- Serializing, deserializing and fetching of the data from hard disk is maintained by Core Data. Thus, the programmer does not implicate in low-level programming details.
- The queries from Core Data are simple, applied using NSPredicate format which is similar to the SQL logic.

Further details can be found on Core Data documentation [57]. When the application is presented in foreground the measurements are being saved

continuously, while as long as it moves to background the measurements are being saved periodically (a user defined setting).

The Core Data/SQLite schema in Figure 3.5 is implemented for saving MySignals App measurements. The single arrow side shows "to-one relationship", while the double arrow side shows "to-many relationship". The relationships between entities can be bedirectional -i.e., one relationship may have an inverse relationship. Each relationship arrow in Core Data Schema starts from its relationship name.

The Core Data (SQLite) Schema represents a comprehensive description of the application domain model and also indicates our logic for recording RSS measurements. There are several points which must be underlined:

- The organization of the schema -i.e., the entity graph- follows the cellular telephony's structure which is mentioned previously. A measurement containing RSSI, Tx Power, ARFCN etc, is paired with the Cell Tower where mobile phone is connected and served. Subsequently, each cell tower belongs to one Location Area Identity. This can be considered inversely: A Location Area Identity (The Code for a specific network in a specific region by a network carrier) has many BTS (Cell Towers). In each BTS can be observed many measurements from the users.

- After getting cellular info "environment" using "AT+CGED=0", MySignals keeps five successive RSSIs (each one needs approximately one second to be fetched) using "AT+CSQ". This is due to the fact that RSSI from "AT+CSQ" changes rapidly if the mobile's reception is unstable or mobile is moving. Therefore, it is desirable to estimate the overall behaviour of RSSI.

- The Measurement Entity provides the basis of the recorded information and is connected with particular relationships to other entities giving a detailed stamp for the RSSI, the location and the cellular information of the mobile phone. The RSSI attribute stores the RSSI which is retrieved by private iOS callbacks. Each measurement has "one to one relationship" with the entity MetaData. The five successive RSSI

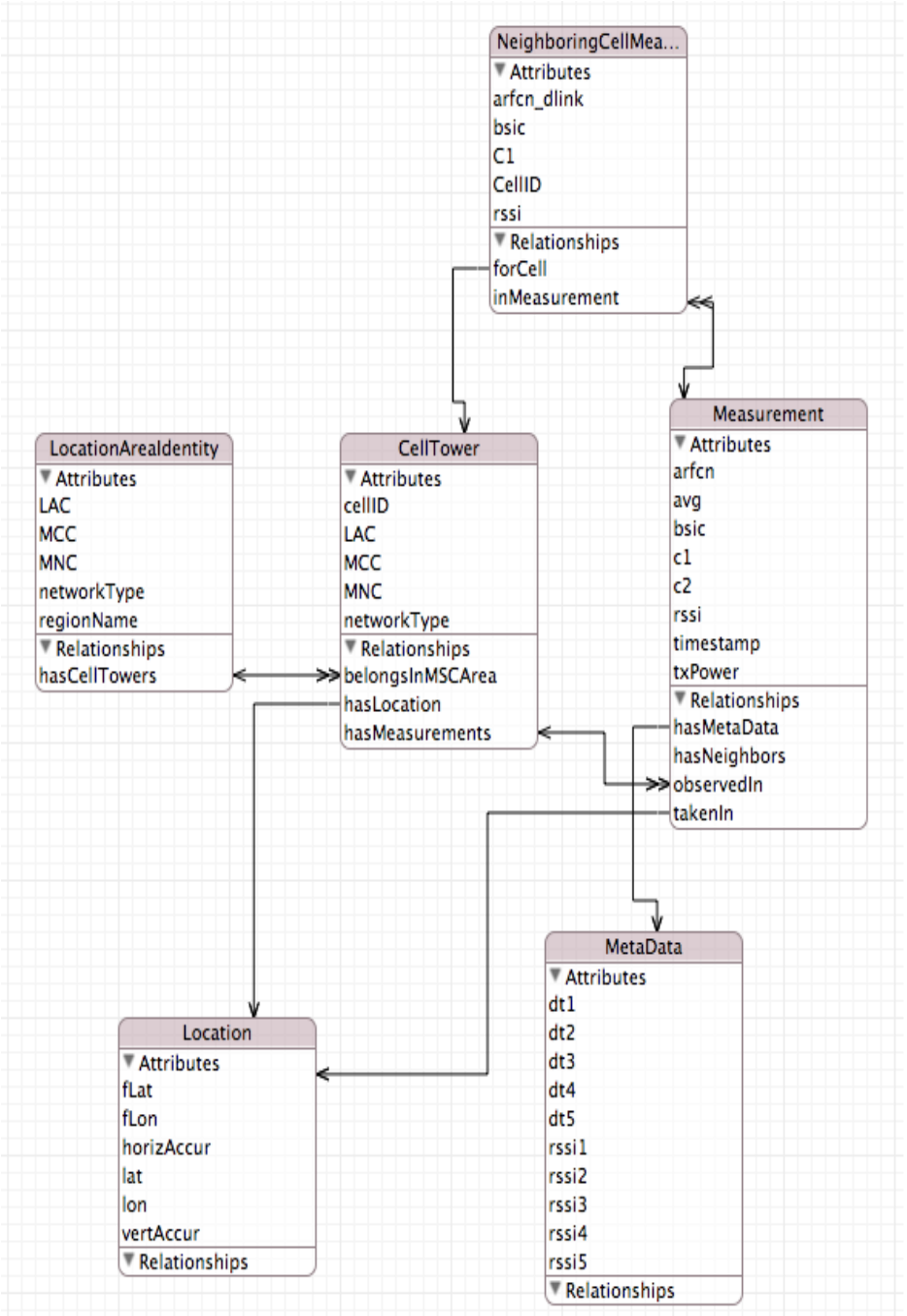

Figure 3.5: Core Data (SQLite) Schema for caching on iPhone the measurements. The Schema represents the application's logic.

values, which are pointed in the previous bullet, from "AT+CSQ" are stored by the MetaData entity. The relative time intervals between the measurements are saved in attributes "dt".

- Each Measurement has one Location Entity. The Location Entity contains the initial coordinates of the measurement and the final coordinates, since the mobile could move during the logging process which lasts several seconds due to baseband's delays. The initial and the final location are provided by CLLocationManager which is included in iPhone's SDK. The best available accuracy was chosen at CLLocationManager, because RSS measurement must be paired to its exact location. Thus, CLLocationManager uses a-GPS [ii] which also provides the accuracy in meters (the radius of uncertainty for the location, measured in meters) for the provided coordinates.

- Combining the successive RSSIs with the initial and the last location gives us an opportunity to detect the user's movement and to study the RSSI behaviour under moving circumstances.

- At the SQLite database, GSM and UMTS measurements share the same entity for practical reasons. The variables which do not exist in the UMTS case are just left empty.

- Timestamp is kept for each measurement, in order to perform a time based analysis of the RSS measurements.

A priority queue (FIFO:First In First Out) is included in MySignals implementation for recording measurements into SQLite. As it is analysed in the next chapters, in some cases the Core Data DB is busy and cannot serve insertion immediately. For example, Core Data may be busy due to extracting data for uploading. Thus the measurements remain in FIFO until Core Data is accessible again.

[ii] Assisted GPS: Using a combination of Wi-Fi and Cell Tower tringulation with GPS

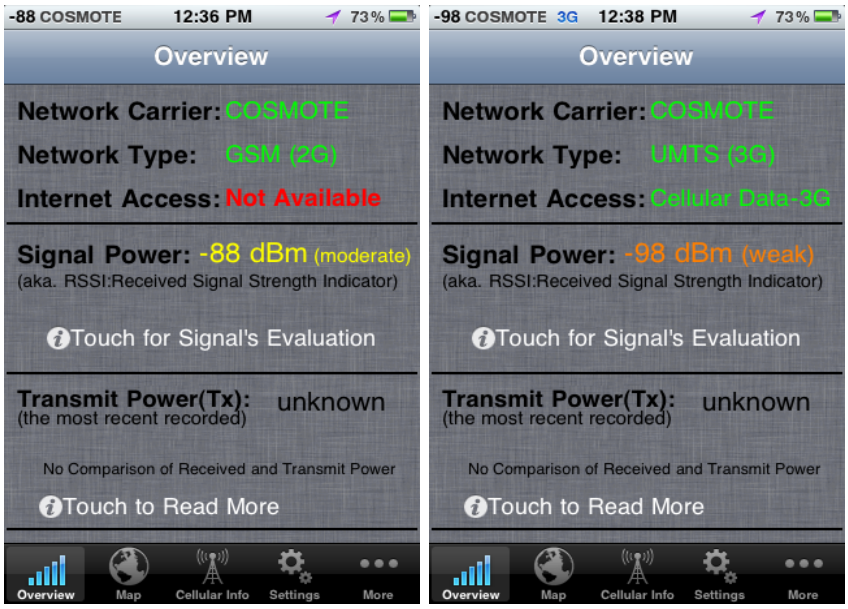

Figure 3.6: Overview screen: An entry point to MySignals App.

3.2.3.3 Content and Features

In this sub-Chapter the screens of MySignals App GUI are presented in order to overview MySignals capabilities and information provided to the users.

Overview Screen

In Figures 3.6 and 3.7 screenshots from MySignals "Overview" screen are demonstrated. The Overview screen was designed as an entry point to MySignals App. Only the basic information are displayed in this screen, such as the Network Carrier, the Netowork Type (GSM-2G- or GPRS-2.5G- or UMTS-3G-), the RSSI and the Tx Power. If the iPhone is out of network, e.g. Airplane Mode, the appropriate messages are displayed, as it is demonstrated in Figure 3.7. Also, a qualitative comment for the RSSI level is shown.

The user is able to read further details for the signal's quality reception level, understand what practically means this RSSI value and realize how important is to have a good signal's reception level (see Figure 3.8).

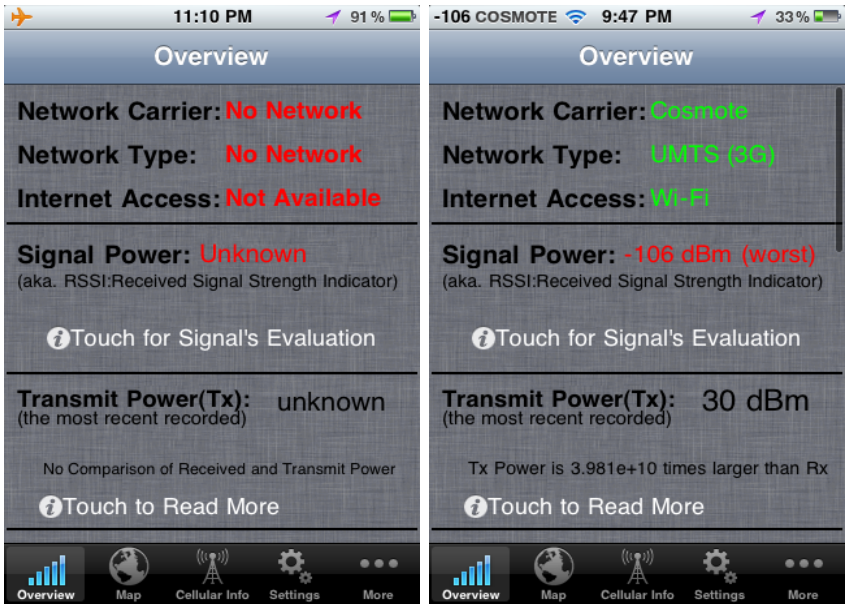

Figure 3.7: i) Airplane Mode ii) A worst signal case.

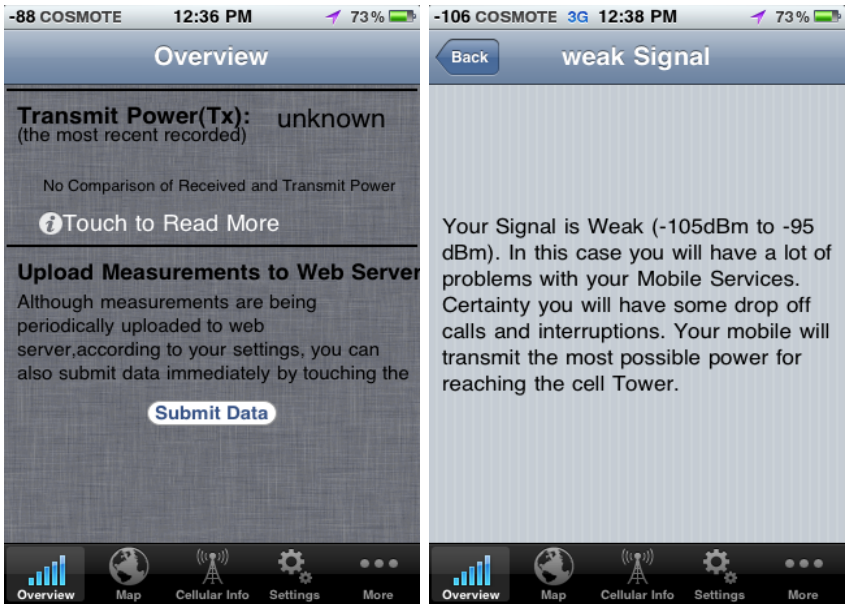

Figure 3.8: i) Immediate upload measurements button ii) RSSI evaluation.

The RSSI label is colourized according to the signal's quality level (Green: Perfect, Excellent, Very Good, good. Yellow: Moderate. Orange: Weak. Red:worst). A button is available for immediate submit of the collected data

(see Figure 3.8). Finally, comparison screen of Tx and Rx Power is also available in order to give users food for thought about the importance of a dense Cell Tower Network (see Figure 3.9).

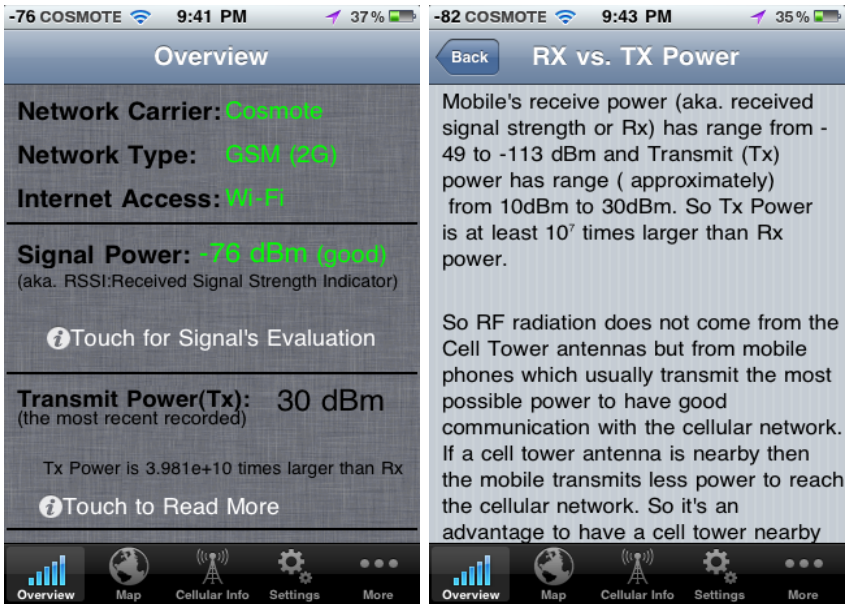

Figure 3.9: Comparing the Receive and Transmit Power.

Map Screen

The user's current location is displayed on Google maps [i] as well as the serving cell tower. A custom pop up bubble was implemented for each annotation on the map. The initial code was published by [58] and was modified for the needs of MySignals.

In Figure 3.10 screenshots from Map Screen are demonstrated.

By pressing the mobile's annotation -i.e., user's current location- a bubble comes on front, displaying:

- RSSI with the qualitative explanation.
- Carrier Frequency.
- Network Type and Network Carrier's name.

[i] Cocoa MKMapView APIs offers a Map environment for displaying your data and annotations.

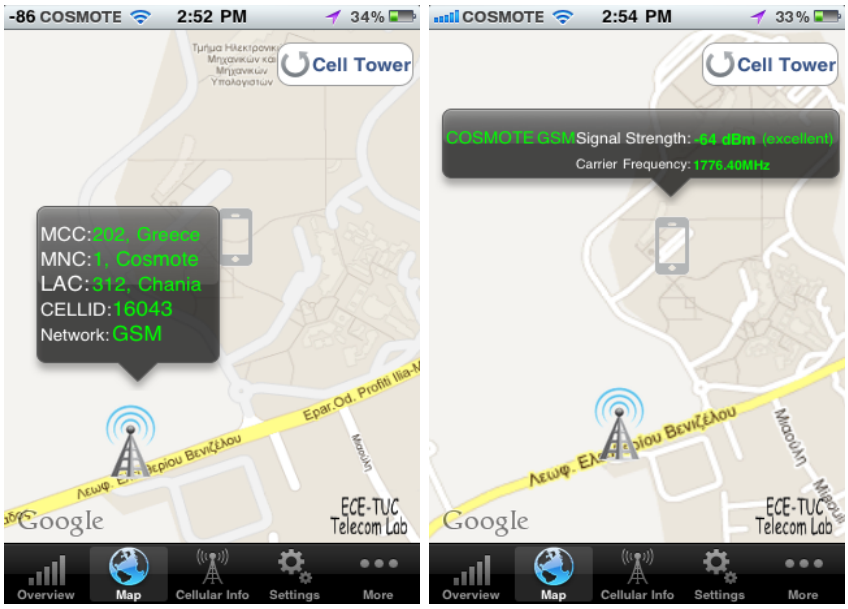

Figure 3.10: Map Screen displaying the serving cell and mobile's information.

By pressing the Cell Tower's annotation a bubble comes on front, displaying:

- Cell-id.
- LAC and Network Type.
- MNC (Network Carrier).
- MCC (Mobile Country Code).

The Cell Tower Position is provided either from a Google hidden API (which provides an estimated position per cell-id) or in the case that current cell-id is not included in that API, a random position is chosen. The Cell Towers positions are not public available in Greece with a few exceptions.

If a change in the connected Cell Tower is detected, then the user is notified by a prompt from MySignals App to refresh the map. As long as Map Screen is opened, for a few seconds a guideline message for tapping icons is appeared. Both cases are demonstrated in Figure 3.11.

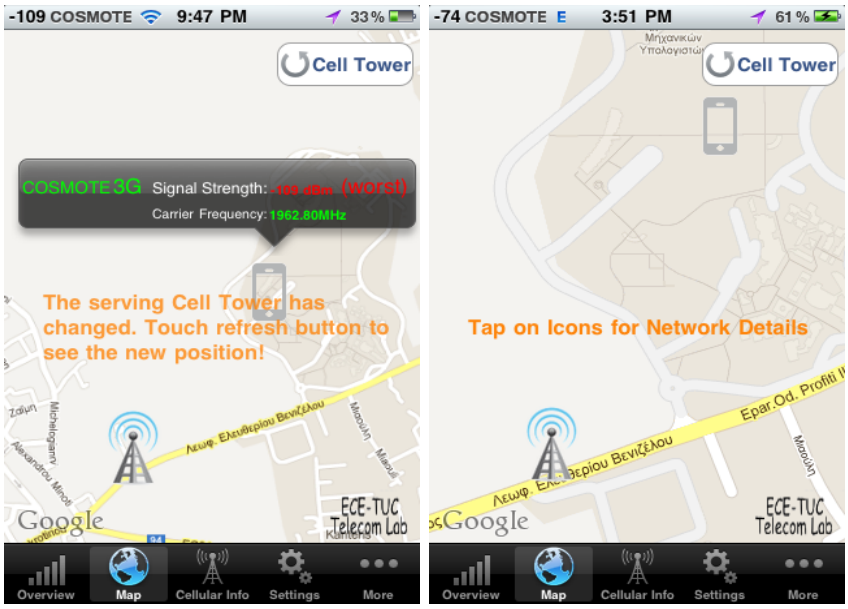

Figure 3.11: Map Screen prompt messages giving guidelines to users.

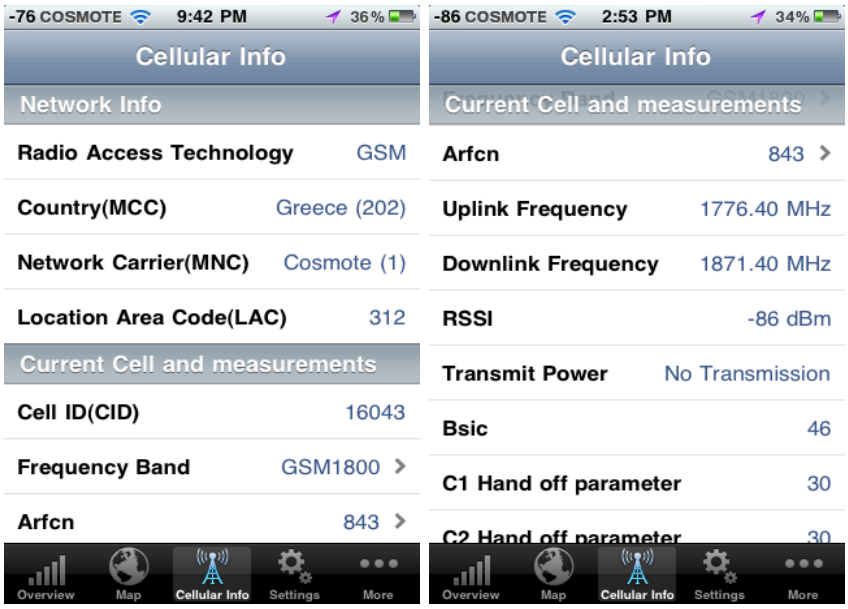

Figure 3.12: Cellular Info Screen: An engineering oriented screen.

Cellular Info

In Figure 3.12 screenshots from Cellular Info screen are demonstrated. It is definitely an engineering oriented screen, providing detailed information

about the cellular network. In addition to what is presented to the above screens, in this screen are also shown the following.:

- ARFCN, downlink carrier frequency and uplink Carrier frequency. Absolute frequencies are calculated as it was discussed in sub chapter.
- A list with the neighbouring GSM cells and parameters for each one (ARFCN, Band, cell-ID, RSSI, C1, BSIC). See Figure 3.13.
- BSIC parameter, a useful code for seperating neighboring BTS.
- Currently Frequency Band. C1 (selection), C2 (reselection) criteria.
- Location coordinates and GPS accuracy (see Figure 3.14).
- System info: iOS Version and iPhone Model (see Figure 3.14).

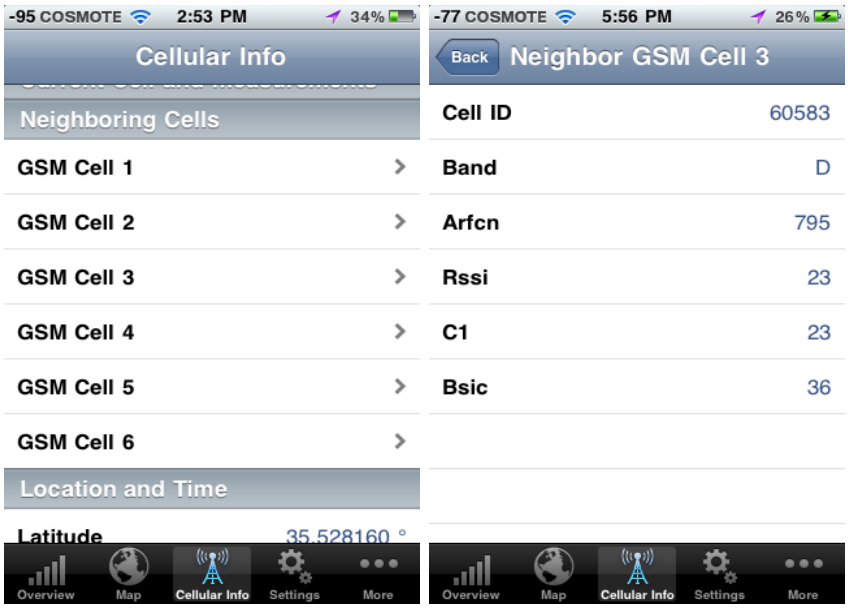

Figure 3.13: Screenshots from Cellular Info Screen.

Settings Screen

In Figure 3.15 a screenshot of Settings Screen is demonstrated. Users can modify several parameters for data logging and uploading procedure, which will be discussed in sub-Chapter 3.3.3, such as:

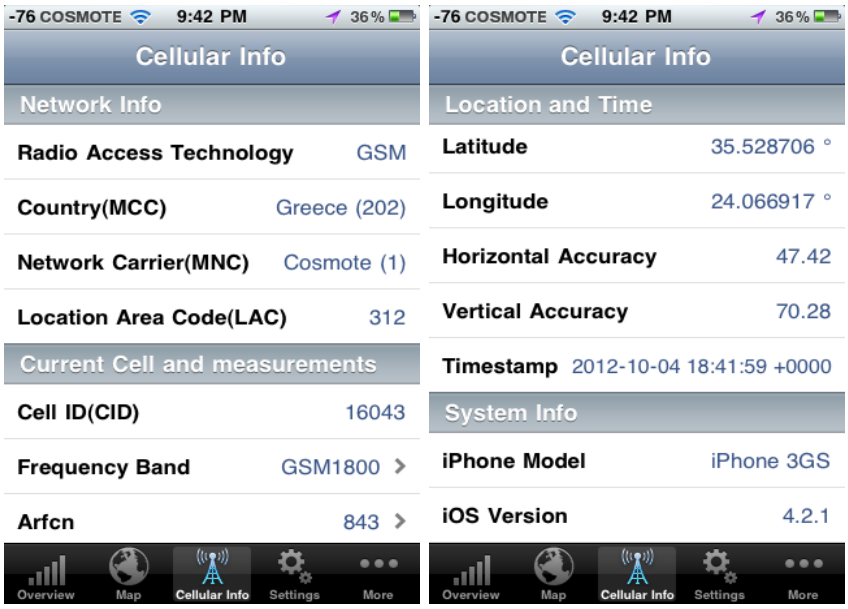

Figure 3.14: Cellular Info Screen provides coordinates, accuracy and system's information.

1. The Measurements logging frequency. When MySignals is on background App wakes up on certain intervals, logs measurements and then sleeps. This time interval can be defined by the users.

2. The time interval between uploading procedure to the web server.

3. The option for data uploading methods (Wi-Fi or Cellular Data). Temporary, Cellular Data functionality is disabled due to some problems in the server responses. Although the cellular data has been tested, the responses some times are lost in the network. The responses from server are crucial for the confirmation of the uploading.

FAQ In Figure 3.15 and 3.16 screenshots from FAQ section are shown. That way the users are introduced to basic concepts and terms of cellular telephony and mobile phones.

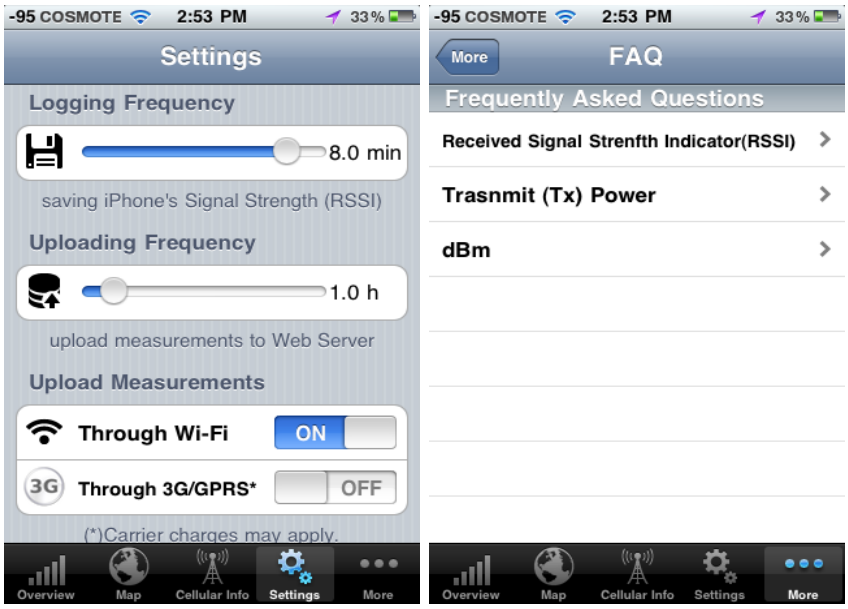

Figure 3.15: i) MySignals Settings ii) FAQ.

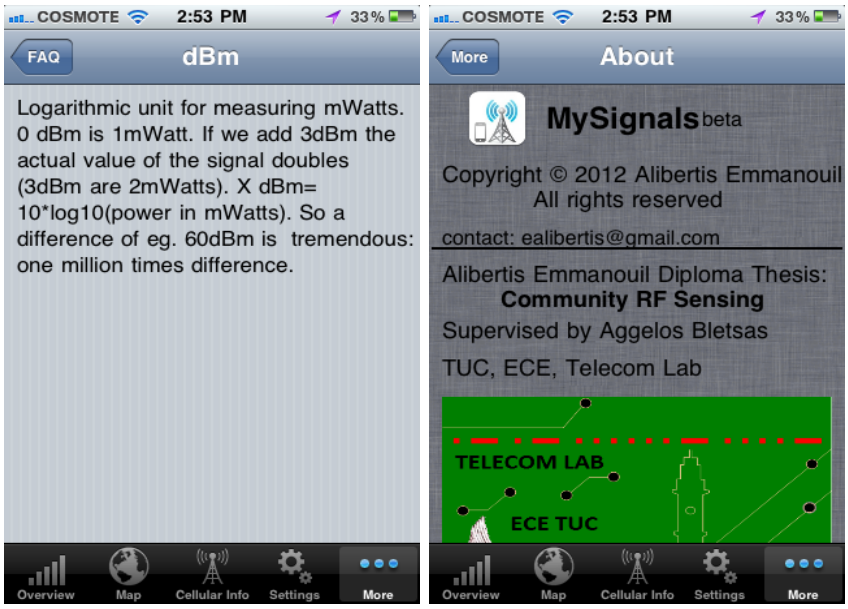

Figure 3.16: i) FAQ, dBm description ii) About MySignals.

3.2.4 Implementation Details

The concurrent operation of:

1. reading from baseband in a background thread,
2. the local caching of measurements in sqlite,
3. the uploading procedure which happens from time to time,
4. the update of the GUI, if a new reading from baseband has been arrived,

must be handled in such a way that MySignals will be a real world system for recording and uploading RSSI and cellular information. The basic programming restrictions and practical difficulties which appeared in implementation were:

1. **Core Data Restrictions**: If two threads access concurrently the Core Data object graph, then a critical section may produce inconsistency in the data and many crashes in App. These crashes happen randomly due to the parallel execution of threads. It must be ensured that someway thread collision will not occur.
2. **Baseband Restrictions:** Apart from the blocking issue of the Main Thread which is already discussed in sub-Chapter 3.2.2.2, some other technical issues concerning the baseband appeared in long-run tests of MySignals.
3. **GUI Restrictions**: Also, the update of the GUI must be implemented only in the Main Thread of application. For example, if the GUI updates happen from the background thread, that accessing Field Test, then the application will certainly crash.

3.2.4.1 Baseband Implementation Details

The most of the baseband restrictions have been discussed already. In conclusion:

- The reading from the baseband obligatory is implemented in a background thread to avoid freezing the GUI (see 3.2.2.2).

- Also, if the UMTS (3G) is enabled, baseband many time does not respond to "AT+CSQ" (At Command for RSSI), especially if the measurements recording happens in a long-run in background. Fortunately, RSSI reading from private callbacks API works always, hence this restriction does not consist a serious problem.

3.2.4.2 Core Data Implementation Details

In MySignals App there are three different threads accessing the Core Data graph.

1. Insertion of a new Measurement Entity with all the corresponding entities.

2. Extraction of measurements in order to upload data to a central web Server. Analytical details of this software part are discussed in the sub-Chapter 3.3.3.

3. Deletion of uploaded measurements after the successful submission of the measurements to the Web Server.

An approach for thread concurrency in Core Data can be applied but it needs a lot of time to be implemented. Therefore a simpler approach is chosen. Core Data is accessed by maximum one thread. This leads us to create the FIFO, as it is is mentioned previously, for Core Data insertion. The measurements extraction from Core Data and measurements deletion are also submitted to the FIFO. From the FIFO's queue can run only one thread per time. When a thread finishes, the next one starts. Thus, no crashes occur. IPhone SDK offers the NSOperation object for creating queues of threads for executing in a predefined order.

For example, if a new measurement arrives from baseband and the Core Data that time is busy (other insertion or the extraction of data for uploading is active), this measurement is inserted into FIFO and waits until its turn comes.

3.2.4.3 GUI Implementation Details: Use MVC

A Model View Controller design pattern was applied to MySignals in order to achieve clear and simple software structure. Furthermore, MVC protocol has tremendous advantages and ensures code reusability and easy upgrades of software components.

The Model View Controller (MVC) is an extremely popular software design pattern. More specifically, indicates that the View- i.e., the Screens/GUI of an Application- must be separated from the Model- i.e., the source of the data that are displayed- of the application. An intermediate software component, the Controller, must handle the communication of the Model and the View. In Figure 3.17 the general architecture of MVC applied on MySignals is shown.

The model is completely separated from the MySignals GUI. The model in our case is the object which runs on background and fetch the Field Test variables from baseband. Each screen of MySignals has a controller class which can observe the changes in the Field Test variables using a KVO (Key Value Observing) protocol which is provided by iPhone SDK. Hence, if a change is detected in Model, the controller will update the GUI. A small but important detail must be underlined in this point. The object which fetches data from baseband, is running on background thread. Therefore, if Controllers observe the Field Test variables from this thread, the GUI will be updated on a background thread and finally the application will crash. As it is mentioned, GUI handling must be implemented **only** in Main Thread. Thus the background communication thread with baseband, copies all the variables to a Main Thread's object.

This approach makes the implementation code better organized. Each object has exact responsibilities and the maintaining of the code is easier. Also, all the Screens of MySignals "observe" -i.e., use KVO- the same model object for getting values updates. Thus, code reuse was achieved. In future versions of MySignals probably the private CoreTelephony callbacks will be further used since baseband seems inaccessibly for iPhone 4S, but this will not affect the GUI screens. The model fetches and keeps the data, the GUI

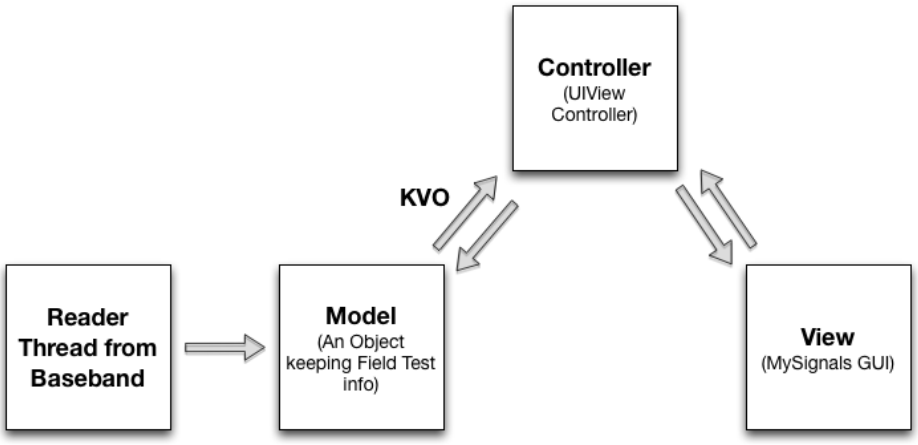

Figure 3.17: The MVC software pattern applied on MySignals App.

just display them. Also, a completely new method maybe will be discovered in the future, for accessing Field Test Mode. If this happens, only the Model object will be changed and GUI source will remain the same with some minor changes in controller.

3.3 MySignals: Web Server - Database

3.3.1 Users Privacy

Someone would think that MySignals violates user's privacy, due to the fact that collected in central database RSS data are connected with user's locations. However, this hypothesis is not valid since MySignals follows a process of saving the data which definitely secures users privacy.

On the other hand, this thesis would like to examine a time based analysis from a specific iPhone. Also, in the case of iPhone 4 were noted signal receptions problems known as "antennagate" [60]. For all these reasons and several more, it is necessary to distinguish the RSS measurements between iPhones participating in MySignals in order to perform an entire RSS analysis and evaluation of several parameters as the examples.

The measurements from a specific user is paired with a unigue and ran-

Figure 3.18: Creation of the Unique, anonymously Identifier for each user.

dom identifier. This iPhoneUID derives from the MD5-hash the iPhone's Mac address. More specifically, Mac Adress is a unique identifier in every Wi-Fi card, which is not public available. Additionally, it is not correlated with the user's name or other personal information. Moreover, Mac address is only visible in the user's local network and not to the entire Internet. Further, the identifier produced by MD5-hash needs an extremely time consuming algorithm to be hacked in order to get the Mac Address. For the above reasons, even if Mac Address is retrieved it is a completely useless information. Thanks to MD5-hash, MySignals respects user's privacy and does not save any user's personal information. The MAD5-hash is produced in user's iPhone and therefore original Mac Address is not visible from MySignals. In Figure 3.18 is demonstrated the approach which is implemented. Further information about privacy and Mac Address can be found on this article [61].

3.3.2 The concept of Web Service

At the beginning, several considerations must be discussed in order to determine the approach used of the uploading procedure of collected data from an iPhone users.

First of all, it is completely wrong to insert data to a central Database which is somewhere hosted in the Internet, directly from a remote mobile device. This gives the "key" of your database to a candidate hacker. A Database is extremely vulnerable if anyone mobile device can access it, or in other words any IP address can access it. Using this approach, the password of the database obligatory exists in MySignals App. The password can easily be discovered by a hacker just by "sniff" the tcp/ip connection of the

iPhone with the central database. Apart from password, the queries and the ER model can be easily extracted. In general, there are several other disadvantages of this approach.

This lead us to create a Web Service which will be responsible for inserting all the collected measurements by iPhones users to the database. As it is shown in Figure 3.1, each iPhone participating in MySignals will communicate with the web server, submit there the data and finally data will be inserted into the central database by the web server. This approach is called a Web Service with Rest API.

For data uploading from iPhone to the web server, JSON format will be used for packetizing the collected measurements. These measurements in JSON format will be submitted through POST variable of HTTP protocol. It would not be an acceptable approach to design a communication protocol from the scratch while solutions are out of the box ready for inter-platform communication. JSON is a lightweight data-interchange format that allows data to be packed into objects in plain text-readable format, as it is indicated in a simple, general purpose, example in Figure 3.19. It is considered as a lightweight alternative of XML. Therefore, packetizing data objects to JSON or extracting saved objects in JSON, is a straightforward process which is supported by the most of programming languages and platforms. Thus cross-platform communications are achieved, as our work demonstrates: iPhone device using JSON, submits data to a PHP server which finally saves data to MySQL server.

3.3.3 From iPhone to Web Server

Many steps are required in order to upload data from the iPhone to the web server. The Core Data objects cannot be converted directly into JSON format since Iphone's SDK does not contain APIs for conversion Core Data to JSON. Therefore, a custom conversion method must be implemented. The steps for converting the Core Data Object Graph to JSON format are summarized bellow:

1. The CoreData is converted to NSDictionary using a custom "explo-

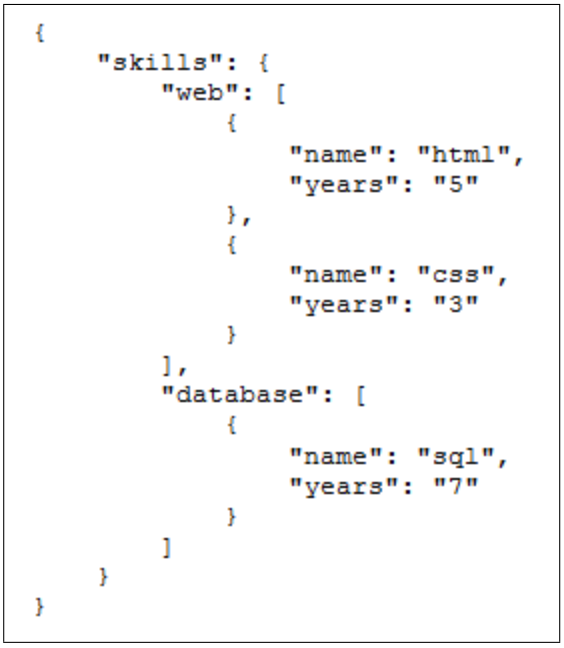

Figure 3.19: A simple JSON example for packetizing objects in plain text.

ration" algorithm of Core Data's object graph. All the measurements coming from baseband will remain and wait inside FIFO's queue, as it was discussed.

2. NSDictionary is converted to JSON format using the JSONkit Library [59].

3. Submit JSON string to the web server as a POST variable through HTTP Protocol. IPhone SDK provides the NSUrlConnection for implementing asynchronous -i.e., App does not block- http connection.

4. Wait for the web server to respond. If the connection succeed then the measurements which were uploaded to the web server, are deleted from the local iPhone's cache. If the connection fails, the data will not be deleted, in order to try to submit them later.

5. Finally, the measurements waiting in FIFO's queue will be served from now on.

6. The PHP Web Server will accept the JSON string. Further details will be discussed.

In Appendix 2 is demonstrated an example of extracted JSON string from MySignals, ready for uploading to Web Server. The packetizing of the data into JSON is straightforward and follow exactly the same logic as in the Core Data Schema 3.5 -i.e., the Core Data Schema (and the relationships) is packetized directly into JSON. All the relationships of the Core Data are included in the JSON as object's attributes. Thus, the LAI is the root of the uploaded measurements. A LAI has many cell towers -i.e., Cell Tower objects are encapsulated into LAI to the JSON string- and a Cell Tower has many RSS measurements -i.e., measurements objects are encapsulated into Cell Towers objects to the JSON string. Similarly the Location object (and the remaining entities) is encapsulated into Measurement object in JSON.

3.3.4 Web Server

The Web Server is hosted by Network Operation Center (NOC) at TUC on a Ubuntu Server machine. The server is on-line 24h/7d since it is installed on a UPS supported Data Center. Apache 5.0 HTTP server, PHP server and MySQL server were installed for supporting MySignals Web Service.

The server side of the web service is implemented in PHP language. For each new incoming HTTP connection, the measurements in JSON format, the iPhone UID and model are retrieved from the POST Variables of the HTTP Connection. Parsing of the JSON string is achieved using the available PHP functions. The JSON string is straightforward itself and give us the structure of the arrived info. As it is discussed above, PHP server can extract objects packetized in JSON and insert all the data to MySQL database (see Appendix 2 for the JSON submitted from the iPhone). The extraction of data from JSON is supported by a official PHP library. If the extracted LAIs and Cell Towers does not exist in MySQL DB are inserted into. All the measurements are inserted into the relative table with SQL insertion queries.

3.3.5 ER Database Schema

In Figure 3.20 the ER (Entity Relationship) schema is displayed. The schema organization represents the logic of the recorded Measurements and follows the organization of the Core Data schema. For a better schema maintenance, GSM and UMTS measurements are seperated to the relative Entities. The foreign keys which are shown in schema have been defined in MySQL environment to ensure data integration.

3.4 MySignals: Web Site - Heatmap

The display method of the mobile coverage maps is a heatmap, a map in which RSS are displayed using an appropriate color code. This is intuitively conceivable from the most of the people. A color coding representation is universal and everybody would easily understand the evaluation of the rssi. For example, red color shows strong signal while a purple color shows a weak signal.

A simple heatmap engine was constructed by Patrick [62] and is available under the "MIT and the Beerware license" [63]. Heatmap is generated using HTML5 canvas library and is attached to Google map. MySignals heatmap engine is a modifiified version of the above heatmap and was developed for displaying the RSSI measurements to their relative positions. Appropriate PHP and javascript scripts for fetching RSSI and location data from MySQL database was written and attached to this engine, as shown in Figure 3.21.

At the data fetching script, a simple RSSI aggregate algorithm was implemented. If several RSSI (by the same network carrier and network Type) are available for a specific location -i.e., the same coordinates, the average of this RSSI is estimated. Unfortunately, the a-GPS almost always has errors. Even under the best circumstances (mobile being outside and having line of sight communication with a satellite), the error is at least several meters and may reach dozens of meters. Indoors the error may be greater. The GPS API provides a "horizontal accuracy" variable which determines the radius of uncertainty for the location, measured in meters. Unfortunately, "hori-

zontal accuracy" variably is inaccurate. It was observed experimentally, that many times the horizontal accuracy given by GPS API was unreasonably high, while the provided position from GPS was accurate and was pointing the user's location with a small error. Thus for avoiding losing many measurements, an upper bound threshold for horizontal accuracy was chosen experimentally at 450 meter. It seems that this value has usually actual error smaller than 100 meters and many times even lower than 30m. Many good measurements would be lost if a very strict threshold (e.g., 40m) was chosen. Concluding, if the horizontal accuracy of a measurement is greater than 450m, the measurement is rejected and it is not displayed in heatmap. Further discussion about GPS accuracy will be done in MySignals Evaluation Chapter 4.

The heatmap engine currently supports with satisfactory speed approximately 10000 points of coordinates on map. In the case of map being zoomed out, many RSS stamps are aggregated in a particular area. Hence, the analysis of the RSS stamps is not clear (only red color is visible). In order to be displayed with accuracy the color of the RSS stamps, map in the area of interest must be zoomed in. This is obvious in the examples which are demonstrated in Chapter 4. In addition filtering of RSSI based on Network carrier and network type are provided as it is demonstrated in the web site demonstration screenshots in the following Figures 3.22 and 3.23.

RSSI	**Qualitative Level**	**Color Coding**
$RSSI > -55$ dBm	Best, Perfect Signal	Red
-55 dBm$< RSSI < -65$ dBm	Excellent Signal	Yellow
-65 dBm$< RSSI < -75$ dBm	Very Good	Green
-75 dBm$< RSSI < -85$ dBm	Good Signal	Cyan
-85 dBm$< RSSI < -95$ dBm	Moderate Signal	Open Blue
-95 dBm$< RSSI < -105$ dBm	Weak Signal	Purple
$RSSI < -105$ dBm	Worst Signal	Transparent Purple

Table 3.8: Color coding for RSSI values

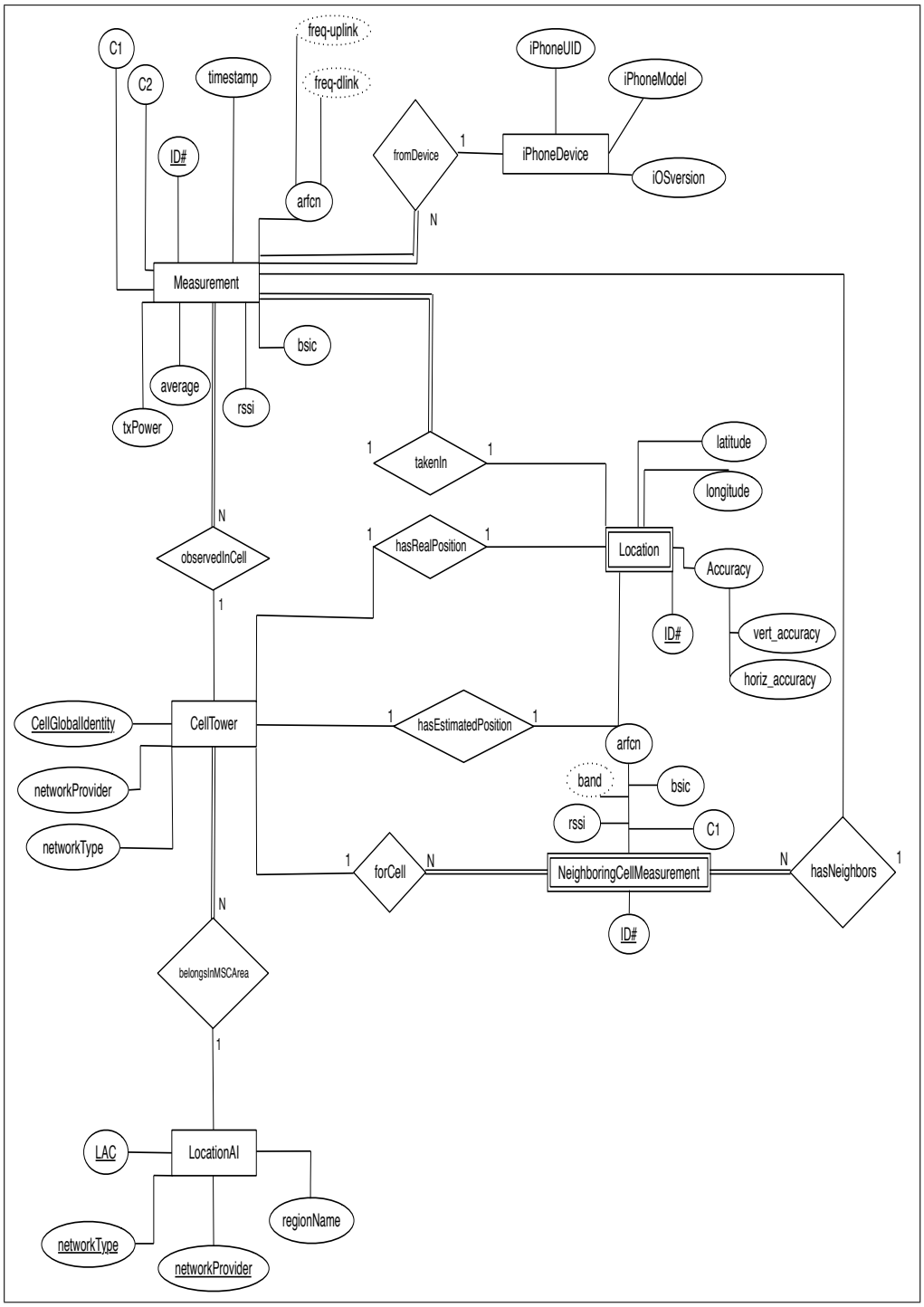

Figure 3.20: The ER relational schema of MySignals DB.

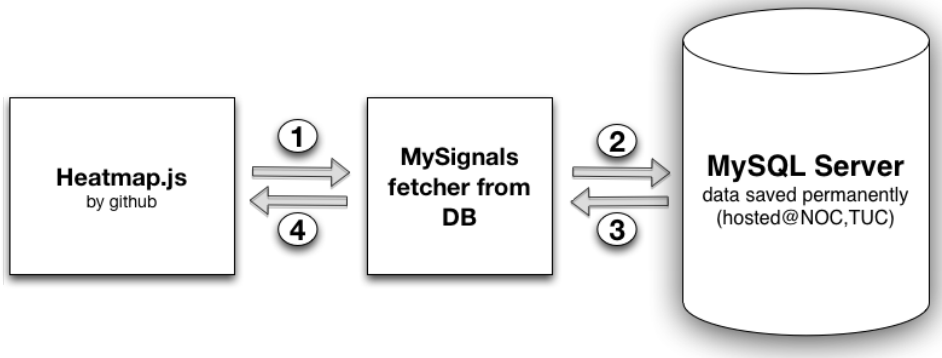

Figure 3.21: MySignals heatmap engine for displaying mobile coverage maps.

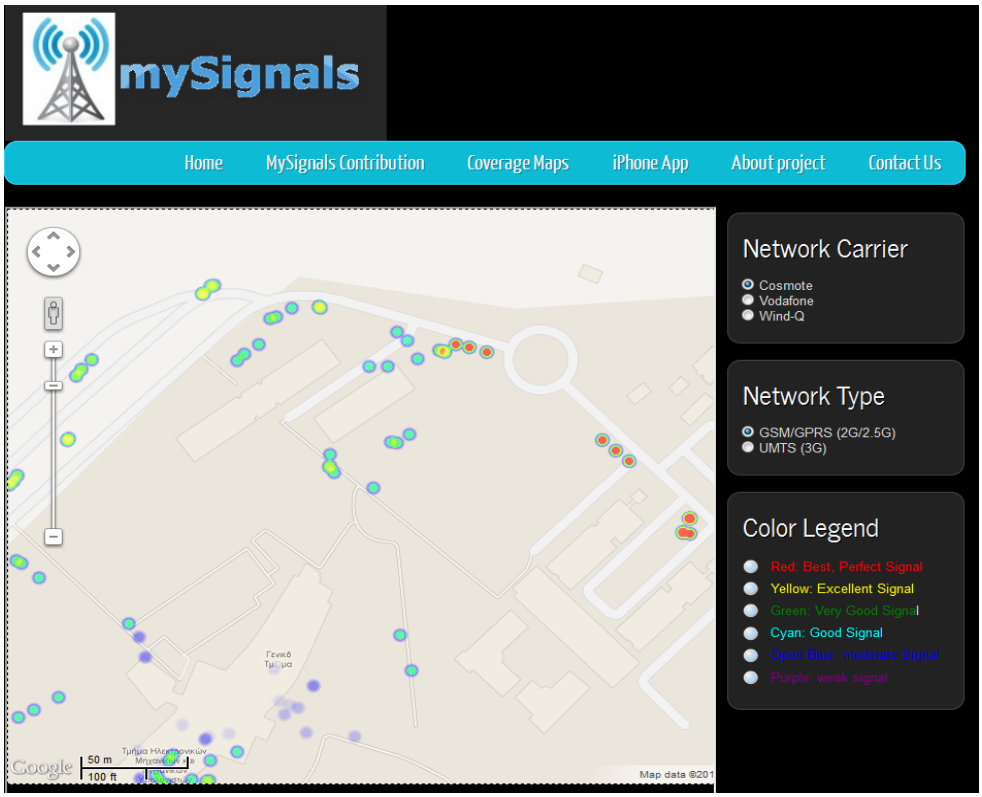

Figure 3.22: MySignals website demonstration. User can choose from filters the Network Carrier and Network Type.

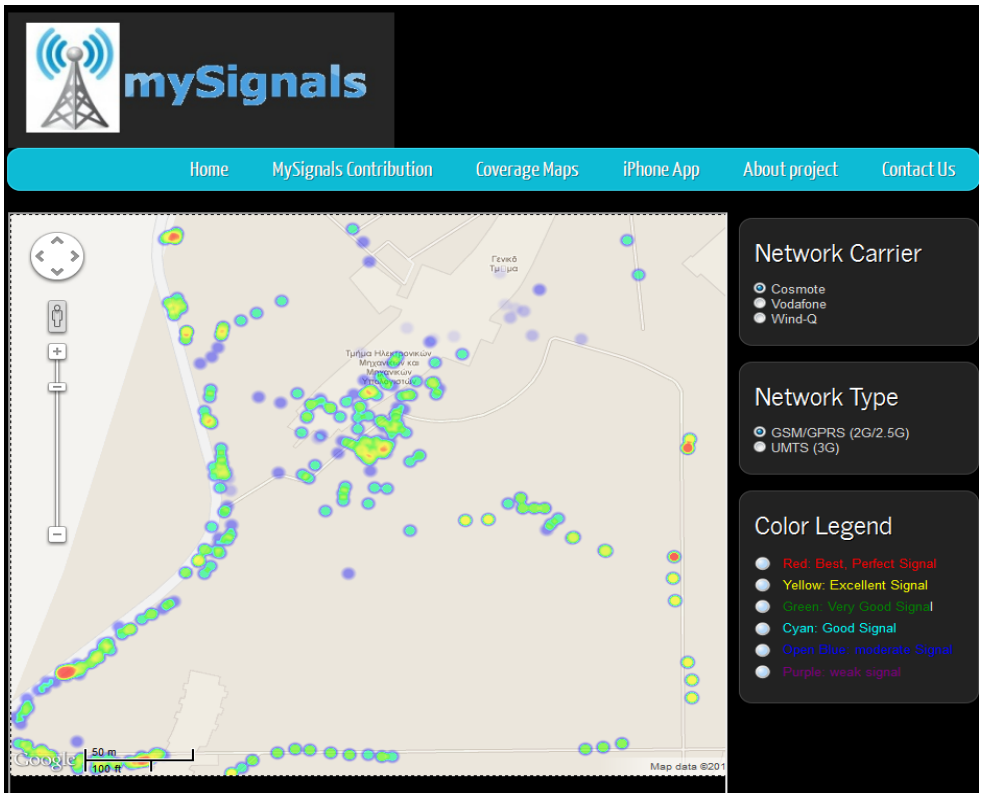

Figure 3.23: A snapshot of Cosmote GSM network at TUC Campus.

Chapter 4

Evaluation of MySignals

4.1 Testing and Debugging Platform with real iPhone Users

Installation of MySignals App in real iPhone users was necessary, in order to fulfill the purpose of this thesis which was creating a mobile coverage map from users themselves. Many difficulties and bugs were encountered during the installation of MySignals on real users due to iPhone's baseband fragmentation and incompatibilities between iOS 4 and iOS 5. A general review of supported iPhone models and iOS versions from MySignal is summarised on table 3.4.

Baseband's socket port of iPhone 4 has to be granted with administrator rights (from ssh terminal) after a hardware reboot, in order to work with At Commands and take measurements. This was a great downside but unfortunately there was no other approach since iOS does not allow system commands from user's program. An appropriate script was given to user in order to run it from terminal every time the iPhone was reboot.

Moreover, some users did not have their iPhone Jailbroken or even had older iOS versions than 4.0 which is the minimum required by MySignals. Therefore the appropriate updates and Jailbreaking was applied. Also manual installation of MySignals for each user was preferred, instead of releasing it as a package on Cydia Store. Finally, during the first installation steps , a severe iOS 5 bug was discovered while on the other hand iOS 4 was totally functional. Particularly in iOS 5, Core Data was saving the cell-IDs as negative numbers even though they were provided correctly. In order to avoid this problem, cell-IDs were saved as strings in Core Data since the problem could not be determined.

All the above problems indicate that when real world applications and software are being applied in practice, bugs, problems and inconsistencies appear unexpectedly, even if applications have been thoroughly tested. This is due to the amazing complexity of the nature of technology.

Battery performance

Battery performance is one last point which must be underlined. MySignals runs in background and records RSSI measurements with their respective location and network information. This happens only if MySignals is registered in iOS [i] for location updates [ii] which means having the GPS module continuously open. Otherwise the Application will be banished and "killed" after 10 minutes of execution in background [iii]. If the location manager -i.e., the GPS module, of iPhone is closed by MySignals in the interval between two measurement for battery saving, then MySignals will be immediately "discovered" and killed by iOS. Therefore, MySignals is executed in background for more than 10 minutes, only if GPS module is continuously opened. This leads to very poor battery performance. MySignals drains a fully charged battery after approximately 8 hours. This is definitely a great downside but unfortunately it cannot be solved to the day since it is a restriction of the mobile operating System. A solution to this problem will be investigated in a future version of MySignals.

4.2 Evaluate Measurements and Network Behavior

4.2.1 Statistics for Collected Data

Over 42000 cellular telephony stamps (RSSIs with their corresponding location and cellular information) have been collected for over 3 weeks from seven iPhone users at Chania City and Athens City. Certainly the nubmer

[i] More specifically, in info.plist file are written all these Application runtime and "build"-linking settings

[ii] (one of the 4 allowed Background running modes of iOS)

[iii] This is part of Apple's policy for better resource management.

iPhoneUID	iPhone Model	iOS Version	Network Carrier
22223276 ···	iPhone 3GS	4.2.1	Cosmote
51063500 ···	iPhone 3GS	4.1	Vodafone
7023889b ···	iPhone 4	5.1.1	Cosmote
7cbc37da ···	iPhone 4	4.3.3	Cosmote
8fb4fd3d ···	iPhone 3GS	5.0.1	Vodafone
a841f74e ···	iPhone 3GS	4.2.1	Cosmote
bba30992 ···	iPhone 3GS	5.0.1	Vodafone

Table 4.1: iPhone Users participating in MySignals Evaluation.

iPhoneUID	Network Carrier	No. Meas. (GSM)	% accepted $accur_{gps} < 450m$	$RSSI_{avg}$ iOS API	$RSSI_{avg}$ AT+CSQ
22223276 ···	Cosmote	4379	57.7%	-79.9 *dBm*	-76.8 *dBm*
51063500 ···	Vodafone	112	99.9%	-82.1 *dBm*	-76.5 *dBm*
7023889b ···	Cosmote	3713	75.9%	-79.3 *dBm*	-77.6 *dBm*
7cbc37da ···	Cosmote	11007	58.0%	-74.0 *dBm*	-72.4 *dBm*
8fb4fd3d ···	Vodafone	2030	68.0%	-93.8 *dBm*	-91.7 *dBm*
a841f74e ···	Cosmote	18773	82.3%	-77.8 *dBm*	-75.8 *dBm*
bba30992 ···	Vodafone	2407	94.8%	-75.5 *dBm*	-72.8 *dBm*
Total	**42777 Measurements**		**72.5%**	**-77.9** *dBm*	**-76.5** *dBm*

Table 4.2: Statistics summary for the collected data for GSM network.

of collected measurements would be greater if there was not a limitation by GPS in battery performance. More specifically, the users were obligated to close MySignals App to avoid draining their battery quickly. The participating users and their respective iPhone models and iOS versions are shown on table 4.1. A statistics summary of the collected data is shown in table 4.3. The first fact that one could observe is that the overwhelming majority of the measurements comes from GSM network and not from 3G networks. This indicates that users prefer GSM network instead of 3G (UMTS) in order to save battery and money. Users will be charged by using 3G network if they do not have a cellular data package. Also, the percentage of the accepted measurements due to the 450m threshold in GPS horizontal accuracy is presented, which is explained in sub-Chapter 3.4.

Considering the GSM collected data, several conclusions can be drawn. Firstly, the 28% of the collected measurements are rejected due to the GPS

iPhoneUID	Network Carrier	No. Meas. (UMTS)	% accepted $accur_{gps} < 450m$	$RSSI_{avg}$ iOS API
22223276 ···	Cosmote	0	-	-
51063500 ···	Vodafone	179	29%	-94.5 dBm
7023889b ···	Cosmote	0	-	-
7cbc37da ···	Cosmote	0	-	-
8fb4fd3d ···	Vodafone	38	57.0%	-85.7 dBm
a841f74e ···	Cosmote	1821	61.5%	-90.1 dBm
bba30992 ···	Vodafone	0	-	-
Total	**2038 Measurements**		**58.0%**	**-89.5** dBm

Table 4.3: Statistics summary for the collected data for UMTS network.

accuracy threshold, although this threshold is not strictly defined. It was experimentally observed that sometimes when the App was running in the background and the iPhone was locked, the a-GPS accuracy uncertainty was rose from meters to even kilometres. Probably, in these cases iOS did not activate the GPS module but it was using the Wi-Fi - Cell Tower triangulation for localization. The latter usually finds the location with a larger error, leading to a high a-GPS accuracy uncertainty. Either iPhone could not active GPS module due to lack of battery, as it was observed experimentally, or it could not connect to satellites to get accurate coordinates. Also, a-GPS has a small error even under the best conditions. Unfortunately, despite all these downsides there is no other way to determine the RSSI's location. Some other observations are discussed in RSSI space analysis sub-Chapter.

Secondly, from the comparison of the two measuring methods of RSSI (iOS private APIs and AT+CSQ command) the following can be derived:

- Private RSSI API seems to be an average of the RSSIs provided by AT+CSQ, in a specific time frame, in which the RSSIs are provided instantaneously. Interestingly, the $RSSI_{avg}$ reaches the $RSSI_{avg}$ by AT+CSQ when the number of measurements increases. Probably with hundreds of thousands of measurements the values will be equal.

- In the case of the user "51063500" who submitted only 112 measurements the difference of 5dBm between the two methods is expected

since AT+CSQ command is not accurate for a short time frame and few measurements.

- The most important is that iOS source code is not publicly available, therefore the exact parameters of the mechanism of iOS RSSI calculation, such as the exactly time frame, are not accessible if iOS rejects outlier RSSIs from baseband etc. Thus, the difference of 1.4dBm $\approx$ 1dBm for all the measurements in the collected dataset is not of grave importance.

UMTS dataset is not worth mentioning since collected measurements are very few.

4.2.2 RSSI analysis over Time and Space

Since the measurements from COSMOTE GSM network were the majority of collected data, the evaluation of MySignals over time and space was performed using this dataset.

Analysis over Time

As it has already been discussed in the Introduction of this thesis, RSS for a Cellular Network is changing continuously due to many reasons. One common reason for this is that the BTS transmitted power is dependent to the network's status which is changing during the day. This practice is called "GSM Power Control" and it was already mentioned in sub-Chapter for transmit power Data Interpenetration 3.2.3.1. For example, usually RSS differs between morning and night for a fixed location. In order to study this effect, RSSI over time has been plotted for one specific location. A specific user was asked to leave MySignals open for several hours and different time periods during the day at the same place. For locating measurements at users fixed locations, appropriate filtering in MySQL database was applied.

In Figure 4.1 location stamps from a specific user at a specific location are shown. Definitely, the a-GPS error can be observed, since all the measurements are from a fixed location (probably user's home). Unfortunately, a-GPS error is inevitable and extended research is needed for filtering it out.

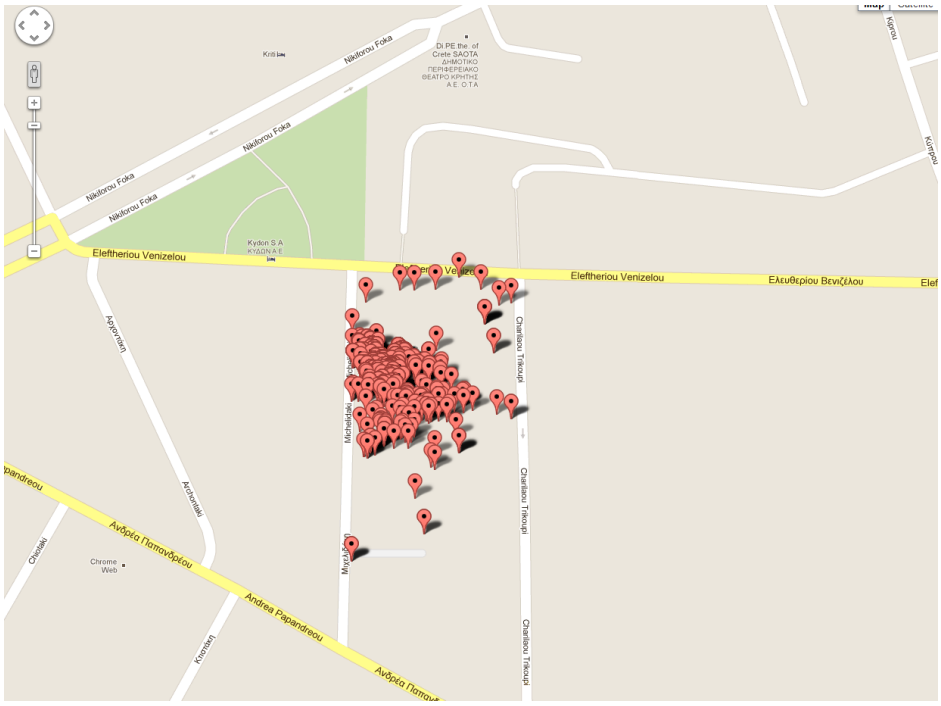

Figure 4.1: Location Stamps observes from a specific user at a fixed location. The reader can clearly observe the iPhone's GPS errors since measurements refer to a specific indoor area.

In Figure 4.2 RSSI values from the above locations, are plotted during 20:00 PM and 14:00 PM of the next day. Since the user was in a fixed position and the measurements are overnight, the iPhone is surely stationary and also connected continuously to the same BTS -i.e, the same cell-ID is observed-, GSM Power Control effect can be observed. The RSSI value is changing from time to time.

Analysis over Space

The evaluation of the collected data over space, leads to very interesting observations, since a well known area with very poor signal quality in Chania was discovered by MySignals community coverage maps. More specifically, this area is the Akrotiriou turns on the road from Kounoupidiana to Chania. The mentioned area is shown in Figure 4.3. It is an common observation that in this area, the signal is so poor that leads to a call failure. The

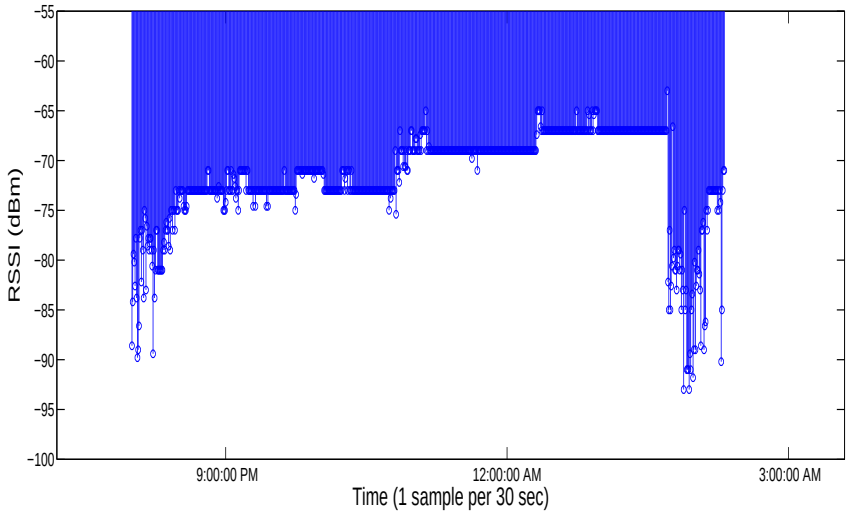

Figure 4.2: RSSI VS. TIME from a specific user at a fixed location. This comparison strongly demonstrates the results of GSM Control Power.

route from Chania to Kounoupidiana, as it is observed in the demonstrated example, has areas with good or moderate signal, but the marked area has the lowest possible (very transparent purple) signal. MySignals coverage maps intuitively demonstrate the areas with very poor signal coverage. This indicative example was chosen since it is one of the most known area in Chania where someone has dropped calls and very poor coverage. Several other regions with poor signal are visible on the map.

Another example for the evaluation of MySignals over space, is demonstrated in Figure 4.4 which displays the TUC campus. At the upper right corner (road next to the Mineral Engineering Department) excellent rssi readings are displayed (deep red color) while the rest rssi measurements have good (yellow color) or weak value (purple) or very weak (very transparent purple). This is absolutely expected since line of sight communication with a BTS is achieved in the road next to the Mineral Engineering Department. More specifically a BTS is installed next to the church of Kounoupidiana which is visible from the road and no obstacles interfere between the BTS and the Mineral Engineering Department.

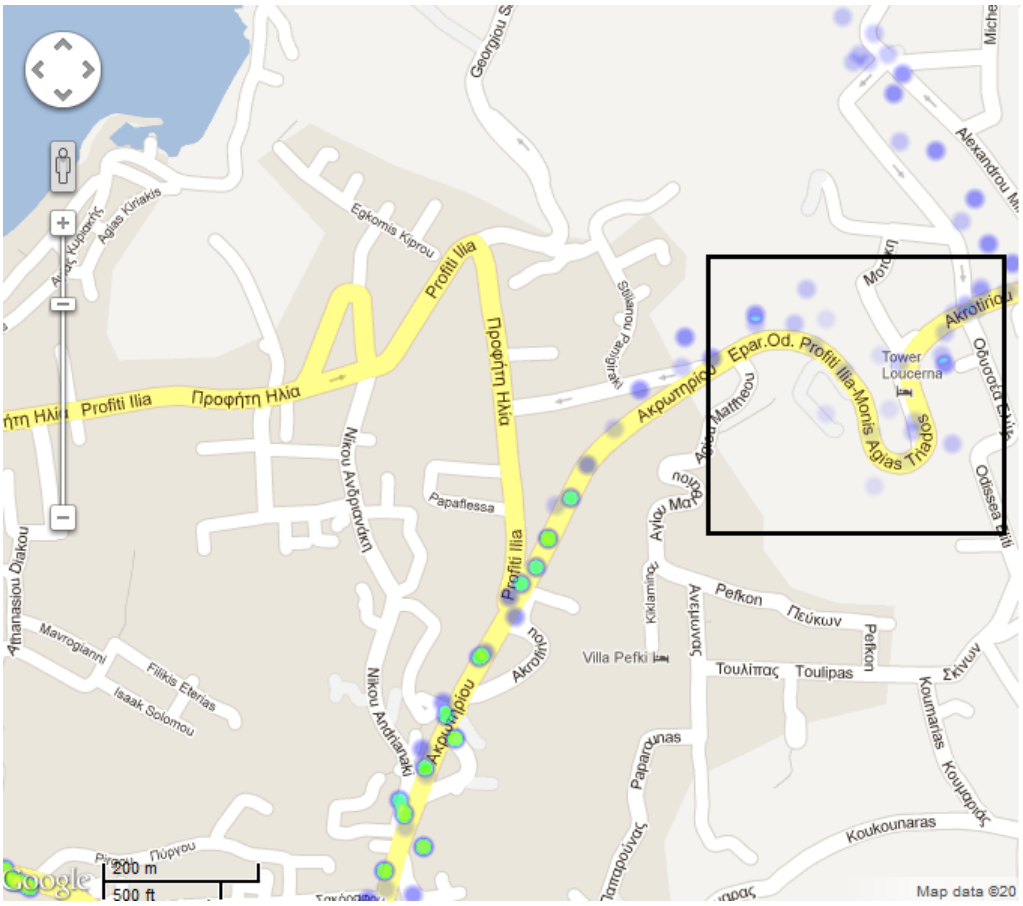

Figure 4.3: Akrotiriou Turn: Poor signal region discovered by community mobile coverage maps.

Several other examples are demonstrated in this section. In order to be able to see the measurements with their exact resolution, the users must zoom in due to the fact that heatmap engine aggregates measurements if the map is zoomed out, as it is shown on examples. In Figure 4.5 a covered region in Rafina, Attiki is shown, beginning from panoramic view and ending in a full zoom resolution. In Figure 4.6 a panoramic view of Chania City is shown, demonstrating that RSSI measurements that have been collected at a big variety of regions. In Figure 4.7 a snapshot of Chania centre and old harbour is shown. In order to get better resolution and see the exact rssi color code values, in Figure 4.8 two well known places with cafe/bars at

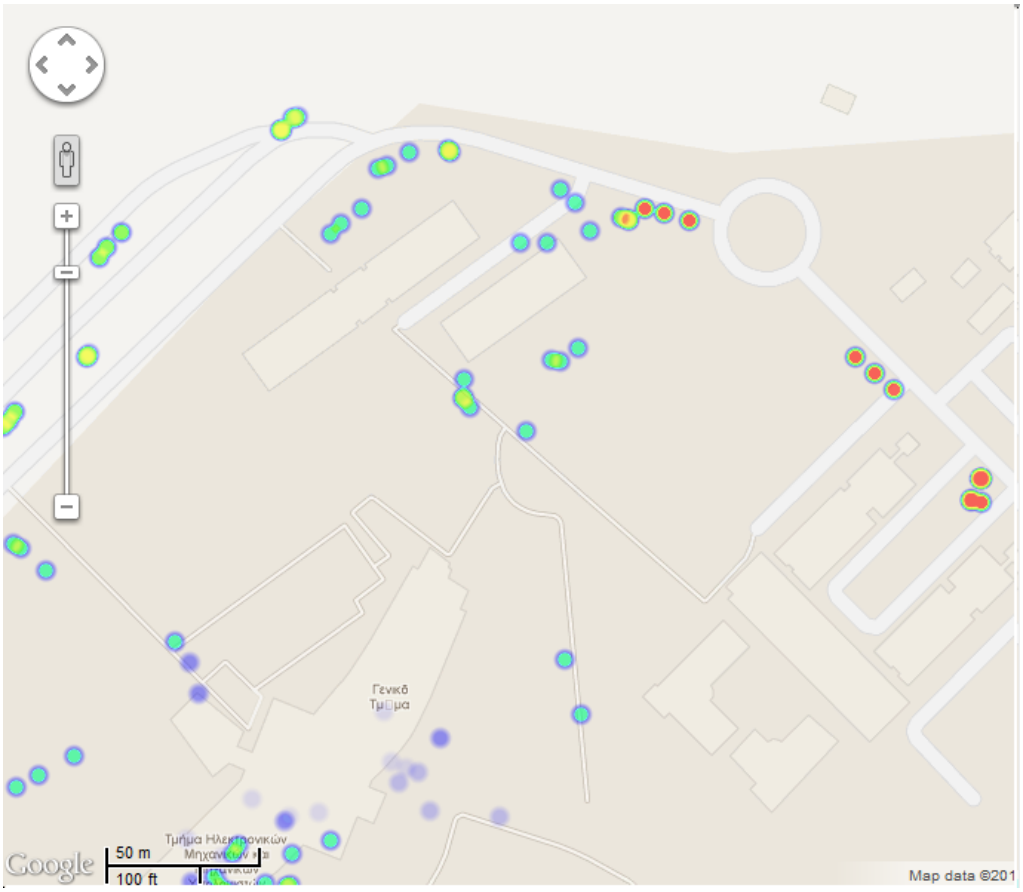

Figure 4.4: A snaphsot from TUC campus. Excellent signal is discovered at Mineral Engineering Department, while at ECE building the signal ranges from moderate to weak.

chania are shown. Users were frequently visiting these places, therefore a lot of measurements have been recorded there. The GPS errors are perceivable in the above examples. For example, measurements on the sea surface is clearly due to the GPS error. Probably this outdoors measurement , has a very good GPS accuracy but it continues to be inaccurate for some meters (the measurements was taken on Cafes/Bars on Old Harbour jetty).

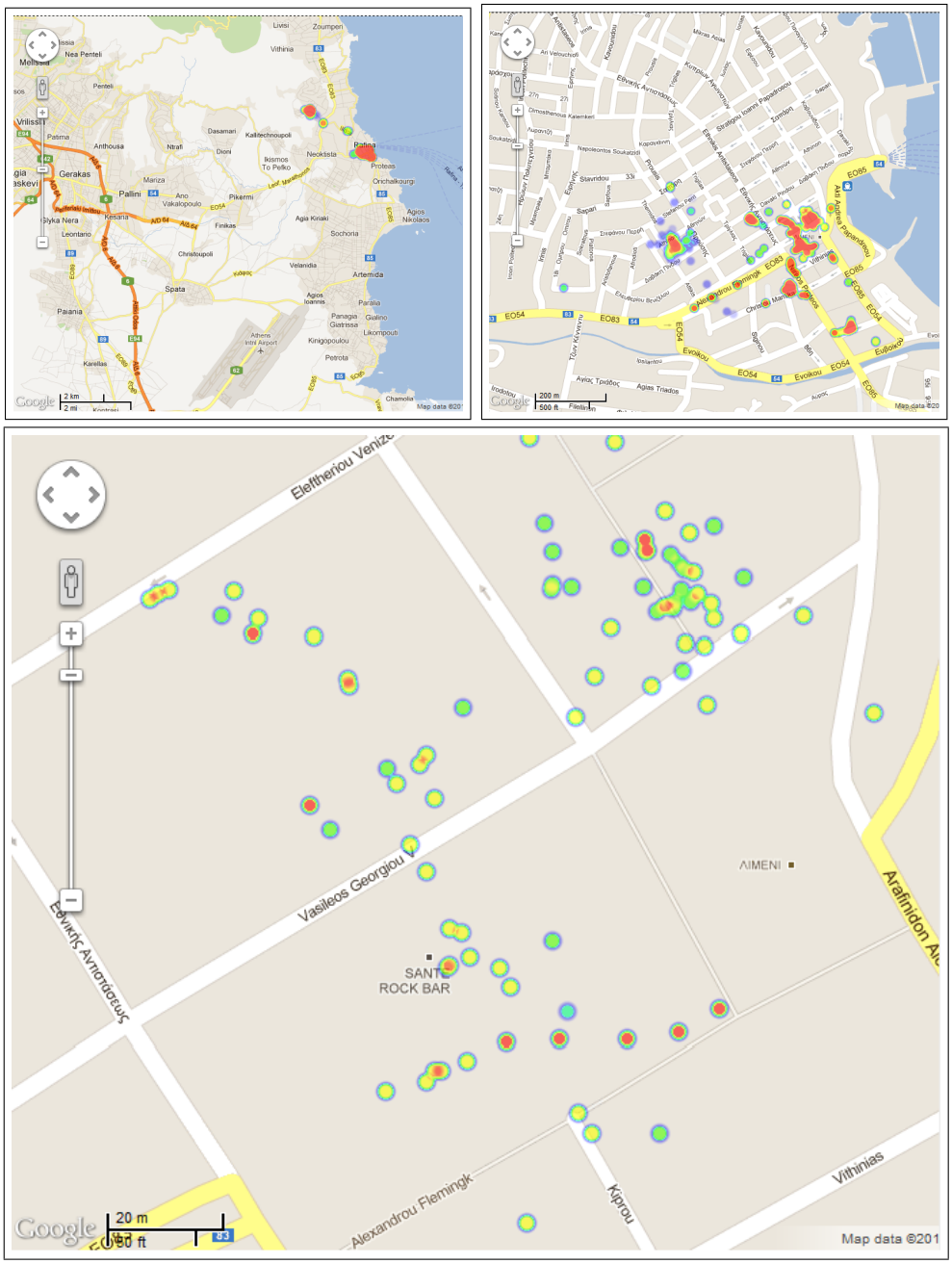

Figure 4.5: (starting from the upper left corner) i) Zoomed out: measurements are aggregated and giving only red color over covered regions. ii) Zooming in: the measurements become more clear. iii) Clear color code representation of recorded measurements. GPS error are perceivable by the reader.

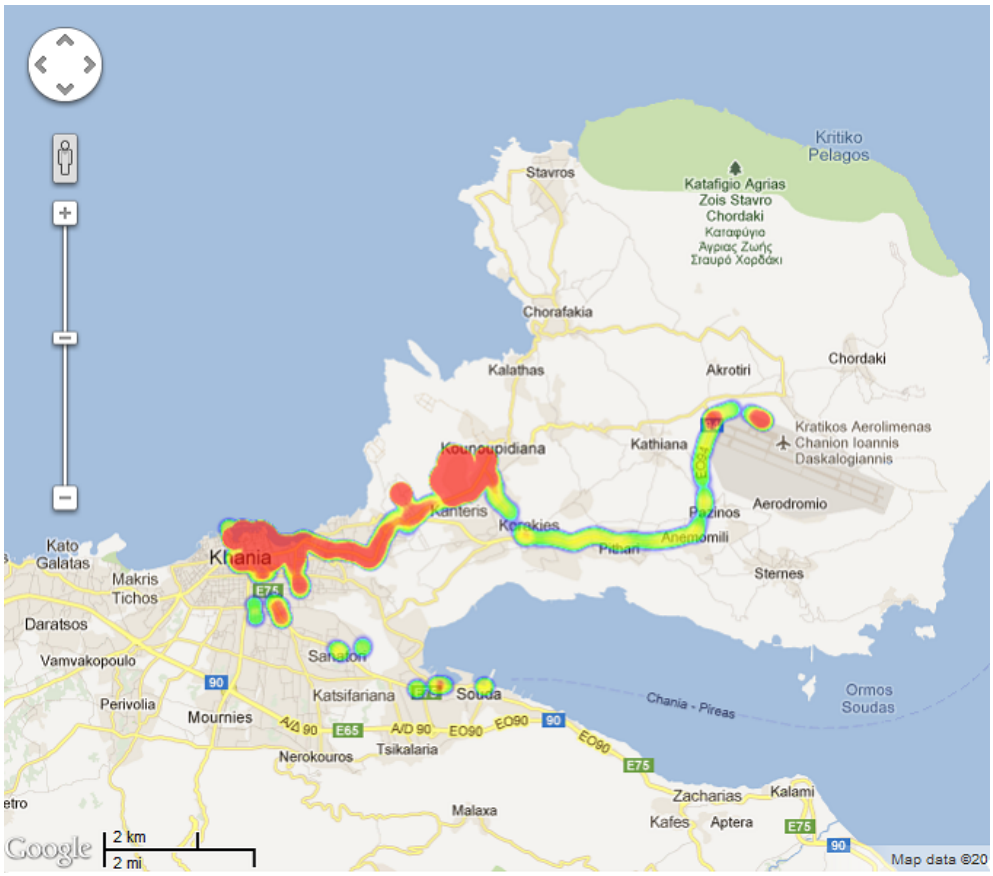

Figure 4.6: Chania City, Panoramic view.

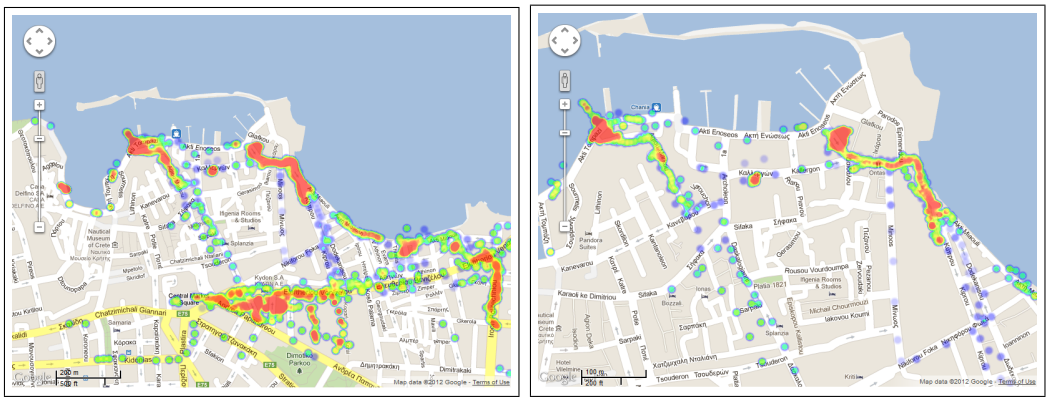

Figure 4.7: i) Chania Centre and ii) Old Harbour.

Figure 4.8: Old Harbour and centre of Chania: zoomed in for exact color resolution. i) Palace, a Cafe/bar at Old Harbour jetty. ii) Cafe/bars, commonly known as "Stenaki".

4.3 Future Direction: Discover a Cell Tower Location with Particle Filters

4.3.1 Dynamic Bayesian Network and Particle Filters

During the implementation of this thesis an idea was born for exploiting the collected data. The motivation derived from the fact, that Cell Tower positions are unknown and unlisted apart from few exceptions. It would be a great opportunity to discover a Cell Tower Location using the collected measurements from the community. The RSSI give information for the distance between the BTS and the mobile phone. However this reflection comes with extremely high noise due to scattering, GSM Power Control etc. It is extremely difficult to be modelled due to all these factors.

The problem of the Cell Tower Localization could be modelled with a Dynamic Bayesian Network [64], as it is shown on Figure 4.9. The filtering for getting $P(\overline{X}_{tower}|\overline{RSSI})$ is performed with Particle Filters (PFs). The algorithm, implementation details and an extend dicussion for PFs can be found on [65].

In order to investigate if Particle Filters are able to give us the Cell Tower position, a mapping scenario was simulated. GPS inaccuracy is set equal to zero and the error sensor model for the RSSI observation, was modelled as

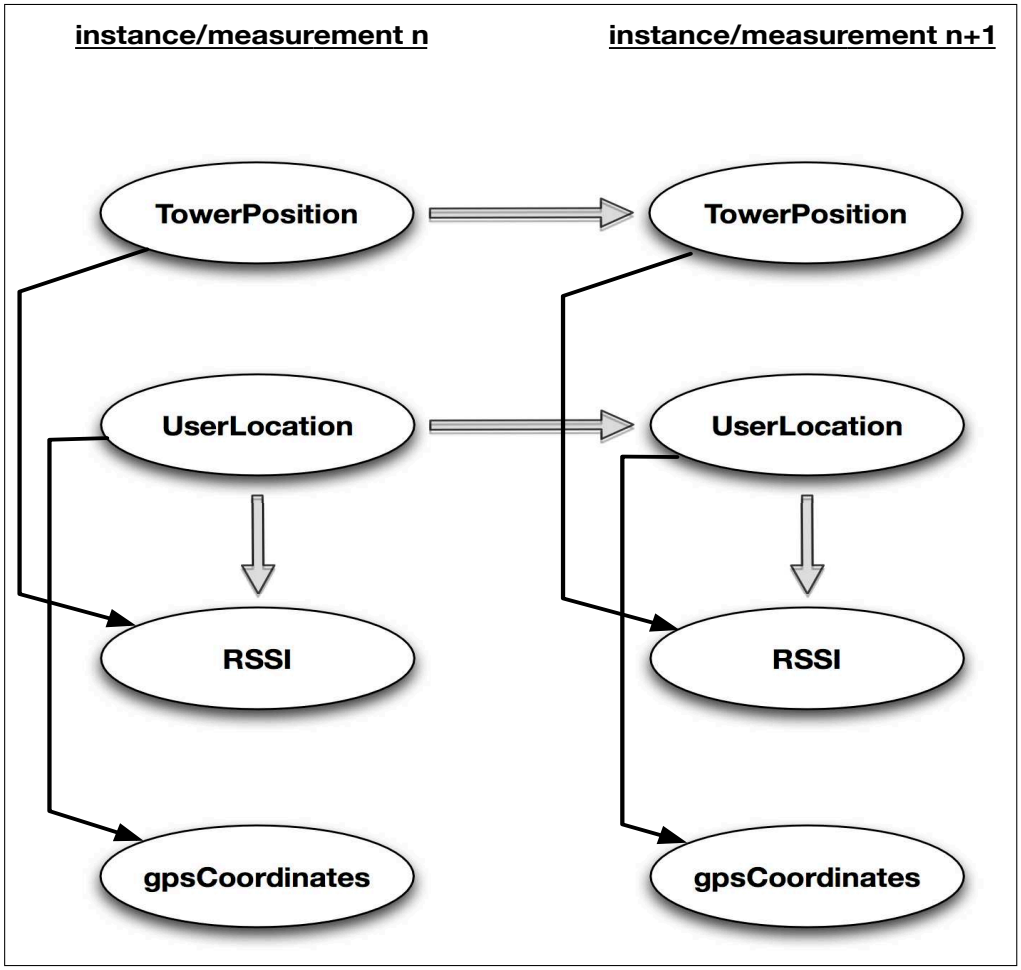

Figure 4.9: Dynamic Bayesian Network for discovering Cell Tower Position. Tower Position and UserLocation are the State Variables. RSSI and gpsCoordinates are the observation from the "sensors".

a log-Normal distribution, as [66]. The two devices that are communicating are marked with i,j:

$$P_{ij}(dBm) \sim N\left(\bar{P}_{ij}(dBm), \sigma^2_{dB}\right)$$

With:

$$\bar{P}_{i,j} = P_0(dBm) - 10n_p log_{10}(d_{i,j}/d_0)$$

where, $d_{i,j}$ is the euclidean distance between i,j and P_0 is measured in a distance d_0 from the transmitter.

The density function of the received power in watts is :

$$f_{p|\bar{\gamma}}\left(P_{ij}|\bar{\gamma}\right) = \frac{\frac{10}{\log 10}}{\sqrt{2\pi\sigma_{dB}^2}} e^{\left[-\frac{b}{8}\left(\log\frac{d_{ij}^2}{\alpha_{ij}^2}\right)\right]}$$

The weight each particle takes during the update phase of the algorithm. This is straightforward, each particle takes the weight according to the observation, using error sensor model. $\vec{l}$ is the current measurement location.

$$P\left(m_j|\vec{x}_{t-1},\vec{l}\right) = N\left(\bar{P}_{ij}(dBm),\sigma_{dB}^2\right)\left(P_i\right)$$

The RSSI data was produced by assuming the model discussed. For getting the estimated Cell Tower position, the Maximum Likelihood Estimator is used:

$$pos^* = \sum \begin{pmatrix} x \\ y \end{pmatrix} * P(\begin{pmatrix} x \\ y \end{pmatrix} |measurements)$$

Where $\begin{pmatrix} x \\ y \end{pmatrix}$ the coordinates of the simulated area. The running algorithm and the results are demonstrated in Figures 4.10, 4.11, 4.12, 4.13 and 4.12. It is clearly that if it is found a good error sensor model for the RSSI, discovering the BTS is possible through Particle Filters.

The GPS error sensor model is presented, in order to be used in MySignals future work. Gaussian 2D function is a sufficient approach for error sensor model for the GPS accuracy since the probability of the actual location of the user is higher nearby the estimated position.

$$N_n\left(\bar{\mu},\Sigma\right)\left(\bar{x}\right) = \frac{1}{\sqrt{\left(2\pi\right)^n|\Sigma|}} e^{-\frac{1}{2}\left((\bar{x}-\bar{\mu})^\top\Sigma^{-1}(\bar{x}-\bar{\mu})\right)}$$

$$\bar{\mu}_n = \begin{bmatrix} \mu_1 \\ \mu_2 \end{bmatrix} = \overline{gps}_n = \begin{bmatrix} \mu_1 = gps_{nlat} \\ \mu_2 = gps_{nlong} \end{bmatrix}$$

The latitude is completely independent from longitude, so the autocorre-

lation table is:

$$\alpha = E\left[\left(x_1 - \mu_1\right)\left(x_2 - \mu_2\right)\right] = E\left[x_1 x_2 - x_1 E\left(x_2\right) - x_1 E\left(x_2\right) + E\left(x_1\right) E\left(x_2\right)\right] =$$

$$= E\left[x_1\right] E\left[x_2\right] - E\left[x_1\right] E\left[x_2\right] = 0$$

$$\Sigma = \begin{bmatrix} \sigma_{x_1}^2 & 0 \\ 0 & \sigma_{x_2}^2 \end{bmatrix} \overset{\sigma_{x_1}^2 = \sigma_{x_2}^2}{=} \begin{bmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{bmatrix}$$

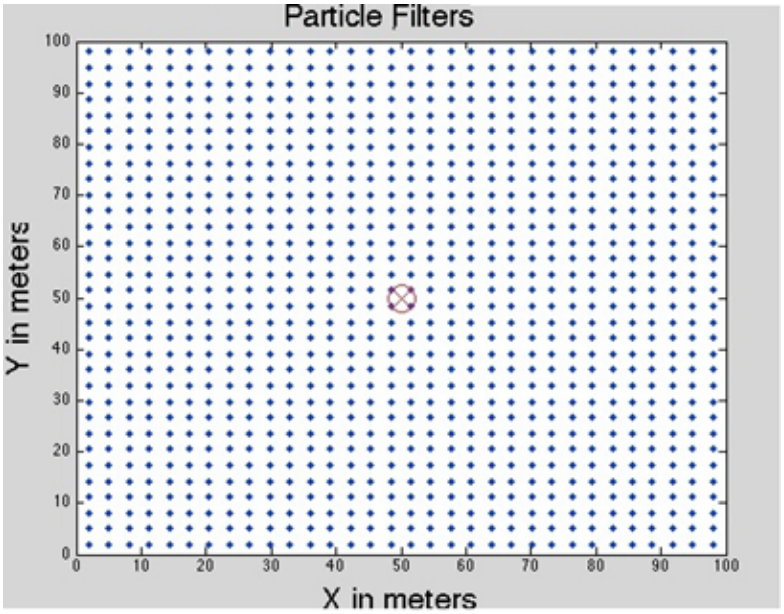

Figure 4.10: The circle with "X" symbol indicates the real BTS position. Every position in grid is possible to be the BTS location a priori. For this reason particle filters are applied uniformly.

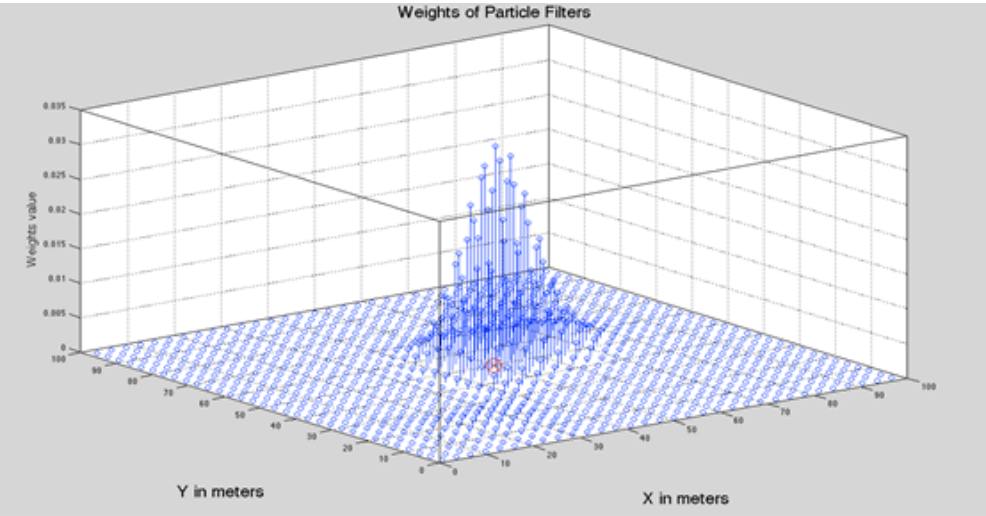

Figure 4.11: The weights of particle filters are increased nearby the real position of the Cell Tower. At the other position, particles weights are reaching zero.

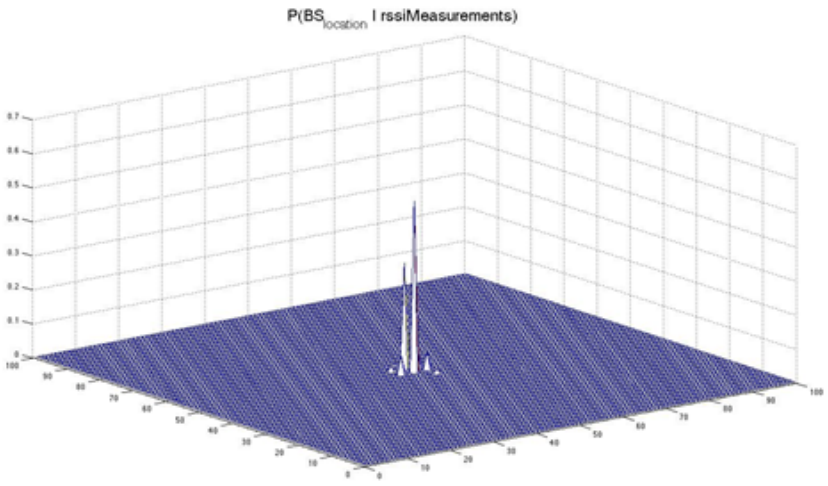

Figure 4.12: The continuous PDF for the BTS position is extracted using K-mean.

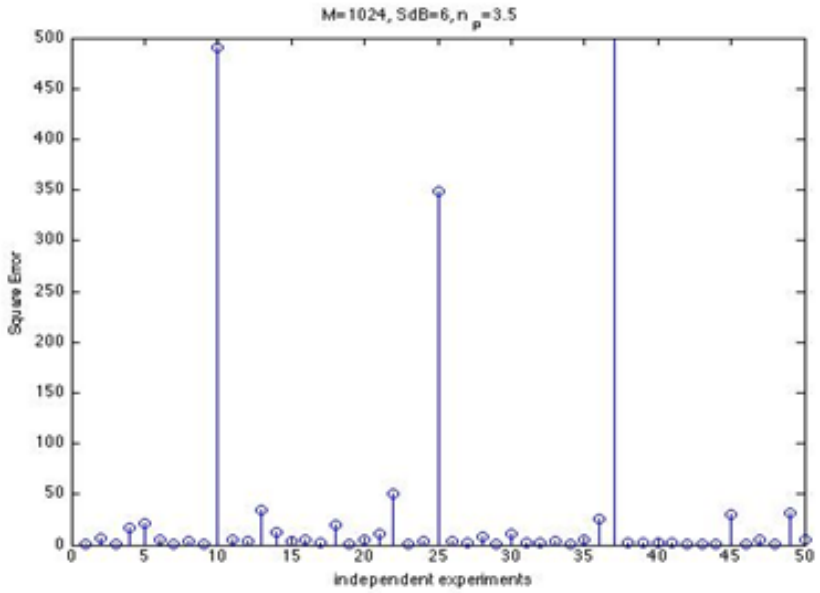

Figure 4.13: M=1024 Particle Filters, Mean Square Error is 52.67 m^2.

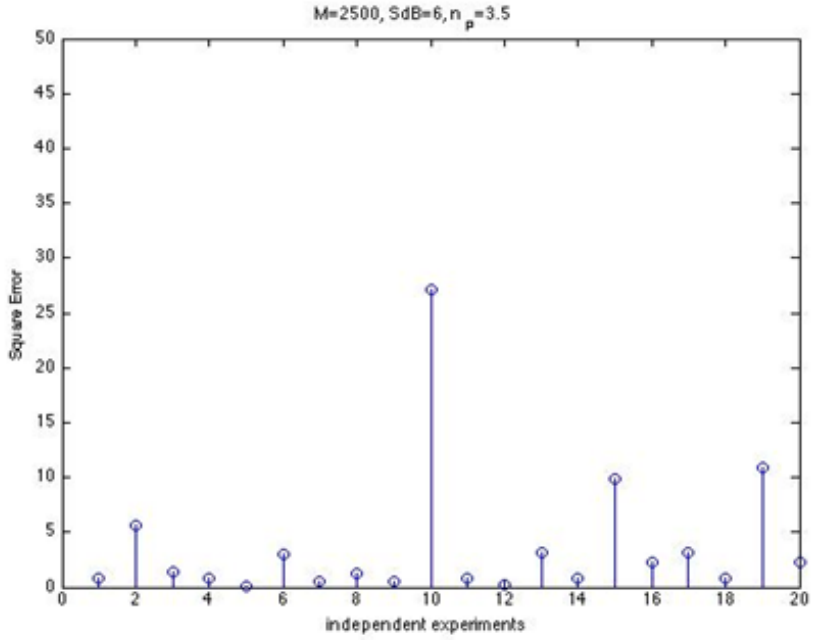

Figure 4.14: M=2500 Particle Filters, Mean Square Error is 3.68 m^2.

Chapter 5

Conclusion, Ongoing and Future Work

5.1 Thesis Contribution

This thesis develops iPhone's Community RF sensing, which to the best of our knowledge is the first community of such a kind in iPhone platform. This was achieved by exploiting iPhone capabilities for implementing a recording signal network using them as sensors, instead of deploying stationary measuring stations. MySignals iPhone App was developed and bypassed all the iOS restrictions for accessing RSSI and cellular information and details. RSS measurements connected to mobile's location provided by a-GPS are saved locally in iPhone and are forwarded periodically to a central MySQL server database. The collected measurements are displayed in a central GIS, using a heatmap -i.e., each recorded RSSI is displayed using a color code. Thus, a detailed mobile coverage map per network type and network carrier is available, providing an informational tool for signal quality per region. At the same time, MySignals users on iPhone can be informed for various cellular network parameters, their cellular network performance and mobile basic principles of operation.

A real world evaluation of MySignals has been performed, collecting over 40000 measurements from seven real users for over three weeks. A time and a space analysis on the collected data has been performed. The time analysis of the RSSI demonstrated in practice the "GSM Power Control" pattern which is applied by the cellular mobile networks. Except time analysis, specific regions with extremely poor signal were discovered indicating that MySignals can provide a detailed mobile coverage map. Additionally, the space analysis

reveals the poor performance of iPhone's GPS since over 28% of the collected measurements had over 450m inaccuracy, which was not acceptable by our approach. Moreover the iPhone's GPS even under the best circumstances (outdoors measurements) has errors. Concluding, the collected RSS with their corresponding locations and cellular information could be used in a wide range of research applications. An example for a possible future direction is demonstrated by applying Particle Filtering in RSS data in order to discover the position of a Cell Tower.

MySignals GIS approach and the applied software design patterns can be easily introduced to any smartphone platform, since MySignals was created following as much possible generic design patterns. The ER schema (data model) and the JSON implementation can be used independent from the used as a sensor smartphone, since they represent a general model for Cellular Mobile Networks. Also, the central Web Server Database and the web site was implemented in such a way that measurements could easily be collected by other smartphone platforms. MySignals is aiming to be adopted widely by the users.

5.2 Ongoing and future work on MySignals Project

Our future plans and goals include the following:

- MySignals project aims to be ported on iPhone 4S (using private - callbacks- APIs) and the newer iPhone 5. The above is a goal of grave importance for achieving a wide MySignals adoption from the users.

- For supporting full functionality of MySignals, iPhone 4s must be "hacked", allowing this way, querying AT Commands to baseband. A close look to the evolution in Jailbreaking scene and accessing newer iPhone's baseband, is necessary. It will be also interesting to contribute in unlocking iPhone's baseband.

- It is essential to create an iOS 5 and iOS 6 widget to the notification center.
- iOS 6 Jailbreak for iPhone 3GS/iPhone 4, which are currently supported from MySignals, is expected for testing MySignals in these devices.
- Moreover the future introduction of a social game of collecting points, will certainly attract many users. This could include lists Hall of fame, lotteries, and conversions of points into presents or services. This would lead to a wide adoption of MySignals.
- Addition of new screens and features in MySignals, which will show the measurements history, the average of measurements per region etc.
- To provide a new screen inside iPhone, representing the coverage map of user's network.
- More importantly, restriction in iPhone 4 rebooting must be solved, by creating, for example, an automatically script at the booting of the iPhone, that it would unlock baseband socket.
- Further improvements in the heatmap engine, the color coding and the performance of the heatmap engine.
- A time based filtering of the collected measurements will be implemented in heatmap engine and it will be added on website.
- MySignals web site (pages: "project description", "contact us", "FAQ" etc) must be finished soon.
- A REST protocol is in our future goals, for bidirectional communication between MySignals and Web server, thus, MySignals could retrieve Cell Tower coordinates and other information from its own server.
- Further research localization and discovering BTS positions will be considered. Exploiting the collected data for research applications is our primary goal.

- In general the wide adoption of MySignals as an engineering, research and informational tool.

One can easily understand that MySignals Project is just on its first steps and provides great opportunities for future evolution.

Appendix 1

The cell dump environment answer from iPhone's baseband to the command, using "At+CGED=0":

at+cged=0
+CGED: RAT:"GSM",
RR:10
txpwr:255, RxLevServ:026, RxQualFull:255, RxQualSub:255,
dtx_used:True, drx_used:False,
SFRLC: 0, RSR: 2, RC: 5, LM:0
GSM Serving Cell:
B:"D", Arfcn: 803, Rssi: 26, C1:26, C2:26, Bsic:27, MA:0, MADed:65535
GSM Neighboring Cell:
Ci:ed13, B:"D", Arfcn: 867, Rssi: 27, C1:27, Bsic:27
Ci:eca7, B:"D", Arfcn: 795, Rssi: 21, C1:21, Bsic:24
Ci:ecad, B:"D", Arfcn:1009, Rssi: 17, C1:17, Bsic:24
Ci:ffff, B:"D", Arfcn: 814, Rssi: 7, C1: 7, Bsic:26
Ci:ffff, B:"D", Arfcn: 807, Rssi: 0, C1:-1, Bsic:ff
Ci:eca6, B:"D", Arfcn: 800, Rssi: 0, C1:-1, Bsic:ff
UMTS Neighboring Cell:
MM:
Process:CO, MMs: 4, MMSs:16, MSC:D, T:0000
Process:CS, MMs: 5, MMSs: 5, LUS:1, T:0004, L:0, lu_rej_cause:0
Process:PS, MMs: 9, MMSs: 5, LUS:1, T:0008, L:0, GS:1, R:0, attach_reject_cause:0, rau_rej_cause:0, act_rej_cause:0
Cell change counters:
CRT: 4, IRCR: 0
AIRCR: 0, IRHO: 0, AIRHO: 0

Coding Scheme:

dl_sc:NB_CS_1, ul_sc:

amr_acs:0, amr_cod_ul:0 amr_cod_dl:0 amr_c_i:0

Equivalent PLMNs:

MCC:202, MNC: 1

Serving PLMN:

MCC:202, MNC: 1, LAC: 312, CI:ed15, RAC: 1, AcT:1

GPRS-Parameters:

SplitPg:False, NCO:00000, NOM:002, T3192:01f4,

Acc_Burst_type:00016, DRX_Timer_Max:03, PBCCH:False, Ext_Measure_Order:00000,

PSI1_r_per:00 si13_location:"BCCH_NORM" packet_psi_status:False, packet_si_status:True, ext_upl_tbf_supported:False, ccn_active:True, pfc_feat_supported:False

Count_LR:00, Count_HR:01, C_R_Hyst:06, C31:-0001, C32:00026, Prior_Acc_Thr:06

.

The answer in AT+CSQ command, which gives back the RSSI in ASU format:

at+csq +CSQ: 18,99

Appendix 2

An comprehensive example of the JSON string which is sent from the iPhone to the Web Server. In this examples, 2 measurements stamps are packetized for submission to the server. The root of the objects is the LAI which has cell towers and the cells towers have observed measurements. With this approach we can packet hundred or even thousand of measurements in JSON. For demonstration purposes and for space saving, only two measurements are included to the JSON as an example.

{
"MNC": 1,
"networkType": "GSM",
"hasCellTowers": [
{
"hasMeasurements": [
{
"bsic": 46,
"hasMetaData": {
"dt1": "1.02",
"dt4": "1.02",
"rssi1": -75,
"rssi3": -73,
"rssi5": -73,
"dt3": "1.02",
"rssi2": -75,
"rssi4": -73,
"dt2": "1.02",
"dt5": "1.02"

},
"timestamp": "2012-09-11T01:45:11.141+0300",
"hasNeighbors": [
{
"CellID": 60691,
"C1": 23,
"bsic": 39,
"arfcn_ dlink": 867,
"rssi": 23
},
{
"CellID": 60583,
"C1": 28,
"bsic": 36,
"arfcn_ dlink": 795,
"rssi": 28
},
{
"CellID": 16041,
"C1": 10,
"bsic": 46,
"arfcn_ dlink": 783,
"rssi": 10
},
{
"CellID": 60651,
"C1": 8,
"bsic": 39,
"arfcn_ dlink": 837,
"rssi": 8
},
{
"CellID": 16042,

”C1”: 17,
”bsic”: 46,
”arfcn_ dlink”: 818,
”rssi”: 17
}
],
”txPower”: -255,
”avg”: 0,
”arfcn”: 843,
”rssi”: -73,
”takenIn”: {
”fLat”: 35.528962655,
”fLon”: 24.06939691,
”lon”: 24.06939691,
”lat”: 35.528962655,
”vertAccur”: ”-1.0”,
”horizAccur”: ”100.00”
},
”c1”: 32,
”c2”: 32
},
{
”bsic”: 46,
”hasMetaData”: {
”dt1”: ”1.06”,
”dt4”: ”1.02”,
”rssi1”: -77,
”rssi3”: -75,
”rssi5”: -75,
”dt3”: ”1.02”,
”rssi2”: -75,
”rssi4”: -75,
”dt2”: ”1.02”,

”dt5”: ”1.02”
},
”timestamp”: ”2012-09-11T01:44:07.758+0300”,
”hasNeighbors”: [
{
”CellID”: 60691,
”C1”: 23,
”bsic”: 39,
”arfcn_ dlink”: 867,
”rssi”: 23
},
{
”CellID”: 16042,
”C1”: 17,
”bsic”: 46,
”arfcn_ dlink”: 818,
”rssi”: 17
},
{
”CellID”: 16041,
”C1”: 10,
”bsic”: 46,
”arfcn_ dlink”: 783,
”rssi”: 10
},
{
”CellID”: 60651,
”C1”: 8,
”bsic”: 39,
”arfcn_ dlink”: 837,
”rssi”: 8
},
{

”CellID”: 60583,
”C1”: 28,
”bsic”: 36,
”arfcn_ dlink”: 795,
”rssi”: 28
}
],
”txPower”: -255,
”avg”: 0,
”arfcn”: 843,
”rssi”: -75,
”takenIn”: {
”fLat”: 35.528962655,
”fLon”: 24.06939691,
”lon”: 24.06939691,
”lat”: 35.528962655,
”vertAccur”: ”-1.0”,
”horizAccur”: ”100.00”
},
”c1”: 33,
”c2”: 33
}
],
”MNC”: 1,
”cellID”: 16043,
”networkType”: ”GSM”,
”LAC”: 312,
”MCC”: 202
}
],
”regionName”: ”Chania”,
”LAC”: 312,
”MCC”: 202

```
}
```

Bibliography

[1] "Brief History of GSM & the GSMA", *available online,* *http://www.gsma.com/aboutus/history/* . 15, 34

[2] http://www.itp.net/588064-global-mobile-penetration-hits-85 ,http://www.indexmundi.com/map/?v=105,25/09/2012 15

[3] Canadian Radio-television And Telecommunications Commision, "Telecommunications Glossary," *available online,* *www.crtc.gc.ca/dcs/eng/glossaryT.htm*. 15

[4] Newspaper Proto Thema, "15.25 million mobile subscriptions in Greece," *available online* *http://www.protothema.gr/technology/article/?aid=183926*, March 17, 2012. 16

[5] P. Vecchia, R. Matthes, G. Ziegelberger, J. Lin, R. Saunders, A. Swerdlow, "Exposure to high frequency fields, biological effects and health consequences (100KHz-300GHz)," *International Commission of Non-Ionizing Radiation Protection(ICNIRP)*, 16/2009. 18

[6] Greek Atomic Energy Commission, GAEC, *www.eeae.gr*. 18

[7] F. Mavromatis, A. Boursianis, Th. Samaras, Ch. Koukourlis and J. N. Sahalos, "SMS-K: DESIGN OF A MONITORING SYSTEM FOR ELECTROMAGNETIC RADIATION MEASUREMENTS", *URSI General Assembly*, Chicago, USA, 7-16 August, 2008. 8, 19, 20

[8] F. Mavromatis, A. Boursianis, Th. Samaras, C. Koukourlis and J.N. Sahalos, "A Broadband Monitoring System for Electromagnetic Radiation Assessment", *IEEE AP Magazine*, Vol. 51, No.1, pp. 71 -79, Feb. 2009. 20

[9] Fasma Program, *http://www.fasmaprogram.gr/*. 20

[10] A. Gotsis, N. Papanikolaou, D.Komnakos, A. Yalofas, P. Constantinou, "Non-ionizing electromagnetic radiation monitoring in Greece", *GET and Springer Verlag France 2008, published online*: 17 January 2008 20

[11] NTUA, AUTH, "Hermes Project", *http://hermes.physics.auth.gr/en/desc_ihermes*. 20

[12] Professor T. Luhrmann, "iPhone Addiction Survey" *by Stanford University* *http://www.msnbc.msn.com/id/35768107/#.UF4dglFadEw*, *http://www.iphonehellas.gr/14729/iphone-addiction-survey/*, 25/09/2012 24

[13] J.D. Power and Associates, "2012 Wireless Smartphone Satisfaction Study", *http://www.iphonehellas.gr/38808/apple-satisfaction-top/*, "96% Customers Satisfied with iPhone 4S" *http://www.iphonehellas.gr/32034/iphone-4s-satisfaction-rate/* *by Research firm ChangeWave.* 24

[14] Apple, "iPhone 5 Pre-Orders Top Two Million in First 24 Hours", *Apple Press Info,* *http://www.apple.com/pr/library/2012/09/17iPhone-5-Pre-Orders-Top-Two-Million-in-First-24-Hours.html*, September 17, 2012,
Apple, "iPhone 5 First Weekend Sales Top Five Million", *Apple Press Info,* *http://www.apple.com/pr/library/2012/09/24iPhone-5-First-Weekend-Sales-Top-Five-Million.html*, September 24, 2012 24

[15] Hacker Planetbeing (Yiduo David Wang), Dev Team member, Achievements and references: *http://theiphonewiki.com/wiki/index.php?title=User:Planetbeing*. 26

[16] Yiduo David Wang, "Signal", *Cydia Store*, http://signal.kssh.ca/. 26

[17] "OpensSignalMaps", *Android Market*, *http://opensignal.com/*. 26

[18] "Cellumap", *Android Market, Symbian platform, Blackberry Platform,* http://www.cellumap.com/, /play.google.com/store/apps/details?id=com.cellumap&hl=en , http://www.cellumap.com/phone-symbian.html 28

[19] Tawkon App, available on Android market and Cydia Store, http://tawkon.com/, https://play.google.com/store/apps/details?id=com.tawkon 28

[20] K. Li and P. Jiang, "Open Google Project", *available online, http://code.google.com/p/location-estimation-trials*. 28

[21] *http://www.comlab.hut.fi/opetus/238/lecture2.pdf* 33

[22] B.A. Forouzan and F. Mosharraf, "Computer Networks A Top-Down Approach", *McGraw Hill Higher Education.* 33, 36, 37, 38

[23] "Mobile Technologies GSM overview", *by ETSI, http://www.etsi.org/website/technologies/gsm.aspx*. 34, 35

[24] A. Bletsas, "Telecommunication Systems II (Course Notes), Mobile Architecture, Continuous Phase Modulation (CPM) and the special cases of MSK, GMSK", at the *Electronic And Computer Engineering Dept., Technical University of Crete*, Spring 2012 35

[25] T. Turletti, "GMSK in a nutshell", *Laboratory of Computer Scinece, Massachussets Institute of Technology.* 35

[26] GSM radio technology is specified in the 3GPPTM TS (Technical Specifications) 45.-series specifications. The overall GSM network architecture is described in 3GPPTM TS 23.002 and a complete list of Technical Specifications for GSM systems is given in 3GPPTM TS 41.101, www.3gpp.org, www.3gpp.org/specification-numbering,www.etsi.org. 34, 35

[27] Gunnar Heine, "GSM Networks: Protocols, Terminology, and Implementation", *Artech House, Boston - London*, 1999. 35, 53

[28] Krister Bjrnsj, "Frequencies for IMT-2000 in a global perspective", June 22, 2000, *www. umtsworld. com*. 8, 36

[29] 3GPP, ETSI, "Radio Access Network, Radio Transmission and Reception", Chapter 2, "Frequency bands and channel arrangement", release 8, *3GPP Technical Specification* 45.005 V8.8.0 (2010-03). 37, 53, 54

[30] 3GPP, "User Equipment (UE) radio transmission and reception (FDD)", 3GPP TS 25.101

[31] 3rd Generation Partnership Project, www.3gpp.org/About-3GPP. 37

[32] Cosmote GR Press Info, "The first 4G cellular telephony network by Cosmote", August 1, 2012. 39

[33] Vodafone GR Press Info, "Vodafone invests in 4G cellular telephony network", August 8, 2012. 39

[34] 3GPP LTE Overview, http://www.3gpp.org/LTE. 39

[35] Motorola Corp, "Long Term Evolution(LTE), A technical Overview", technical white paper, *available online*. 39

[36] Apple, "iOS Developer Library, Documentation and References", *available online developer. apple. com/ library/ ios/ navigation/* 41, 42

[37] Apple, "The Objective-C Programming Language, Reference Manual," *available online*. 41

[38] Apple, "Advanced Memory Management Programming Guide," *available online*. 41

[39] Stanford University, Computer Science Department, "CS 193P iPhone Application Development Course," included in syllabus at 2009, *available on iTunes U* 45

[40] Steve Jobs, formerly Apple's CEO, "Answer on a demand for opening private CoreTepephony SDK" *http://www.maclife.com/article/news/steve_jobs_tawkon_no_interest_opening_sdk_radiationtracking_app*, April 30, 2011 46

[41] ETSI , "Digital cellular telecommunication system (phase 2+), Radio subsystem link Control," *ETSI, GSM Technical Specification,* TS 05.08, July 1996 46, 53

[42] U.S. Copyright Office decision, "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies" *http://www.cnet.com/8301-17918_1-20011824-85.html*, *http://www.copyright.gov/1201/* 48

[43] *http://developer.apple.com/library/ios/#documentation/ToolsLanguages/Conceptual/DevPortalGuide/CreatingandDownloadingDevelopmentProvisioningProfiles/CreatingandDownloadingDevelopmentProvisioningProfiles.html* 49

[44] *http://www.youtube.com/watch?v=ErLt2Le558Q* 49

[45] "Install Apps on iPhone without the official paid developer program," *by Jailbreaking Community* *http://jaischeema.com/2012/06/05/running-xcode-applications-without-provisioning-developer-profile.html* 49

[46] otool, Mac Developer Library, textiturlhttp://developer.apple.com/library/mac/# documentation/-Darwin/Reference/ManPages/man1/otool.1.html 50

[47] http://en.wikipedia.org/wiki/George_Hotz 50

[48] G. Athanasopoulou, E. Alibertis, "Remote Sensor Network via GPRS", semester project for the TEL412 "Analysis and Design (Synthesis) of Telecom Modules", Fall of 2010-2011 at ECE Department,

TUC, *available on-line,* http://www.telecom.tuc.gr/~aggelos/tel412_fall2010/projects.html 50

[49] George Hotz, also known as Geohot, "Core Telephony reversed engineer headers", a*vailabe online,* http://iphone-wireless.googlecode.com/svn/trunk/CellStumbler/CoreTelephony.h 50

[50] Liqiang Yang, "iPhone-SMS project," by Jailbreaking Community, *available at google code* http://iphone-sms.googlecode.com. 51

[51] iPhone 3G/3GS: Infineon X-GOLD 608, *specification sheet available online.*
Iphone 4 and iPad 2: Infineon X-Gold 618, *specification sheet available online.*
Iphone 4s: Qualcomm MDM6610.Iphone 5:Qualcomm MDM9615M. 52

[52] TELTONICA, "At Commands Manual", ch.5 "Specific AT Commands", *available online* 52, 53, 57

[53] 3GPP, ETSI, "AT command set for User Equipment (UE)," *3GPP, ETSI, GSM specification sheet*, TS 27.007. 52

[54] Francois Guilleme, "Iphone-delivery-report," *available at google code,* http://code.google.com/p/iphone-delivery-report/wiki/iPhone_4S 55

[55] ETSI, GSM Technical Specification, "Digital cellular telecommunication system (phase 2+), Radio transmission and reception", *ETSI, GSM Technical Specification*, ch. 4.1 "Ouput Power", GSM TS 05.05, May 1996. 54, 58

[56] 3GPP, ETSI, "AT command set for User Equipment (UE)," *3GPP, ETSI,GSM Specification Sheets,* TS 27.007. sub clause 8.5, 8.69 See also TS 27.133, 8.69. 57

[57] Apple, "Introduction to Core Data Programming Guide", reference manual, *available online* 60

[58] Asalom, "Custom Map Annotation Callouts for iOS Maps," *available online at Github*, https://github.com/asalom/Custom-Map-Annotation-Callouts 66

[59] Johnezang, "JSONKit, Objective C JSON", *available online at Github*, *https://github.com/johnezang/JSONKit* 78

[60] Steve Jobs, "Press Conference: Antennagate problem,", *Apple Press Conference*, July 16, 2010. 75

[61] A. Drake, "Mac Address Privacy Considerations," *http://aadrake.com/mac-addresses-udids-and-privacy.html* 76

[62] P. Wied, "A heatmap canvas javascript library", *available online at Github*, *github.com/pa7/heatmap.js* 80

[63] The MIT Licence (MIT), *http://opensource.org/licenses/MIT*. 80

[64] S. Russel, P. Norvig, "Artificial Intelligence, A modern Approach", *Klidarithmos 2nd American Edition*, ch. 14. 96

[65] S. Thrun, W. Burgard, D. Fox, "Probabilistic Robotics," *Klidarithmos greek edition*, ch. 3, Particle Filters, 2011. 96

[66] Neal Patwari, A. O. Hero, M. Perkins, N. S. Correal and R. J. O'Dea, "Relative Location Estimation in Wireless Sensor Networks," *IEEE Transactions on Signal processing*, vol 1, No. 8, August 2003. 97