TECHNICAL UNIVERSITY OF CRETE
SCHOOL OF ELECTRONIC AND COMPUTER ENGINEERING
TELECOMMUNICATIONS DIVISION

Smart Sensors of RF and Backscatter Signals with Localization

by

Emmanouil Alimpertis

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE MASTER OF SCIENCE OF

ELECTRONIC AND COMPUTER ENGINEERING

August 5, 2014

THESIS COMMITTEE

Associate Professor Aggelos Bletsas, *Thesis Supervisor*
Associate Professor George Karystinos
Associate Professor Michail G. Lagoudakis

Abstract

Information may be more valuable when the location of its source is known. This thesis develops localization algorithms based on received signal strength (RSS) measurements for unknown radio frequency (RF) sources and bistatic scatter radio tags (sensors). This thesis demonstrates RF source location estimation utilizing RSS measurements by a community of smartphone users, within 800m (or more) from the source. The location estimation algorithm incorporates careful modeling of the time-varying source transmission power, source antenna directionality (even with a single 4-parameter model) and different path loss exponents among the various source-user links. More importantly, a vast number of measurements is collected and exploited through an automated community of smartphones. Location estimation error on the order of 50m is achieved, even when users are within 800m or more from the RF source. Furthermore, multiple input single output RSS localization for bistatic scatter radio is also considered. The RF scatter radio tag is illuminated by multiple low-cost carrier emitters, operating consecutively. Experimental validation of the proposed algorithm reports localization error on the order of 3m for tag and emitters placed at an area of 70m x 70m. Both estimation algorithms on real-world data exploit non-parametric estimation based on particle filtering.

Thesis Supervisor: Associate Professor Aggelos Bletsas

Acknowledgements

I would like to wholeheartedly thank and express my gratitude to all my dear friends, my colleagues, my advisor and my family. They gave me courage to keep up during this academic journey. Their help and mentoring was essential in order to complete this thesis.

Firstly, I would like to express my gratitude Dr. Aggelos Bletsas for his support, the valuable research guidelines during this thesis and his help for continuing my studies as a Ph.D. student at USA. He is a big source of motivation for hard work and for implementing as much as possible real world telecommunications and software applications. His research mentality, that an engineer must combine theory with real world applications from all the electronic and computer engineering fields, inspires me and drives my work.

It is very hard to express my feelings and gratitude through words for my friends. The only I can say is a big THANK YOU: Nikos Pavlakis, Nikos Kofinas (aka Kofi), Mitsos Iliou, Keimis Perros, Fia Nikolakaki, Giannis Demertzis and Helen Kountourakis you made me feel like at home in Chania! Indeed, you were my family and we will never break our friendship! Thank you from the bottom of my heart!

Moreover, I would like to thank all my colleagues at Telecom Laboratory for the cooperation, valuable technical advises, trolling and research time we had: Nikos Fasarakis, Konstantinos Tountas, Eleftherios Kampianakis, John Fountzoulas, Nikos Agadakos and George Theodorakis.

However, Nikos Fasarakis earns a second acknowledgement for the endless conversations related our research and our problems; indeed we had a great time exchanging ideas. His advises, tips, and his know-how was extremely valuable to complete this work.

Last but not least, I would like to thanks all MySignals beta testers: Kostas Tsichlis, George Krokos, Mitsos Iliou, Katerina Zenelli and Giannis Demertzis! I really thank you guys for draining your battery and using the application in order to collect measurements for my M.Sc. Professors Michail Lagoudakis and Polychronis Koutsakis should also be in the acknowledgments section since they have helped me and motivated me in many aspects.

Finally, I would like to thanks my parents and my sister for their deepest love and support in all stages of my life...Everything that has a beginning has an end. After eight amazing years at Technical University of Crete with amazing people, the new journey for seeking a Ph.D. degree begins!

To my dog Rake, the most loyal friend, who died at the end of this thesis.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation for Smart RF Sensors with Localization

In a modern era, information may be more valuable when the location of its source is known. The recent rapid advances in the satellite services for global positioning such as the introduction of Global Positioning System (GPS) or other similar systems (Gallileo and GLONASS[1]) highlight the inherent importance of location awareness and have acted as key elements of location based- services. Each single smartphone is equipped with a positioning system, enabling countless navigation and ubiquitous computing applications. Current research trends and concepts such as the "Internet of Things" advocate the necessity for accurate localization of each single RF device-sensor.

However, satellite localization services are accompanied by many practical limitations. First of all, the GPS or relevant modules are relatively expensive, (e.g. GPS costs approx. 20-30 $[2]), prohibiting each single sensor to be equipped with such a module, more so in ultra-large scale sensing applications. Furthermore, positioning services rely on line of sight (LOS) communication with the satellites and hence are not always available (especially in indoor scenarios). Note, that in cities with tall buildings there are a lot of blind spots. Most importantly, GPS and similar modules have high energy consumption; smartphones drain their battery if their GPS is opened and low-energy sensors cannot possibly supply such amount of energy.

Apart from wireless sensor networks, there is a universal need for localiza-

---

[1]Galileo and GLONASS global navigation satellite systems are developed by the European Union and Russia respectively. GPS was developed by the U.S.A.

[2]For example, www.alibaba.com/showroom/low-price-gps-module.html.

tion of *any* RF device. For instance, FCC[3] requires that the mobile phones must be localized by the network providers in the case of emergency, with a certain accuracy even without the presence of GPS. Moreover, RF-sources (i.e. base stations) localization is necessary in many cases since the exact knowledge of their unknown and unlisted locations could enable a vast number of applications. For example, work in [8], estimates the base stations' locations in order to determine the empty spectrum areas for utilization by cognitive radio networks.

The aforementioned GPS constraints indicate the necessity for GPS alternatives[4] localization of RF devices, in a variety of different wireless propagation scenarios (e.g. low cost sensors, smartphones, wireless routers, cellular base stations etc). As a promising alternative to GPS, localization techniques based on received signal strength (RSS) measurements (e.g. in [9]) have emerged the recent years. These techniques are very popular due to the fact that RSS is readily available at each single RF device and acts as an indicator of distance between the transmitter and the receiver. On the downside, RSS is generally very noisy, motivating considerable research effort in exploring its applicability for location estimation (e.g. in [10]).

Thus, RSS-based localization is a universal prerequisite for a variety of applications such as public safety, low energy RF device localization and optimal resource allocation in wireless networks. At the same time, it is a key-enabling feature for the adoption of ultra large scale sensing applications in everyday life. This thesis develops RF smart sensors with RSS-based localization for two different wireless propagation scenarios. The problem of the unknown RF-source location estimation as well as the problem of sensor localization in large-scale backscatter sensing networks are both considered.

---

[3]Federal Communication Committee (FCC) requires providers to localize users' mobile in the case of emergency. The location information must be accurate to within 50 to 300 meters, depending upon the type of location technology used. Further information is available at http://www.fcc.gov/guides/wireless-911-services.

[4]For example, Skyhook company provides location services based on the cell tower or Wi-Fi access points locations etc. www.skyhookwireless.com

1.2 Thesis Contributions

1.2.1 RF Source Location Estimation by Users

Location estimation of radio frequency (RF) emitters (i.e. sources) is important for GPS-free services, location-relevant business, social awareness as well as for optimal resource and frequency allocation in wireless networks (e.g. in [8]). The explosion of mobile cellular telephony using *smartphones*, including GSM or newer 3G/4G technologies, with over 6 billions subscribers worldwide, has opened new avenues for innovative, location-aware applications. However, the locations of the base stations are unlisted and unknown since they are considered corporate-trade secret. Knowledge of the base stations locations could allow the development of user's localization by its RSS measurements.

This thesis *experimentally* studies the problem of RF source location estimation, using a large collection of received signal strength (RSS) measurements, readily available from a community of mobile telephony, smartphone users.

Related literature in RSS-based RF source localization is quite rich. Localization error on the order of a few tens of meters is reported with Wi-Fi terminals and communication ranges on the order of tens of meters (e.g. work in [11] and references therein), as opposed to ranges on the order of hundreds of meters in this thesis. Work in [12] solves a semi-definite programming problem (SDP), assuming a common and known path loss exponent (PLE) between an RF source and measuring terminals, with unknown, time-constant RF source transmitted power. Work in [13] assumes that the PLE is unique across all measuring terminals and unknown, the RF source power is constant and known and offers a nonlinear least-square estimator. Work in [14] proposes a weighted least squares solution, considering both transmitted power and (the unique) PLE, constant and unknown. Moreover, work in [15] follows the same assumptions and exploits measurements collected by a moving sensor. Work in [16] assumes different PLE per measuring terminal and each grid point receives votes, based on a bounding-voting pro-

cedure; the grid point with the most votes is the estimated emitter location. All the aforementioned approaches are based on simulated data. Examples of experimental cell tower localization, based on the strongest measurement or a weighted average of the K-strongest measurements [17–19], or user localization, based on modeling of the coverage areas with a student distribution [20], exploit *wardriving* (a.k.a. fingerprinting): RSS measurements and their respective GPS location are recorded, while moving in a specific area, before any processing is applied.

In sharp contrast to prior art, this work utilizes a vast collection of real world RSS measurements based on community RF sensing. Moreover, in sharp contrast to prior art, PLEs across different users are considered unequal and unknown, transmission power from source is considered time-varying, while cases between directional or isotropic source antenna are both considered. It is shown that the adoption of a directional antenna model, even a simple one, in conjunction with the rest of the aforementioned realistic assumptions, as well as the vast number of measurements - due to community RF sensing - can significantly reduce the absolute location error. Experimental results with absolute error on the order of 50m are reported, where the sources are real-world deployed mobile telephony base stations within extended ranges on the order of 800m from the measuring users-RF sensors.

1.2.2 Sensor Localization in Bistatic Scatter Radio Networks

Recent work and current research trends point towards the adoption of large-scale backscatter sensor networks for large scale, large resolution environmental sensing applications. This emerging type of network (e.g. [6] and [21]) is based on the principle of reflection; the sensor is built from a simple antenna and a switching RF transistor which modulates an incoming carrier. In doing so, expensive and power demanding electronics such as mixers, low noise amplifiers (LNAs), and filters, are not required; communication is achieved with a single RF transistor, an antenna and a low-cost low-power micro-controller unit (MCU).

The scattering principle is not new; it has been extensively utilized by RFID platforms, where the RF tags modulate the incoming carrier generated by the reader to scatter back their ID (i.e. a monostatic architecture). However, this setup suffers from round-trip path loss and coupled with passive (i.e. battery-less) tags offers limited communication ranges, on the order of few meters. In contrast, bistatic architectures [6] de-attach the carrier emitter from the reader: this way multiple low-cost emitters can be placed stochastically in a given area to simultaneously illuminate many different RF tags. In conjunction with semi-passive (i.e. battery assisted) tags and low bit rates (suitable for environmental sensing applications), communication ranges on the order of 100m have been reported [6], [22].

RF tag localization in the context of bistatic backscatter arises from the necessity of auto-localization and auto-organization of potentially hundreds or thousands of nodes on a field. It is simply not practical to record each single location on such large scales. In addition, sensor's location may change, therefore static location assignment is not practical.

Relevant prior art has mainly focused on RFID localization utilizing multiple network readers for short ranges. For example, work in [23] utilize multidimensional scaling on each tag's RSS which is captured by many reader. Similarly, work in [24] utilizes multiple readers, where the power levels are calibrated against reference sensitivity. Moreover, work in [25] develops tag localization based on angle-of-arrival (AoA) measurements in bistatic architectures.However, the relevant ranges are smaller than 2 meters and the localization platform utilize multiple readers and a single emitter each time.

In sharp contrast to relevant prior art, this work utilizes multiple low-cost carrier emitters rather than multiple readers for tag localization. This is beneficial since carrier emitters may come in the form of an oscillator, a power amplifier and an antenna, and can thus be two orders of magnitude cheaper than the reader. In addition, the setup is much simpler and only a time division multiple access (TDMA) scheme is needed, in contrast to localization with multiple readers which pre-require the collection of the measurements at a central point. Moreover, this work departs from relevant prior art by considering both unknown and different path loss exponents (PLEs) across

each carrier-to-tag link, as well as the carrier-to-reader links.

Chapter 2

Community RF Sensing: Architecture

2.1 Problem Formulation

Our goal is to estimate the unknown location of an RF source (i.e. base station) which serves N mobile smartphone users, using RSS measurements. In this work, a specific GSM base station in Chania, Crete, Greece serving many users, is used for experimental validation. The system topology for RF-source location estimation is depicted in Fig. 2.1.

The known static location of user j is denoted as $\mathbf{x}_j \triangleq \begin{bmatrix} x_j & y_j \end{bmatrix}^T$ and the location of the RF source *to be estimated* as $\mathbf{x}_{\mathrm{BS}} = \begin{bmatrix} x_{\mathrm{BS}} & y_{\mathrm{BS}} \end{bmatrix}^T$. The collection of all user locations is denoted by $\mathbf{x} \triangleq \begin{bmatrix} \mathbf{x}_1 & \cdots & \mathbf{x}_N \end{bmatrix}$.

2.2 Large-Scale Measurement Campaign

The cellular telephony measurements are collected by a community RF sensing infrastructure (developed in [26]) for cellular mobile networks, utilizing users' mobiles as sensors. The developed smart RF sensors community allows us to monitor in detail the cellular network in each single location. Apart from the development of algorithms for RF-source localization, the platform and the collected data could enable a vast number of diverse research applications.

The community RF sensing platform is presented in Fig. 2.2: An application named MySignals running on smartphones, records the received signal strength (RSS), the detailed cellular network information and the smart-
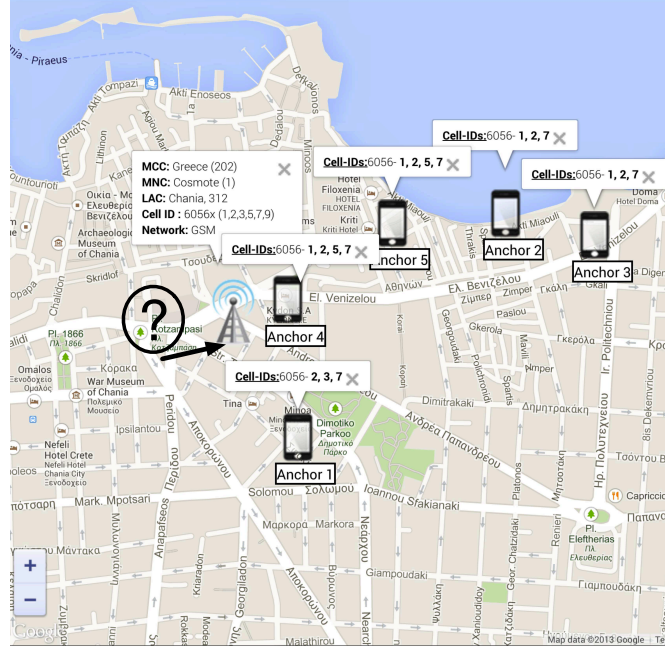
Figure 2.1: Base station localization case study: 5 users (at their home) record the RSS (in dBm) of specific base station cells in the city of Chania (BS installed at Tzanakaki street with the exact location provided by the network carrier).

phone's location. The users' measurements are collected, with the use of the smartphone's Wi-Fi, by a central web database for permanent storage. In doing so, detailed mobile coverage maps, available at www.mysignals.gr [1], are created by the users themselves and the public can determine the network performance per region. Furthermore, the system could assist in city-wide evaluations and in the maintenance of existing cellular telephony network deployments.

The measurements of GPS coordinates validate that users were indeed located at their predetermined locations **x**. The subset of the measurements regarding the specified cells is available at www.mysignals.gr/dataset.zip, providing a long term study for GSM networks (see Table 3.1 of chapter 3). Hundreds of cells with several million distinct measurements are also available (both for 2G and 3G). The users mostly their 2G connection, since 3G signal

---

[1]Site is in beta version. Web Browser with HTML 5 is required.

is not as good, thus draining the batter quicker.

2.2.1 Smartphones as RF Sensors: iPhone Application

The iphone platform was chosen for the implementation of the smart RF sensor application. The iPhone's *official* APIs (application programming interfaces) neither provide access to RSSI (RSS Indicator), nor to cellular network information, which is necessary for implementing the smart RF sensor. Consequently, jailbreaking the iPhone is necessary in order to grant access to this information. Thus, the application is able to submit AT Commands to the baseband's socket (modem) in order to gather and record the desired measurements. Each measurement includes RSSI and relevant cellular network information: Network Carrier Name, Network Type, Location Area Code, Absolute Radio Frequency Channel (ARFCN), Cell Identity, neighbouring cell towers' information, transmit power level and several other network pa-
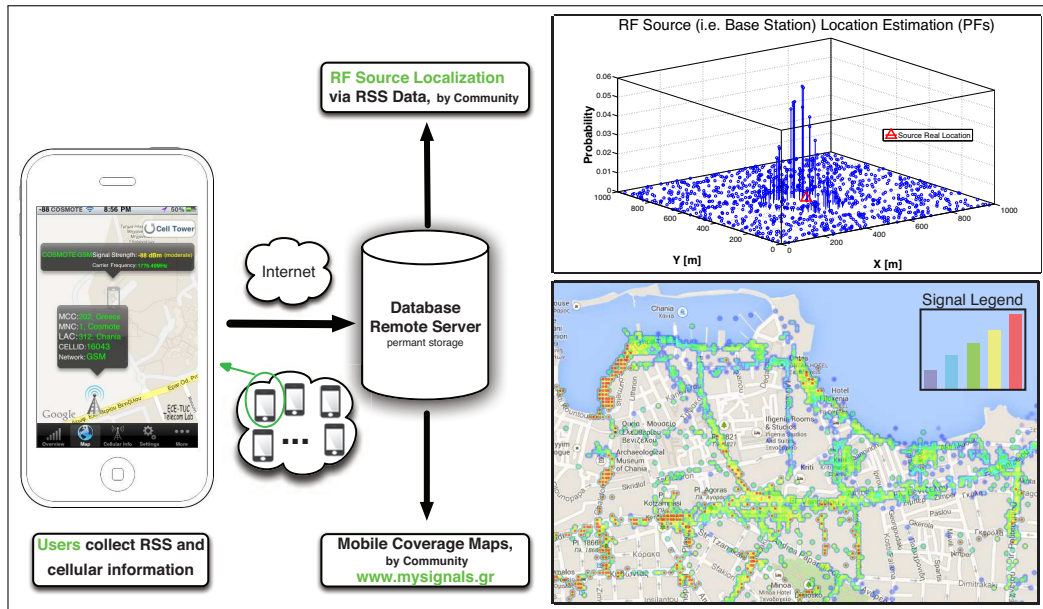
Figure 2.2: Implemented community RF sensing: measurements from users' smartphones (e.g. RSS, GPS location) are gathered at a web database for mobile coverage maps (www.mysignals.gr) and RF-source localization.
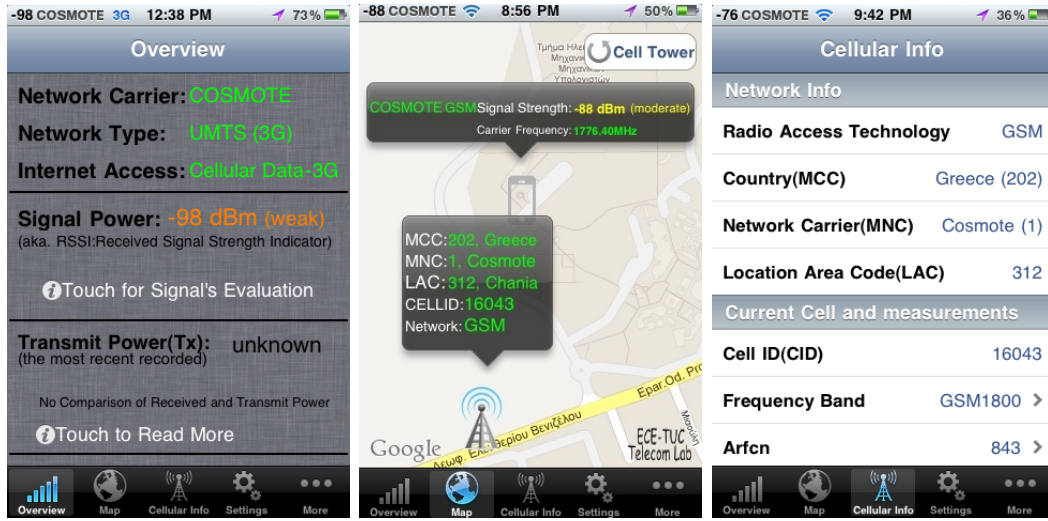
Figure 2.3: The *MySignals* application utilizes the smartphone as a RF Sensor: It records the received signal strength (RSS), GPS location, and relevant cellular network information (e.g. cell-ID, carrier frequency). Measurements are uploaded periodically to the central web server for permanent storage.

rameters (see Fig. 2.9). In addition, MySignals records the measurements' timestamp and the mobile's location through the GPS module of the iPhone. All the aforementioned cellular network information is displayed by a user-friendly graphical interface (e.g. Fig. 2.3, 2.4 and 2.5). In addition, users can be informed about the basic principles and practical aspects of mobile phones and cellular network operations.

Each measurement is saved locally in the iPhone's storage (i.e. data cache) and more specifically in an SQLite database, utilizing the Core Data framework and an SQLite wrapper provided by iPhone software development kit(SDK). In regular time intervals or when the user selects it (see Fig. 2.5), all these measurements are packetized using a custom implemented protocol based on JSON[1]. Then, data is sent to the central web server for permanent storage through HTTP protocol. Extensive discussion on the application is included in [26].

---

[1]JSON (JavaScript Object Notation) is a lightweight data-interchange format, commonly used by web services.
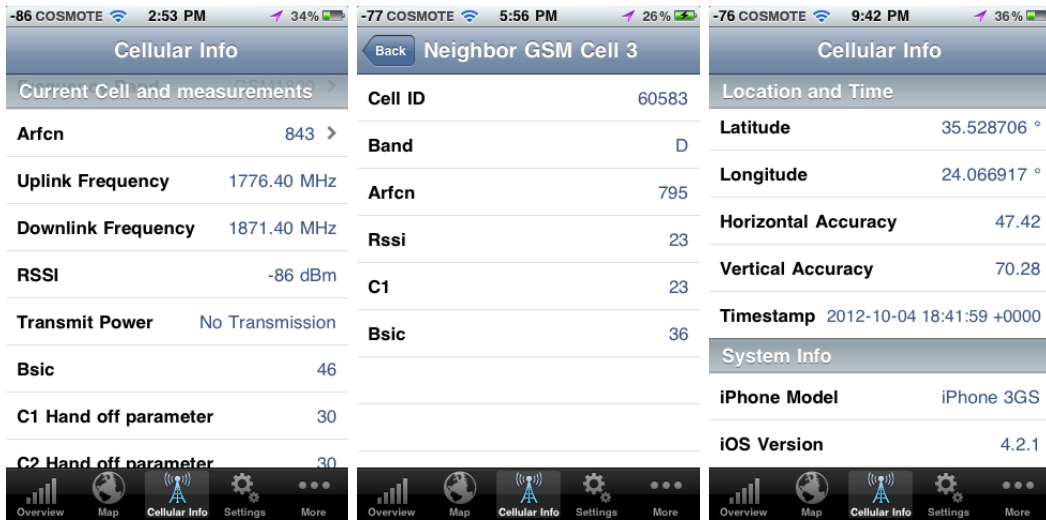
Figure 2.4: Left: Detailed cellular network information (e.g. uplink/downlink frequency). Center: Neighbour cell details. Right: Mobile's location details (e.g. GPS coordinates, expected accuracy) and measurement's timestamp.

2.2.2 Web Server & Database

The measurements are unpacked on the central web server via a custom implemented JSON parser and saved permanently in a MySQL database (DB schema is depicted in Fig. 2.9). Thus, data is available for processing and visualization by the mobile coverage maps. The web server database is encapsulated for security reasons, by an appropriate web service written in PHP and served by an Apache 5.0 HTTP server. The server is hosted by the Network Operation Center's (NOC) data center[1] in TUC on an Ubuntu Server 11.04 machine. Mobile coverage maps created by the users themselves are available online at the site www.mysignals.gr and a preview can be seen in Fig. 2.7 and Fig. 2.8. Coverage maps are implemented as heatmaps, i.e. the RSS level is represented by a different color code, and the users can be informed about the network quality per mobile telephony company and network type (2G or 3G). Complementary to [26], this work developed a graphical web tool [2] which displays figures on web browsers; RSS measurements of a specific user at a specific location are plotted throughout time

---

[1]Available online 24h/7d since NOC's data center is UPS supported .

[2]http://www.mysignals.gr/monitorAndRetrieveGraphsPage.php
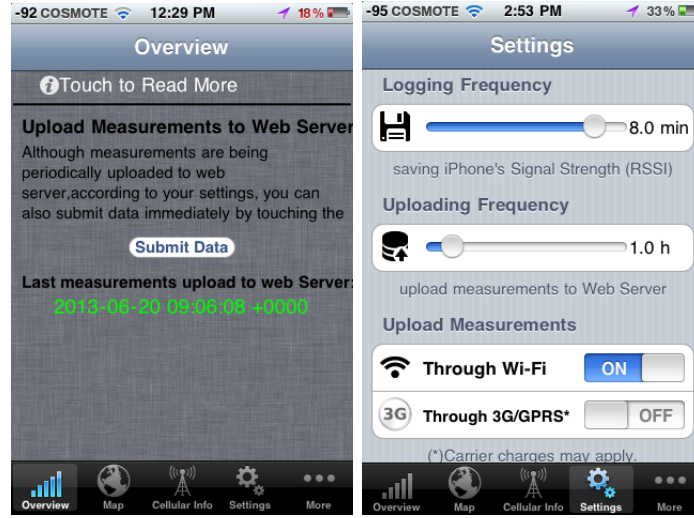
Figure 2.5: Left: Trigger for manual upload to the server and time of the last submission. Right: MySignals settings.

(an example is depicted in Fig. 2.6). This tool is of immense importance for research and quick data disambiguation (e.g. understanding the time variant nature of RSS).
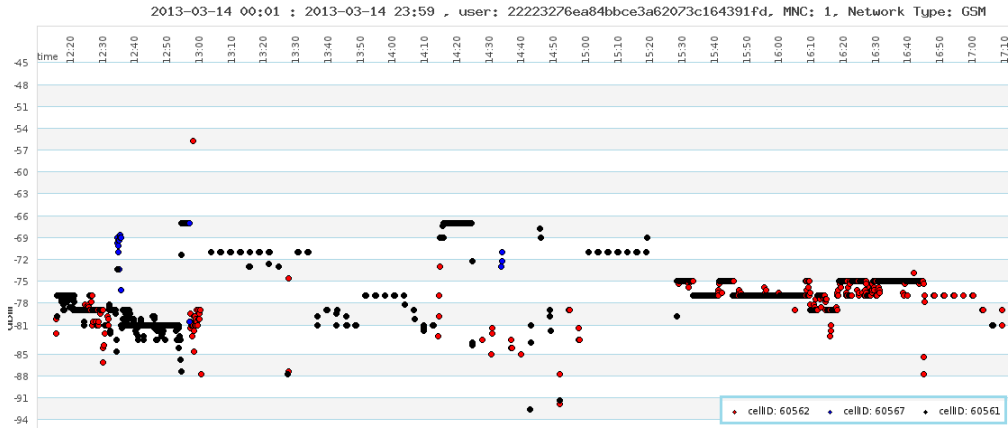
Figure 2.6: RSS as a function of time for a specific user at a specific location, generated by the graphical web tool. The large RSS fluctuations are explained by the fading during the busy noon hours.

Hence, the presented platform allows diverse research and network engineering. Further details can be found in [26]. In this work, the collected RSS measurements are utilized for RF-source localization, subsequently presented
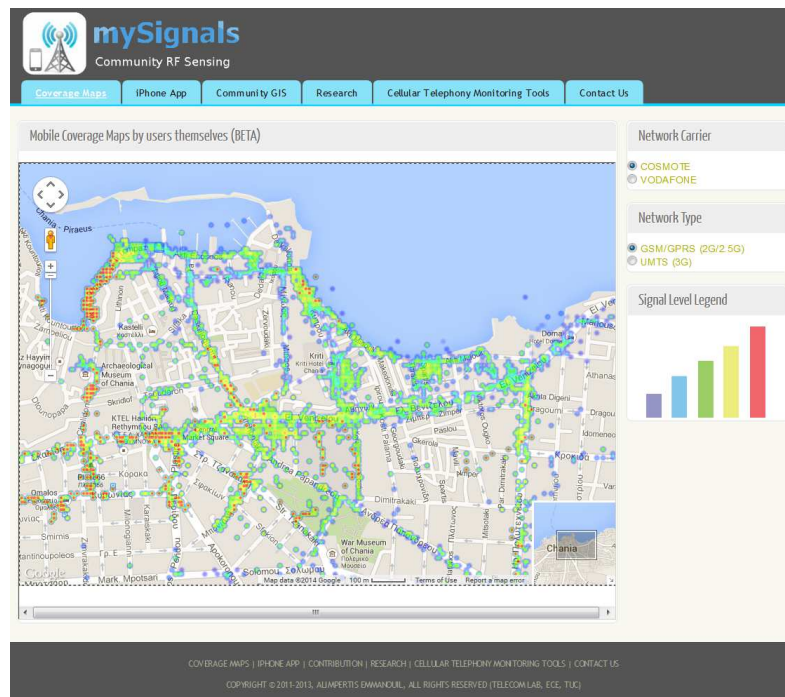
Figure 2.7: MySignals website demonstration. Users can select among the available network carriers and network types to determine the signal quality.

in chapter 3.
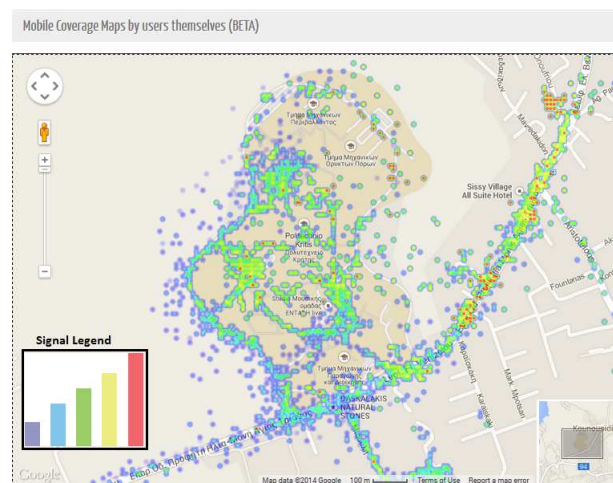
Figure 2.8: Cosmote GSM coverage map at TUC campus, Chania, Crete, Greece. Weak purple color indicates very weak signal, while the red color indicates strong signal. Community revealed areas with weak signal.
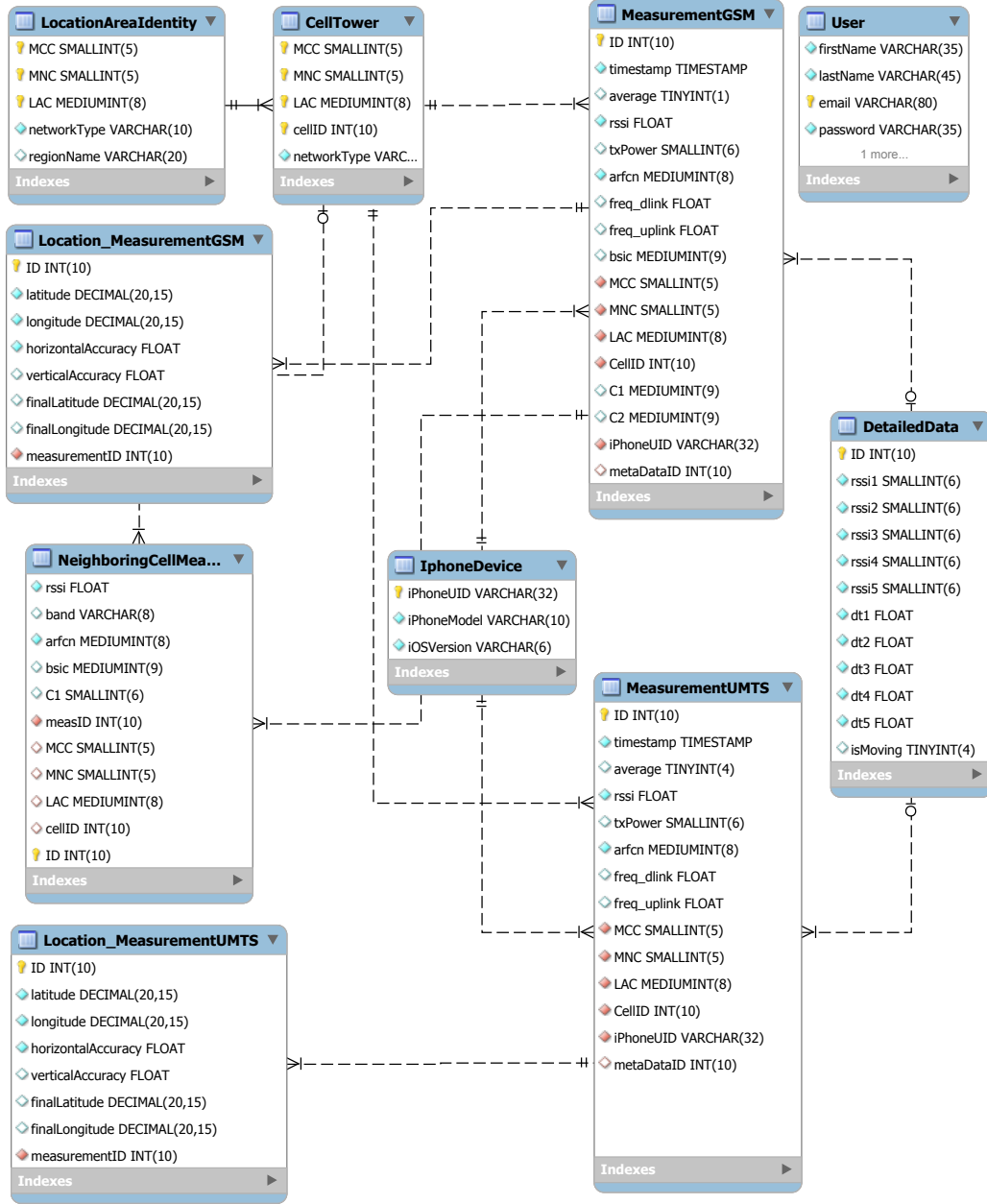
Figure 2.9: MySignals database (DB) schema for permanent storage. The schema indicates the application domain, i.e. the specific parameters that are recorded.

Chapter 3

Community RF Sensing: Source Location Estimation

3.1 System Model

In this chapter, unknown RF source location $\mathbf{x}_{\mathrm{BS}} = \begin{bmatrix} x_{\mathrm{BS}} & y_{\mathrm{BS}} \end{bmatrix}^T$ will be estimated utilizing a vast number of RSS measurements, readily available from the described community of the smartphone users, at locations $\mathbf{x} \triangleq \begin{bmatrix} \mathbf{x}_1 & \cdots & \mathbf{x}_N \end{bmatrix}$. Careful system modeling should be done in order to take into account real world system parameters and practical aspects for the localization algorithm.

3.1.1 Received Signal Strength (RSS)

Each user j at a specific location records κ RSS measurements at time instances $t_1, t_2, \ldots, t_\kappa$, for each specific cell-ID: $\mathbf{z}^{[j,\mathrm{cID}]} \triangleq \begin{bmatrix} P_{[j,\mathrm{cID}]}^{(t_1)} & \cdots & P_{[j,\mathrm{cID}]}^{(t_\kappa)} \end{bmatrix}^T$. The collection of all measurements is denoted by $\mathbf{z}^{[\mathrm{cID}]} \triangleq \begin{bmatrix} \mathbf{z}^{[1,\mathrm{cID}]} & \cdots & \mathbf{z}^{[N,\mathrm{cID}]} \end{bmatrix}$.

The RSS measurement (in dBm) for user j from a serving cell is modeled as a random variable that follows the log-normal distribution [27], [9], i.e. Gaussian distributed in dB, with distinct PLE and variance:

$$P_{[j,\mathrm{cID}]}^{(t)} = P_0^{(t)} - 10 n_j \log_{10}\left(\frac{\|\mathbf{x}_{\mathrm{BS}} - \mathbf{x}_j\|_2}{d_0} \right) + w_j^{(t)}, \tag{3.1}$$

where $P_0^{(t)}$ is the received power at reference distance d_0 ($d_0 = 1\mathrm{m}$ in this work) and is calculated by the free-space path loss (Friis) transmission equation, with downlink frequency corresponding to the specific cell ID (typically at the 1800 MHz regime), user antenna gain equal to 0 dBi and base sta-

Number of measurements for the studied cells, at fixed users locations:

	cell-ID				
	60561	**60562**	**60563**	**60565**	**60567**
User 1	-	85.499	193.658	-	54.826
User 2	422.441	227.319	-	-	45.866
User 3	365.858	306.344	-	-	426
User 4	413.400	47.123	-	8.182	2.028
User 5	320.162	95.607	-	145.7	6.609

Table 3.1: Timespan: 13-09-2012 to 23-04-2013. Users were asked to collect RSS measurements at their homes in order to study RSS behaviour over a large time interval. Other cells are omitted since their locations are unknown.

tion antenna gain as explained below. Parameters n_j, w_j are the PLE and measurement noise, respectively, of the specific user j. Measurement noise is modeled as a zero-mean Gaussian with variance σ_j^2 (expressed in dB). In sharp contrast with prior art, this work considers distinct PLE and noise variance values across users. Prior work has mainly focused on propagation models where the PLE is assumed equal across all users, which is untrue for real environments. Details about Eq. (3.1) can be found in the Appendix.

3.1.2 Transmission Power

Prior art assumes that the transmission power of the RF source remains constant during time, however, commercial base stations perform downlink power control in order to save energy in low traffic conditions and avoid interferences to neighbouring frequencies. More specifically, a specific downlink channel of the BS is of interest, called broadcast control channel (BCCH), which is used by all the commercial mobile phones to measure the RSS [1], [28].

Commercial implementations of BCCH power control (e.g. [2], [3]) utilize two different transmission power levels. The BS transmits at maximum power when the network traffic is high; otherwise, when the BCCH software controller detects low traffic, the transmitted power is decreased by 2 dB [1], [2], [3].
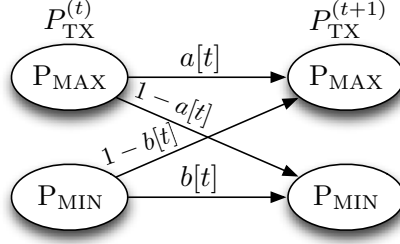
Figure 3.1: The two state Markov model for the two-level RF source transmission power. The model reflects the power control at the broadcast control channel (BCCH) [1], [2], [3] to save energy and reduce interferences, during low network traffic.

Hence, the transmission power $P_{\text{TX}}^{(t)}$ of the RF source is modeled as a binary random variable with values P_{MIN} and P_{MAX} (Fig. 3.1). The exact value of $P_{\text{TX}}^{(t)}$ is a priori unknown and must be estimated. A Markov chain is used to model the transition between $P_{\text{TX}}^{(t)}$ and $P_{\text{TX}}^{(t+1)}$ with transition probabilities that depend on the traffic load (Fig. 3.1); when traffic load increases, the probability for transmission at maximum power will also increase.

According to [29], GSM call arrivals in a cell are modelled satisfactorily by Poisson arrivals with a time variant arrival rate $\lambda(t)$[1]. The occupied slots, $s(t)$, in a cell can be expressed as a function of time:

$$s(t) = n(t) + n(t-1) - d(t), \tag{3.2}$$

where time t is discretized in seconds, $n(t)$ quantifies new users' arrivals in the cell, $\lambda(t)$ assigned real world values according to [1], $n(t-1)$ indicates the slots that are already occupied and $d(t)$ specifies the departures from the cell. The service time of each new user follows the exponential distribution with an average value $\mu = 100$ sec. Fig. 3.2 presents a realization of the stochastic process $s(t)$ during a day and the number of offered slots by the cell.

Considering the power control performed by the BCCH transmitters, the

---

[1]In other words, a non-homogeneous Poisson process.
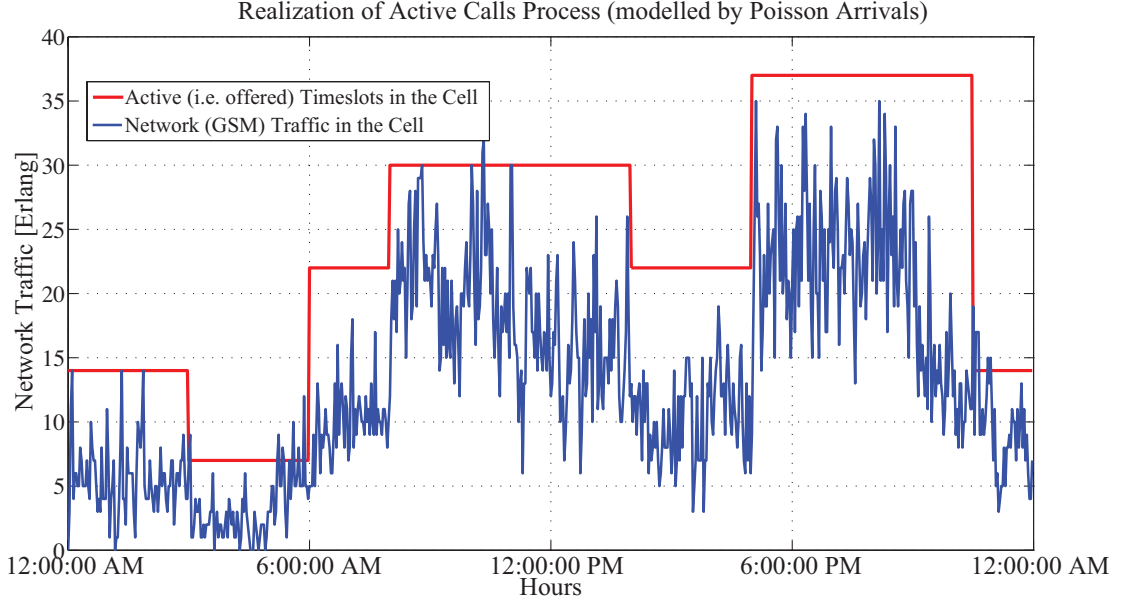
Figure 3.2: A realization of the stochastic process $s(t)$: Number of occupied slots in the cell and the offered slots are presented during day's hours.

stochastic process which models the transmitted power can be expressed as:

$$P_{\text{TX}}^{(t)} = \begin{cases} \text{P}_{\text{MAX}}, & h(t) \geq l, \\ \text{P}_{\text{MIN}}, & h(t) < l, \end{cases} \qquad (3.3)$$

where, $h(t) = \frac{s(t)}{c(t)}$, with $c(t)$ offered in [1] and $l = 50\%$ selected as a generic threshold for high traffic load into a cell [30].

The cumulative density function (CDF) of r.v $s(t = t_0)$ does not have a closed form expression[1]. Thus, we emulate $K = 10000$ realizations, i.e. days, of $P_{\text{TX}}^{(t)}$, in order to calculate transition probabilities. Consequently, transition probabilities $a[t], b[t]$ for the 2-state Markov model of Fig. 3.1 are estimated by counting the transitions at each specific hour of the day. The calculated probabilities are presented in Fig. 3.3, indicating that the BS is likely to transmit with P_{MAX} at busy hours.

Last but not least, it is noted that these 2 dB fluctuations are reflected

---

[1]Departures from the cell, $d(t)$, is a Laplace distributed random variable since interleaving time of a user is the difference between 2 exponential distributed random variables.

Probability of Retaining the State P$_{\text{MAX}}$

Probability of Retaining the State P$_{\text{MIN}}$
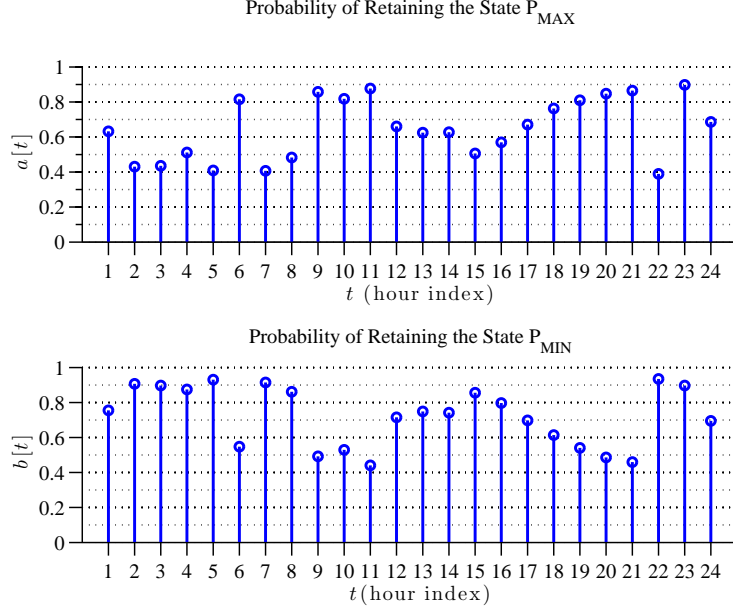
Figure 3.3: Estimated transitions probabilties for the two-state Markov model (3.1). When traffic load increases, the probability for transmission at maximum power will also increase.

experimentally in the RSS level of the collected data, especially during night hours when the RSS is affected less by the fading (see Fig. 3.4).

3.1.3 RF Source Antenna

A typical base station in a cellular network consists of three (or more) sectors (i.e. cells), typically served by directional antennas. For example, Figure 3.6 demonstrates the measurements' cell-IDs at Chania center, indicating the split of the serving area into sectors.

Directional antennas have a very complex radiation pattern with multiple peeks and nulls [4] (e.g. in Fig. 3.5). A simplified 4-parameter model of a directional antenna is utilized in this work (Fig. 3.7), which reflects the basic radiation characteristics of the directional antennas. Specifically, a main antenna lobe at angle direction ϕ is assumed (with respect to the x-axis), with lobe opening of $2\phi_s$. The base station-RF source antenna gain at

RSSI Demonstratiion at Anchor 2
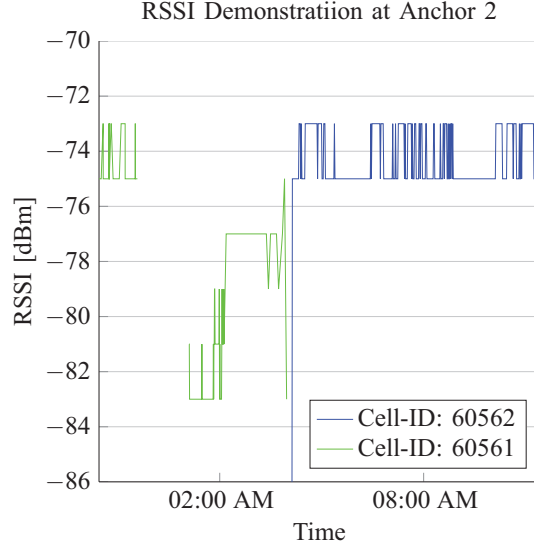
Figure 3.4: Collected data during night hours. The power control (Fig. 3.1) is reflected to the RSS since fading is lower during night .

direction ϕ_j is given by (Fig. 3.7):

$$G_H(\phi_j, \phi) = \begin{cases} G_0, & \phi - \phi_s \leq \phi_j \leq \phi + \phi_s, \\ G_{\text{SLL}}, & \phi + \phi_s < \phi_j \leq \phi + 2\phi_s \\ & \text{or} \quad \phi - \phi_s > \phi_j \geq \phi - 2\phi_s, \\ G_{\text{BLL}}, & \text{elsewhere.} \end{cases} \tag{3.4}$$

Model parameters are assigned values from commercial GSM directional antennas: $\phi_s = 30°$, $G_0 = 0$ dB, $G_{\text{SLL}} = -3$ dB for the side lobe levels and $G_{\text{BLL}} = -23$ dB for the backside lobe level (BLL) (e.g. similar values for BLL and ϕ_s can be found in [31]). The angle direction ϕ of base station-RF source antenna is unknown and must be estimated, while for the omnidirectional (isotropic) base station-RF source antenna, $G_H(\phi_j, \phi) = 0$ dB, $\forall (\phi_j, \phi)$. Thus, the RF source radiated power at angle ϕ_j can be expressed as:

$$P_{\text{TX}}^{(t)}(\phi_j, \phi) = P_{\text{TX}}^{(t)} + G_H(\phi_j, \phi) \text{ (dBm).} \tag{3.5}$$

In sharp contrast to prior art, in this work the 4-parameter model will be

(a) Sector Antenna 3D Pattern (b) Sector Antenna 3D Pattern (c) Sector Antenna 3D Pattern
Side View Front View

(d) Sector Antenna 3D Pattern (e) Sector Antenna (f) Sector Antenna
Top View Azimuth Plane Pattern Elevation Plane Pattern
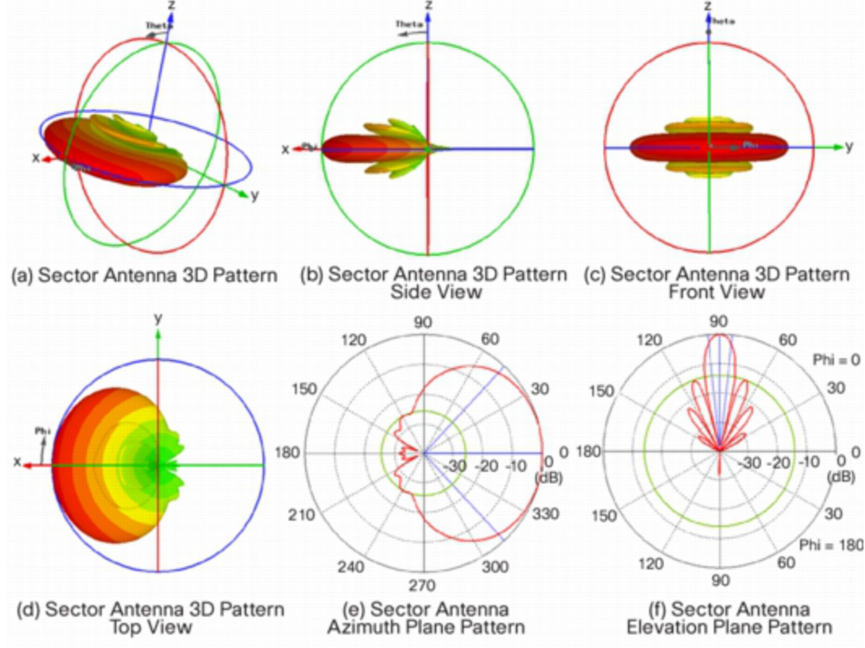
Figure 3.5: GSM sector antenna radiation pattern (Cisco networks [4]).

compared to the isotropic antenna model. It is confirmed that the simplified model is beneficial in real environments, since it exploits essential propagation characteristics and simultaneously avoids complex analytical modeling.

3.2 Estimation Algorithm

The goal is to estimate vector $\boldsymbol{\theta}^{(t)}$, with all the unknowns (including RF source coordinates), from *real-world measurements* $\mathbf{z}^{[\text{cID}]}$, provided by the community of N smartphones-RF sensors:

$$\boldsymbol{\theta}^{(t)} \triangleq \begin{bmatrix} x_{\text{BS}} & y_{\text{BS}} & \phi & P_{\text{TX}}^{(t)} & n_1 \cdots n_N \end{bmatrix}^T. \tag{3.6}$$

It was experimentally found that an initial estimate of the PLEs reduced the localization error, in contrast to the case where PLEs were randomly initialized. That can be explained by the fact that a small variance in PLE changes significantly the RSS according to eq. (3.1). An initial estimate of $\widehat{\mathbf{x}}_{\text{BS}}^{\text{init}}$ is given by the voting algorithm in [32], where PLEs are considered
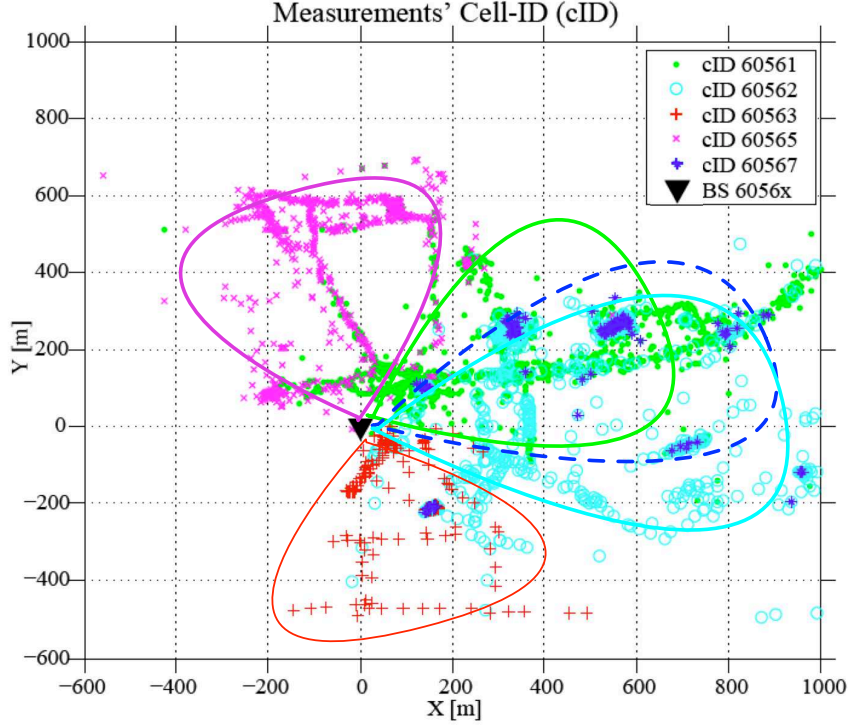
Figure 3.6: Demonstration of the measurements' cell-ID (collected by users' community), indicating the split of the base station's serving area into sectors (i.e. cells). Each cell is served by a distinct directional antenna, roughly illustrated by the corresponding lobe. The presented BS is at Chania centre.

unknown and bounded. Thus, an initial estimate of $\widehat{n}_j$ results from Eq. (3.1):

$$\widehat{n}_j = \frac{\overline{P}_{0_{\mathrm{MAX}}} - (1/\kappa) \sum_{i=1}^{\kappa} P_{[j,\mathrm{cID}]}^{(t_i)}}{10 \log_{10} \|\mathbf{x}_j - \widehat{\mathbf{x}}_{\mathrm{BS}}^{\mathrm{init}}\|_2}, \forall\, j, \tag{3.7}$$

where, $d_0 = 1$m, $\overline{P}_{0_{\mathrm{MAX}}}$ is the received power at $d_0 = 1$m given by the Friis transmission equation (free space path-loss), assuming that the base station is transmitting at $\mathrm{P}_{\mathrm{MAX}}$ and κ RSS measurements were randomly selected for each user j. Although $\widehat{n}_j$ may be in error due to imperfect initial estimation, the estimation algorithm handles this inaccuracy as explained further down.

The base station-RF Source location estimation, i.e. $\boldsymbol{\theta}^{(t)}$ estimation, can be performed if the probability density $p(\boldsymbol{\theta}|\mathbf{z}^{[\mathrm{cID}]})$ is available. More specifically, $p(\boldsymbol{\theta}|\mathbf{z}^{[\mathrm{cID}]})$ is modeled and estimated with non-parametric procedures
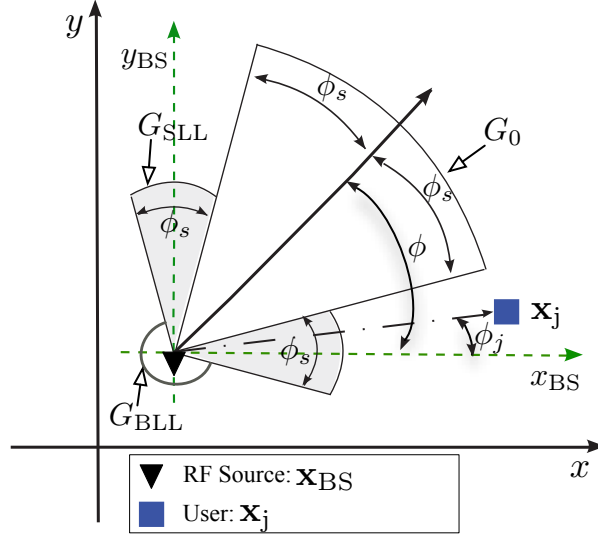
Figure 3.7: Simple 4-parameter RF source directional antenna gain modeling. Parameters $G_0, \phi_s, G_{\mathrm{SLL}}, G_{\mathrm{BLL}}$ are needed.

based on particle filtering [33]. Specifically, M particles at time t are considered, with corresponding weights $\{w_t^{[m]}\}$:

$$\left\{ \boldsymbol{\theta}_t^{[m]} = \begin{bmatrix} x_{\mathrm{BS}}^{[m]} & y_{\mathrm{BS}}^{[m]} & \phi^{[m]} & P_{\mathrm{TX}}^{(t),[m]} & n_1^{[m]} \cdots n_N^{[m]} \end{bmatrix}^T \right\}.$$

Particle filtering consists of two phases; the prediction operation, where particles are drawn from the state transition model in order to consider the time variant parameters of the state and the correction operation which incorporates the likelihood of the observed measurements (i.e. update phase). Resampling of the particles is performed after the prediction and the update phase, but may also be performed after a set of correction phases.

The RF source is assumed immobile since the base station is installed at a fixed location. For the case of RF source directional antenna, each cell is illuminated by the corresponding directional antenna at a fixed direction (unchanged for the measurement period). Moreover, for the time window of utilized experiments, the PLEs are considered constant.

Thus, the *update* operation of particle filtering is restricted to the trans-

mission power of the base station and is given by:

$$P_{\text{TX}}^{(t),[m]} \sim \text{Pr}\left(P_{\text{TX}}^{(t),[m]}|P_{\text{TX}}^{(t-1),[m]}\right), \tag{3.8}$$

where the conditional probability is described by the Markov chain of Fig. 3.1, as discussed in 3.1.2, and the utilized values are given in Fig. 3.3.

The *correction* operation for each particle weight at time t is given by:

$$w_t^{[m]} = p\left(\mathbf{z}^{(t)}|\boldsymbol{\theta}_t^{[m]}\right) = \prod_{j=1}^{N} p\left(P_{[j]}^{(t)}|\boldsymbol{\theta}_t^{[m]}\right), \tag{3.9}$$

where independence of RSS measurements across different users has been exploited. The conditional p.d.f. value of each measurement is based on the log-normal p.d.f. (Eq. (3.1)):

$$p\left(P_{[j]}^{(t)}|\boldsymbol{\theta}_t^{[m]}\right) = \frac{1}{\sigma_j\sqrt{2\pi}}\exp\left(-\left(P_{[j]}^{(t)} - \overline{P_{[m,j]}^{(t)}}\right)^2 \Big/ 2\sigma_j^2\right). \tag{3.10}$$

Parameter $\overline{P_{[m,j]}^{(t)}} \triangleq \mathbb{E}\left[P_{[j]}^{(t)}|\boldsymbol{\theta}_t^{[m]}\right]$ is the expected value of RSS at location $\mathbf{x}_j$, given $\boldsymbol{\theta}_t^{[m]}$:

$$\overline{P_{[m,j]}^{(t)}} = P_0^{(t),[m]} - 10n_j^{[m]}\log_{10}\left(\frac{\|\mathbf{x}_{\text{BS}}^{[m]} - \mathbf{x}_j\|_2}{d_0}\right), \tag{3.11}$$

where $P_0^{(t),[m]}$ is the received signal strength at reference distance $d_0 = 1\text{m}$ calculated by the Friis transmission equation with base station transmission power equal to $P_{\text{TX}}^{(t),[m]}$ and base station cell antenna gain given by Eq. (3.4). Angle ϕ_j for user j given $x_{\text{BS}}^{[m]}, y_{\text{BS}}^{[m]}$ is computed from Fig. 3.7:

$$\phi_j = \arctan\left(\frac{y_j - y_{\text{BS}}^{[m]}}{x_j - x_{\text{BS}}^{[m]}}\right). \tag{3.12}$$

The standard deviation σ_j is estimated from the whole measurement data-set for user j at a fixed location, utilizing standard techniques for parameter estimation with Gaussian random variables (the RSS in dBm values are assumed

Gaussian random variables according to Eq. (3.1)) [34].

For the particles' resampling, the low-variance sampling procedure of the particles was applied [33]. The pseudo-code of the PF follows [35].

PF Algorithm: Particle Filtering for estimating $p(\boldsymbol{\theta}|\mathbf{z}^s)$

---

(1): **Initialization of Variables:**

(2): Set M (number of Particles),

(3): X, Y (dimensions of area of interest), T (time window).

(4): **Initialization of Particles,** $\forall\, m = 1 : M$

(5): $\quad x_{t=0}^{[m]} \sim \mathcal{U}[0, X],\ y_{t=0}^{[m]} \sim \mathcal{U}[0, Y],\ \phi_{t=0}^{[m]} \sim \mathcal{U}[0, 2\pi].$

(6): $\quad P_{\text{TX}}^{(t=0),[m]} = b,\ b \in \{P_{\text{MIN}},\ P_{\text{MAX}}\},\ \Pr(b) = 0.5.$

(7): $\quad n_{j,t=0}^{[m]} \sim \mathcal{N}\left(\widehat{n}_j, \sigma_n^2\right),$ with $\widehat{n}_j$ from (3.7).

(8): $\quad \boldsymbol{\theta}_{t=0}^{[m]} = \begin{bmatrix} x_{\text{BS}}^{[m]} & y_{\text{BS}}^{[m]} & \phi^{[m]} & P_{\text{TX}}^{(t),[m]} & n_1^{[m]} \cdots n_N^{[m]} \end{bmatrix}^T.$

(9): $\mathbf{z}^s \leftarrow$ **Select** T consecutive RSS measurements from $\mathbf{z}^{[\text{cID}]}$

(10): **for** $t = 1 : T$ **do** {*time-step*}

(11): $\quad$ **for** $m = 1 : M$ **do** {*particle index*}

(12): $\quad\quad$ Sample $P_{\text{TX}}^{(t),[m]} \sim \Pr\left(P_{\text{TX}}^{(t),[m]} | P_{\text{TX}}^{(t-1),[m]}\right).$

(13): $\quad\quad$ Calc. $\phi_j,\ \forall j,$ from (3.12).

(14): $\quad\quad$ Calc. $P_{\text{TX}}^{(t)}(\phi_j, \phi^{[m]}),\ \forall j$ from (3.5) given $\boldsymbol{\theta}_t^{[m]}.$

(15): $\quad\quad$ $w_t^{[m]} = p\left(\mathbf{z}^{(t),s}|\boldsymbol{\theta}_t^{[m]}\right),$ from (5.21).

(16): $\quad$ **end for**

(17) $\quad$ Normalize weights $\boldsymbol{w}_t^{[1:M]}.$

(18) $\quad$ $\boldsymbol{\theta}_t^{[1:M]} \leftarrow$ Low-VarianceSampler $\left(\boldsymbol{\theta}_t^{[1:M]}, \boldsymbol{w}_t^{[1:M]}\right).$

(19): **end for**

At the end of particle filtering algorithm the final particles $\boldsymbol{\theta}_T^{[1:M]}$ produce an estimate of the conditional density function $p(\boldsymbol{\theta}|\mathbf{z}^s)$ using the histogram approach [33]. With marginalization, an estimate of the conditional density function $p(\mathbf{x}_{\text{BS}}|\mathbf{z}^s)$ is readily available. The estimate of base station location

$\widehat{\mathbf{x}}_{\mathrm{BS}}$ is offered by the conditional mean:

$$\widehat{\mathbf{x}}_{\mathrm{BS}} = [\widehat{x}_{\mathrm{BS}} \ \ \widehat{y}_{\mathrm{BS}}]^T = \mathbb{E}[\mathbf{x}_{\mathrm{BS}}|\mathbf{z}^s]. \tag{3.13}$$

The procedure is repeated for K different samples $\mathbf{z}^s$ and the final estimation is the average value of all estimates:

$$\widehat{\mathbf{x}}_{\mathrm{BS}}^{mean} = \sum_{k=1}^{K} \frac{1}{K} [\widehat{x}_{\mathrm{BS}}^k \ \ \widehat{y}_{\mathrm{BS}}^k]^T. \tag{3.14}$$

3.3 Results

In this section, numerical results are presented for real-world GSM RSS measurements from similar sensitivity smartphones. The comparison of our approach with prior art is limited to techniques applicable to real-world, non-simulated data. The number of particles M is set to $M = 140000$, $X = Y = 1000$ m and $T = 30$ or $T = 60$ min (line (2) of the algorithm), with approximately 1 measurement per minute per user. It is noted that PFs explore values around the imperfect $\widehat{n}_j$ and finally converge to more accurate PLEs values, therefore, the effect of selecting a value interval for this variance (σ_n) should be analysed. In line (7) of the algorithm, $\sigma_n = 0.3$ has been chosen heuristically (as explained below in Fig. 3.10 and Table 3.3), because a smaller value resulted in particle depletion problem [33], while a larger value also required a larger number of particles. The values $\mathrm{P_{MAX}} = 43.5$ dBm, $\mathrm{P_{MIN}} = 41.5$ dBm were provided by the mobile telephony provider specifications. As explained previously in 3.2, locations $\mathbf{x}$ are apriori known; the GPS coordinates just validate that users are at their predetermined locations.

Fig. 3.8-(a) offers the final estimated base station-RF source location, in which $K = 2000$ different datasets of measurements were used, for $N = 4$ users and a specific cell (60562). In other words, $2000 \times 60 \times 4 = 480000$ independent RSS measurements were utilized. The RF source antenna was assumed isotropic (no directionality). The reported estimated value is based on Eq. (3.14) and the true location is also depicted. An additional user is added in Fig. 3.8-(b) (i.e. $N = 5$) and the estimation is repeated without
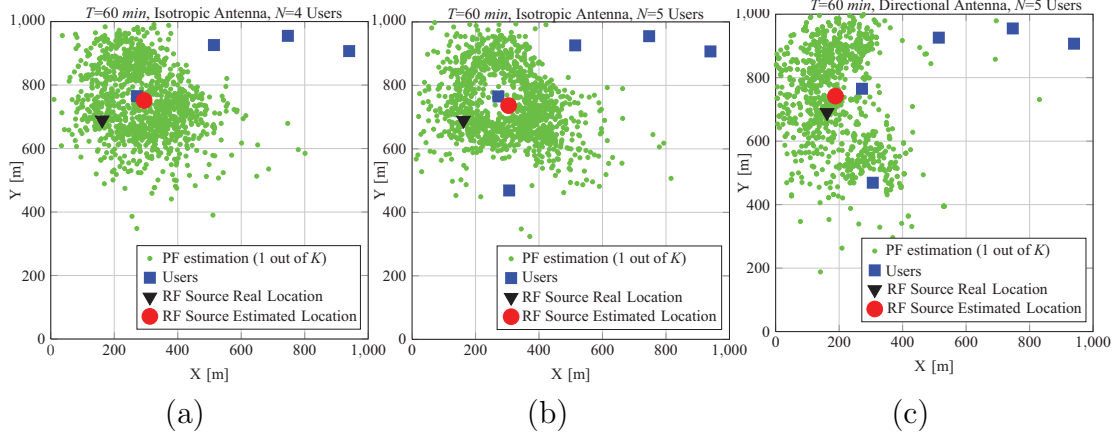
Figure 3.8: Results for cell-ID 60562 located at the city of Chania city center. $K = 2000$ different PF runs were performed. The incorporation of the directionality antenna model, removes the bias and the right part of the estimations' circle. The displayed grid coincides with the map in Fig. 2.1.

significant improvement. When the antenna directionality model is included (Fig. 3.8-(c)), specific areas of interest are excluded and the final estimate is significantly improved. In other words, the rich measurement dataset, due to the community RF sensing infrastructure, was beneficial when the (simple) base station-RF source antenna directionality model was incorporated. Indeed, a directional antenna could not actually serve the users if it was in the right part of the estimations' circle (Fig. 3.8 since it mainly radiates towards one direction (see Fig. 3.5). Thus, the right part of the estimations' circle is excluded by the PFs estimations in 3.8-(c).

Table 3.2 shows that the absolute location error in cell 60562 with base station-RF source directionality modeling is approximately three times smaller

Absolute Localization Error(m)

	1	2	3	4	5	6
60561	516.9	382.4	126.7	93.6	84.2	**48.2**
60562	277.7	419.2	158.3	145.7	149.6	**58.3**

Table 3.2: 1. Top-K RSSI, 2. Strongest RSSI, 3. Grid Voting. 4., 5. PF-Isotropic Antenna ($N = 4$ and $N = 5$ respectively), 6. PF-Directional Antenna.
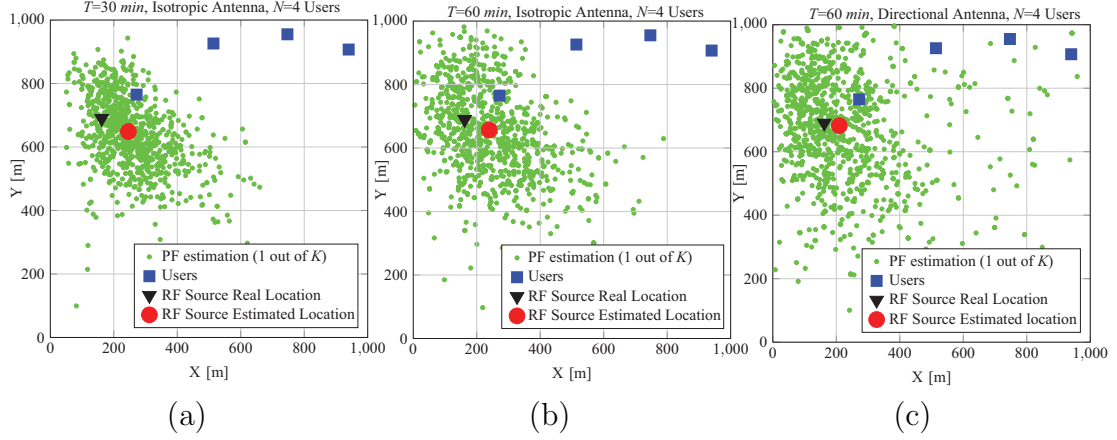
Figure 3.9: Results for cell-ID 60561 located at the city of Chania city center. $K = 2000$ different PF runs were performed. The incorporation of the directionality antenna model, removes the bias from the isotropic antenna.

(scenario 6) compared to the case with isotropic antennas (scenarios 4, 5). It is emphasized that the reported localization error on the order of 50m is achieved even when communication distances between smartphone users and RF source can exceed 800m. Performance of other techniques applicable to real-world measurements (and discussed in the introduction), namely top-K (scenario 1), strongest RSS (scenario 2) [17], [18], [19] and grid voting [32] (scenario 3, Eq. (3.7), $\kappa = 1500$) are also reported. Top-K and strongest RSS algorithms introduce large errors due to the oversimplification of the estimation. Thus, even a few line of sight measurements (LOS) at a far distance from the BS, break down the algorithm since these two algorithms return an average of locations with the strongest measurement. In contradiction, the proposed approach carefully models the wireless propagation and does not have such a problem since it utilizes independently K different datasets.

Similar results were obtained for the cell 60561, which are presented in Fig. 3.9. Again, $K = 2000$ different datasets which were utilized (i.e. K independent estimations by PFs) for $N = 4$ users (only 4 users were served by this cell, see Table 3.1. Fig. 3.9-(a) illustrates the base station location estimation for the isotropic antenna model and $T = 30 \ min$. In Fig. 3.9-(b) $T = 60 \ min$ is utilized and the estimation is slightly improved. However,

once again, the big improvement and the bias removal are achieved when the directional antenna model is incorporated (Fig. 3.9-(c)). The directional model reflects the actual radiation pattern by the BS, therefore, PFs better explores the problem state converging to more likely states.

Finally, experimental results considering different values of σ_n (line 7 of the proposed algorithm) are presented in Fig. 3.10 in order to explain the heuristic selection of the σ_n. Specifically, Table 3.3 shows experimental results for σ_n=[0.1, 0.2, 0.3, 0.4, 0.5] for the following scenario: 60562, $N = 5$, $T = 60\ min$, Directional Antenna. The provided results validate that smaller σ_n results in the particle depletion problem, leading to larger errors. On the other hand, larger σ_n results in greater error since a large number number of particles is required to explore the larger state space. Even small changes in n_j (see eq. 3.1) may significantly change the RSS. For the interested readers, work in [36] investigates in detail the effect of an imperfect estimation of the PLE (however, authors assume that PLE is unique and equal across all users).

Absolute Localization Error (m)

σ_n	0.1	0.2	0.3	0.4	0.5
Fig. 4-(c) Scenario	99.4	95.9	58.3	76.2	153.7

Table 3.3: cellID: 60562, $N = 5$, $T = 60\ min$, Directional Antenna. Experimental results for σ_n=[0.1, 0.2, 0.3, 0.4, 0.5].

(a) $\sigma_n = 0.1$

(b) $\sigma_n = 0.2$

(a) $\sigma_n = 0.3$

(d) $\sigma_n = 0.4$

(e) $\sigma_n = 0.5$.
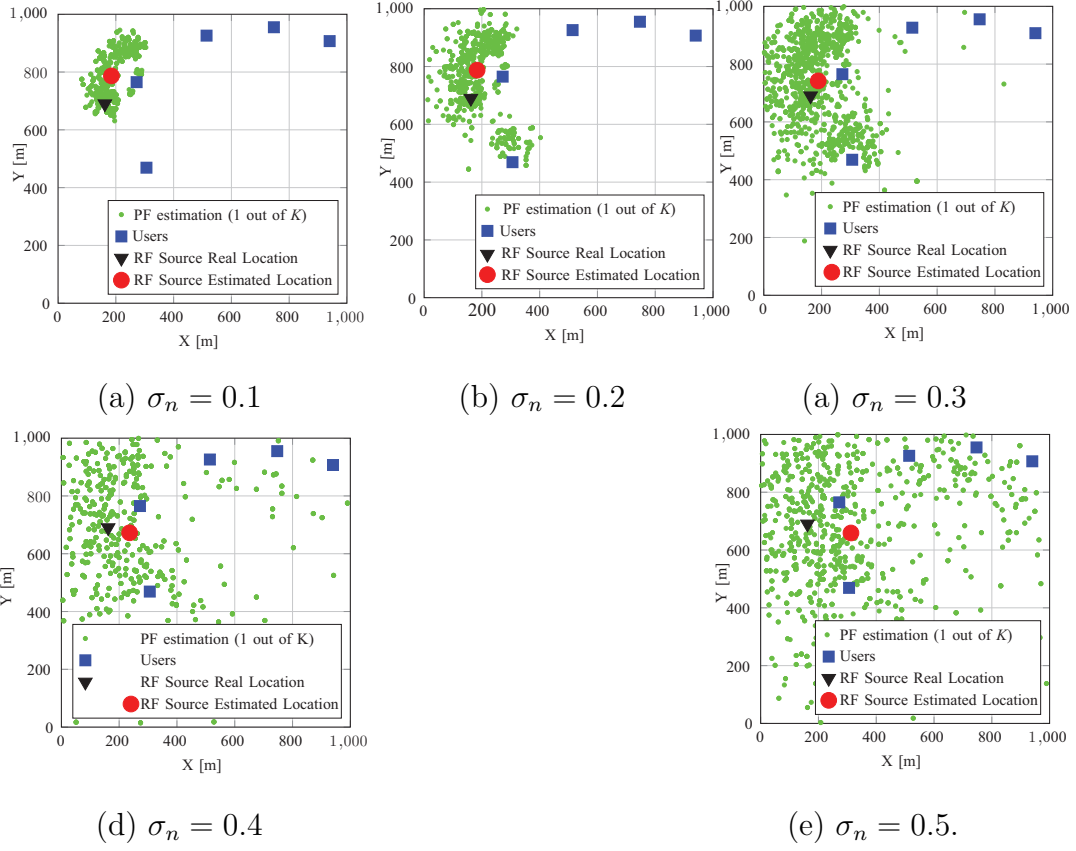
Figure 3.10: Experimental results considering different variances for the scenario: cellID: 60562, $N = 5$, $T = 60\ min$, Directional Antenna.

Chapter 4

Multiple Input Single Output (MISO) RF Sensing for Backscatter Signals: Architecture

4.1 Problem Formulation & Bistatic Scatter Radio Networks

In addition to RF-source localization, our goal is to extend the localization framework and the proposed methodology to other wireless scenarios and RF-devices (e.g. sensors or users' mobiles). RF tag-sensor localization in bistatic scatter radio networks for environmental sensing, is considered as a second localization case study, in this work. The above problem is an intriguing one, since accurate sensor localization is a key-enabling feature for the adoption of sensing applications in everyday life.

More specifically, a bistatic scatter radio network is deployed on the field that comprises of N low-cost carrier emitters, one RF tag (to be localized) and a software defined radio (SDR) reader. A time division multiple access (TDMA) scheme is assumed: the RF tag is illuminated by one emitter at a time and the tag's modulated signal is scattered towards the reader for demodulation and decoding, as illustrated in Fig. 4.1. It is noted that many different sensor tags could be served simultaneously, based on a frequency division multiple access (FDMA) scheme [37]. Furthermore, the serving area can be separated to cells, where each cell is served by a specific carrier emitter
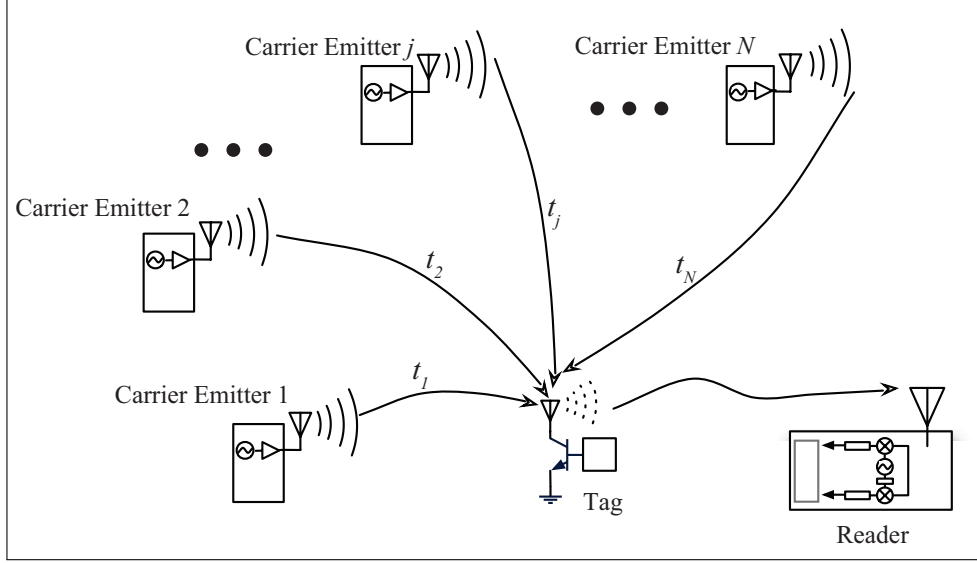
Figure 4.1: The bistatic scatter radio network consists of N low-cost carrier emitters, one RF tag to be localized and the reader (e.g. placed on a field). Only one emitter radiates the tag at a time, while the rest sleep.

in different frequency.

The known and immobile location of each installed emitter j is denoted as $\mathbf{x}_j \triangleq \begin{bmatrix} x_j & y_j \end{bmatrix}^T$ and the static location of the sensor tag is *be estimated* is denoted as $\mathbf{x}_\mathrm{T} = \begin{bmatrix} x_\mathrm{T} & y_\mathrm{T} \end{bmatrix}^T$. The network reader, i.e. a USRP, is placed on a fixed and predetermined location, $\mathbf{x}_\mathrm{R} \triangleq \begin{bmatrix} x_\mathrm{R} & y_\mathrm{R} \end{bmatrix}^T$. The collection of all emitters locations is represented by $\mathbf{x} \triangleq \begin{bmatrix} \mathbf{x}_1 & \cdots & \mathbf{x}_N \end{bmatrix}$.

4.2   Scatter Radio Network Modules

For the experimental setup of this work, the experimental testbed developed in [5] is utilized. A short description of the bistatic scatter radio modules follows, in order to describe the basic principles of the scatter radio communication which are necessary for the RF tag localization.

4.2.1 Scatter Radio Tag

A semi-passive, i.e. battery assisted, tag designed and soldered on a PCB (printed circuit board) as described in works [5] and [37] respectively, is used for the experimental setup in this work. The RF tag is depicted in Fig. 4.2 and 4.4. The authors of these works designed a low-cost and low-power environmental sensor which allows the integration of a variety of sensors (e.g. temperature, humidity or soil moisture). Thus, the RF tag consists of the MCU (a 8051 model), the RF front-end (i.e. the RF transistor modulator attached to the antenna's SMA) and a sensor interface (i.e. connector) which allows the connection of a variety of sensors and a LED. The custom printed on the PCB RF tag is powered by AAA batteries. Further details about the design of the RF tag can be found in [5] and [37].

For information modulation, the tag typically terminates its antenna between two loads; thus, the incident carrier's continuous wave is reflected with altered phase and/or amplitude, according to the load that is chosen each time. In practice, load switching is implemented by switching an RF transis-
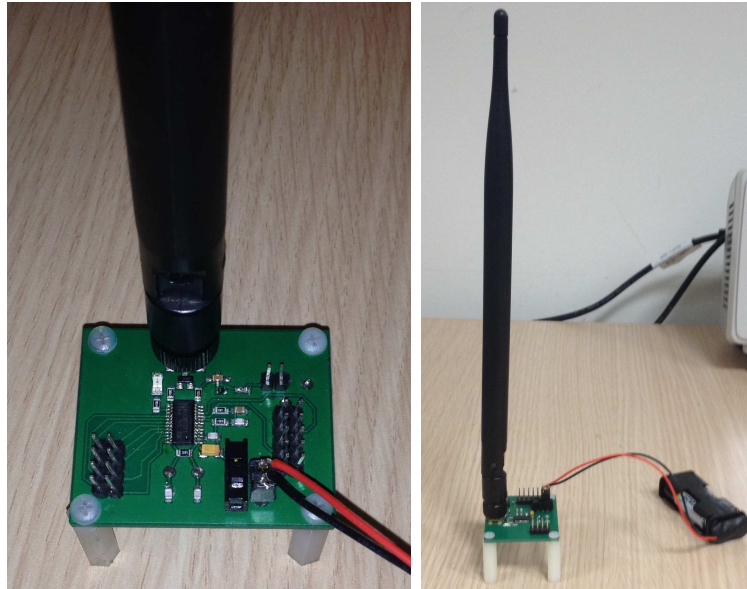
Figure 4.2: The PCB surface of the custom implemented RF tag in [5] is shown on the left. The RF tag connected with its antenna and powered by batteries is depicted on the right.

tor. Typically, RF transistor switching alternates the RF antenna between short and open circuited state and the incident wave is scattered back either with a negative phase or with no phase change, for bit 0 and bit 1, respectively. The RF transistor is controlled by a MCU pin that supplies the transistor with the appropriate bias voltage (0V or 3V) in order to switch it on or off. Further details can be found in work [5].

4.2.2 Carrier Emitter

To achieve carrier generation and transmission, an embedded radio monolithic chip controlled by a low-cost MCU has been used in the experimental setups. The evaluation board produced by Silicon Labs (model Si100x[1]) is shown in Fig. 4.3. The MCU (a 8051 model) allows setting several radio parameters such as the carrier frequency or output power, with the use of software. Typically, the carrier emitter is a minimal WSN node, transmitting a single tone continuous wave (a sinusoid) with frequency F_c. It operates in the European UHF ISM band ($865 - 868$ MHz) and has a tunable output power of up to +13dBm (≈ 20 mW).

It is important to note that the carrier emitter is capable of battery operation, therefore, multiple emitters on the field can be placed on the field. Moreover, the carrier emitter is of ultra low cost; two orders of magnitude cheaper than the reader. The aforementioned properties are key-enable parameters for real world applications and allow the use of multiple carrier emitters across a field to extend communication range and coverage. Most importantly, multiple low cost carrier emitters allow RF tag localization in a more efficient way compared to prior art, which mainly uses multiple readers, that are expensive and increase the implementation overhead.

4.2.3 Software Defined Radio (SDR) Reader

All reception and processing of the backscattered signals is performed on USRP 2[2], a commercial software defined radio (SDR) reader produced by

---

[1] www.silabs.com/products/wireless/wirelessmcu/pages/si1000.aspx
[2] www.ettus.com/product/details/UN210-KIT

Figure 4.3: Carrier emitter evaluation board (Silicon Labs Si100x).

Ettus Research. The reader captures backscatter signals through a UHF RF front-end (SBX daughtercard) and down-converts the received signals to baseband. Fast I/Q analog-to-digital converters (ADCs) provide the sampled baseband waveform to the host PC, where signal processing by software can be performed. The signal processing blocks for tag decoding are done in MATLAB software, running on a PC that hosts the SDR, with custom scripts. Thus, the modulation scheme can be completely controlled and any possible processing can be performed. For instance, measuring RSS is implemented complementary to the software defined receiver for tag-to-reader communication. The reader and the whole bistatic scatter radio testbed is depicted in Fig. 4.4.
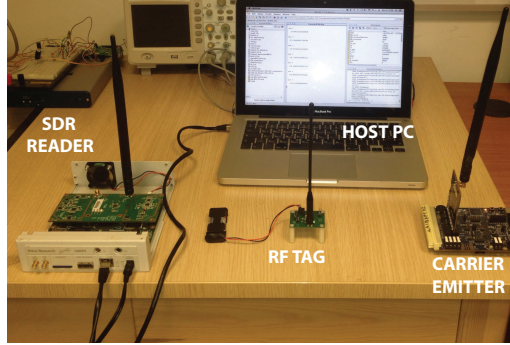
Figure 4.4: Bistatic scatter radio network testbed.

4.3 Modulation Scheme for Bistatic Scatter Radio Communication

Work presented in [6] derives and implements a digital modulation scheme based on FSK, to achieve communication between the tag and the reader. The bistatic scatter radio communication scheme includes a carrier emitter, an RF tag and a software-defined reader. The respective wireless links among the aforementioned elements are depicted in Fig. 4.5. The carrier emitter transmits a sinusoid in the UHF band, illuminating the tag. The latter modulates its information by reflecting the incident sinusoid wave with frequency $\{F_0, F_1\}$ and phase $\{\Phi_0, \Phi_1\}$ for bit $i \in \{0, 1\}$ respectively, as explained in section 4.2.1.

Each wireless channel in Fig. 4.5 is modelled as a Rayleigh flat fading channel. Thus, $h_{\mathrm{CR}}(t) = a_{\mathrm{CR}}e^{-j\phi_{\mathrm{CR}}}$, $h_{\mathrm{CT}}(t) = a_{\mathrm{CT}}e^{-j\phi_{\mathrm{CT}}}$, $h_{\mathrm{TR}}(t) = a_{\mathrm{TR}}e^{-j\phi_{\mathrm{TR}}}$ are the Rayleigh flat fading channels for the wireless links $\mathrm{C}_j \rightarrow \mathrm{R}$, $\mathrm{C}_j \rightarrow \mathrm{T}$ and $\mathrm{T} \rightarrow \mathrm{R}$ respectively. The symbol a denotes the channel attenuation and ϕ denotes the corresponding channel phase, due to signal propagation delay. The tag modulates on the incoming carrier sinusoid and the modulated waveform is subsequently reflected over the wireless link $\mathrm{T} \rightarrow \mathrm{R}$.

The SDR receives and demodulates the superposition of the carrier emitter sinusoid as well as the backscattered-reflected tag signal through channels $h_{\mathrm{CR}}(t)$ and $h_{\mathrm{TR}}(t)$ respectively. Thus, the complex baseband signal received

by the reader, for a time duration of a single bit $i \in \{0, 1\}$ can be written as:

$$y(t) = \left(\underbrace{\sqrt{2P_{\text{TX}}} \left(a_{CR} e^{-j(\phi_{CR} + \Delta\phi)} + s u_0 e^{-j\phi_{CTR}} \right)}_{\text{DC term}} \right.$$
$$\left. + m_{CTR} e^{-j\phi_{CTR}} \cos(2\pi F_i t + \Phi_i) \right) \times e^{-j2\pi\Delta F t} + n(t). \qquad (4.1)$$

To keep notation as simple as possible:

$$\phi_{CTR} = \phi_{CT} + \phi_{TR} + \Delta\phi$$
$$m_{CTR} = \sqrt{2P_{\text{TX}}} a_{CT} a_{TR} \frac{4}{\pi} s, \qquad (4.2)$$

where, P_{TX} denotes the carrier's transmission power in mW, $\Delta\phi$ is the phase offset between carrier emitter and SDR, s depends on the tag inherent scattering efficiency, u_0 is a constant that depends on the tag antenna and Φ_i is a random initial phase of each bit $i \in \{0, 1\}$.

It is emphasized that since modulation occurs directly at the passband, two subcarriers appear for bit i, one at positive frequencies and one at negative frequencies in the spectrum (illustrated in Fig. 4.6). Thus, the bistatic FSK scheme introduces 4 subcarriers, $\{F_0^-, F_0^+, F_1^-, F_1^+\}$, two per each bit $i \in \{0, 1\}$. This must be considered in the RSS measurements.

The reader, after carrier frequency estimation (CFO) and DC term elimination, decides the bit sequence with a non-coherent detector, as derived in [6]. Further details, such as the analytical signal model and the exact signal processing blocks are outside the scope of this work.
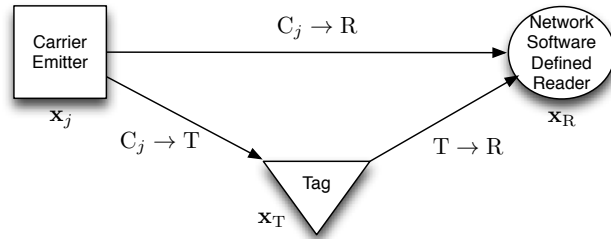
Figure 4.5: Wireless links of the bistatic scatter radio network setup. Thereinafter, these symbols are used for depicting the emitter, tag and reader.
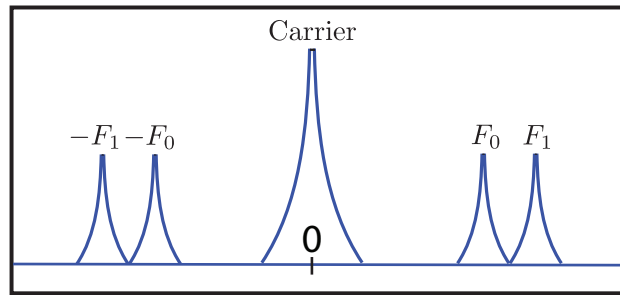
Figure 4.6: Received Signal Power Spectrum for the Binary FSK for the bistatic setup. The 4 subcarriers as a result of the modulation at F_c, are visible in the spectrum [6].

Chapter 5

MISO RF Sensing: Sensor Location Estimation

5.1 System Model

In this chapter, the unknown RF tag location $\mathbf{x}_\mathrm{T} = \begin{bmatrix} x_\mathrm{T} & y_\mathrm{T} \end{bmatrix}^T$ will be estimated, utilizing the tag's RSS by N different emitters at locations $\mathbf{x} \triangleq \begin{bmatrix} \mathbf{x}_1 & \cdots & \mathbf{x}_N \end{bmatrix}$, as described in 4.1. A careful system approach is necessary, in order to take into account real world system parameters and specific features of the bistatic architecture which may affect localization.

5.1.1 Received Signal Strength (RSS)

The reader records S distinct RSS values (in mW) of the RF tag being illuminated by a specific emitter j at time instances $t_1^j, t_2^j, \ldots, t_S^j$ and this is repeated for each emitter j[1]. Time frame $t_k = \begin{bmatrix} t_k^1 & \cdots & t_k^N \end{bmatrix}$ denotes time moments for a set of N tag's measurements, each one generated by a different emitter. Each RSS measurement contains the 4 different tag's subcarriers power (see section 4.3), since subcarriers' power may differ, especially if they are close to the carrier clutter. Consequently, at time instance t_k^j, the reader records: $P_{[\mathrm{T}_j]}^{(t_k^j)} \triangleq \begin{bmatrix} P_{F_0^-}^{(t_k^j)} & P_{F_1^-}^{(t_k^j)} & P_{F_0^+}^{(t_k^j)} & P_{F_1^+}^{(t_k^j)} \end{bmatrix}$. The set of measurements recorded by a specific emitter j is denoted as $\mathbf{z}^{[\mathrm{T}_j]} \triangleq \begin{bmatrix} P_{[\mathrm{T}_j]}^{(t_1^j)} & \cdots & P_{[\mathrm{T}_j]}^{(t_S^j)} \end{bmatrix}^T$. The collection of all tag measurements from the N emitters, is written as: $\mathbf{z}^{[\mathrm{T}]} \triangleq \begin{bmatrix} \mathbf{z}^{[\mathrm{T}_1]} & \cdots & \mathbf{z}^{[\mathrm{T}_N]} \end{bmatrix}$.

---

[1]The subscript j implies that the tag is served by the emitter j and all the other emitters are disabled.
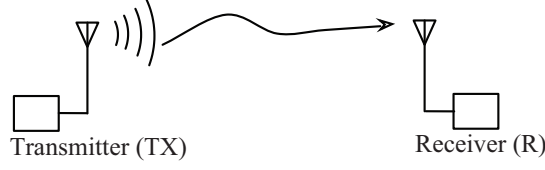
Figure 5.1: A typical point-to-point wireless link. Free space propagation and isotropic transmission are assumed.

Simultaneously, the reader records the RSS of the carrier-to-reader link $(C_j \to R)$, $\mathbf{z}^{[C_j]} \triangleq \left[P_{C_j}^{(t_1^j)} \cdots P_{C_j}^{(t_S^j)} \right]^T$, with the vector $\mathbf{z}^{[C]} \triangleq \left[\mathbf{z}^{[C_1]} \cdots \mathbf{z}^{[C_N]} \right]$ used for the collection of all measurements. Finally, the reader's script calculates the carrier-to-subcarrier (CSR) ratio in dB, $\mathrm{CSR}_{dB}^{(t_k^j)} = 10 \log_{10} \left(\dfrac{P_{[C_j]}^{(t_k^j)}}{P_{F_1^+}^{(t_k^j)}} \right)$.
The corresponding vector is written as $\mathbf{z}_j^{[\mathrm{CSR}_{dB}]} \triangleq \left[\mathrm{CSR}_{dB}^{(t_1^j)} \cdots \mathrm{CSR}_{dB}^{(t_S^j)} \right]$ and the collection of all measurements as is written as $\mathbf{z}^{[\mathrm{CSR}_{dB}]} \triangleq \left[\mathbf{z}_1^{[\mathrm{CSR}_{dB}]} \cdots \mathbf{z}_N^{[\mathrm{CSR}_{dB}]} \right]$.

Moreover, the reader stores relevant information, such as the level of the noise floor $\mathbf{z}^{[NF_j]} \triangleq \left[P_{[NF_j]}^{(t_1^j)} \cdots P_{[NF_j]}^{(t_S^j)} \right]^T$, for each emitter j. The exact procedure followed by the reader, for the RSS calculation is described in section 5.1.2. At this point, an exact formula for the RSS of the tag should be provided. Firstly, a point-to-point link will be studied, in order to demonstrate some basic wireless propagation aspects, that will be used in localization.

Point-to-point wireless link: In Fig. 5.1 a typical point-to-point wireless system is depicted. The antenna transmits isotropically a continuous wave signal of power P_{TX} (in mW) with transmission gain G_{TX}. According to Friis transmission equation, the received power (in mW) at the receiver is:

$$
\begin{aligned}
P_R &= \frac{P_{TX} G_{TX}}{4\pi d^2} A_{eff}^R = \frac{P_{TX} G_{TX}}{4\pi d^2} G_R \frac{\lambda}{4\pi} \\
&= P_{TX} G_{TX} G_R \left(\frac{\lambda}{4\pi d} \right)^2 = P_{TX} G_{TX} G_R K \frac{1}{d^2},
\end{aligned} \tag{5.1}
$$

where $A_{eff}^{\text{R}} = \frac{G_{\text{R}}\lambda}{4\pi}$ is the antenna aperture[2], λ is the wavelength of the radio waves, d is the distance in meters between the transmitting and the receiving antenna and G_{R} is the gain of the receiver. For the final form of the equation, $K = \left(\frac{\lambda}{4\pi}\right)^2$ depends on overall antenna efficiency and is necessary to scale $P_{\text{TX}}G_{\text{TX}}\frac{1}{d^2}$ appropriately in order to offer received values in power.

Tag-to-Reader wireless link: In contradiction, the tag-to-reader link (to measure its RSS) is created by the signal's reflection (see Fig. 4.1) and therefore eq. 5.1 does not apply directly, implying that a more careful analysis is needed. Each emitter j transmits a continuous wave of frequency F_c with constant power P_{TX}. It can be seen in Fig. 4.5 that signal propagation is divided into two wireless links. Carrier C_j illuminates tag T ($C_j \rightarrow$ T) and the signal is scattered to the reader (T $\rightarrow$ R). Thus, the RSS (in mW) of the tag is given by:

$$P_{[\text{T}_j]}^{(t_k^j)} = P_{\text{TX}}G_{\text{TX}}G_{\text{T}} \ \eta_{\text{T}} \frac{1}{||\mathbf{x}_j - \mathbf{x}_{\text{T}}||_2^{n_j}} \ KG_{\text{R}} \frac{1}{||\mathbf{x}_{\text{T}} - \mathbf{x}_{\text{R}}||_2^{n_{\text{T}}}} \ , \qquad (5.2)$$

where G_{TX} is the transmission gain (same for each emitter j), G_{T} denotes the gain of the tag antenna, η_{T} is the tag scattering efficiency and n_j is the PLE for the wireless link $C_j \rightarrow$ T. For the link T $\rightarrow$ R, K depends on the overall antenna efficiency of the reader as explained previously in eq. 5.1, G_{R} denotes the reception gain at the USRP and n_{T} is the PLE for the tag-to-reader link (T $\rightarrow$ R). Similarly, the RSS (in mW) of the carrier-to-reader direct link ($C_j \rightarrow$ R) is given by:

$$P_{[\text{C}_j]}^{(t_k^j)} = P_{\text{TX}}G_{\text{TX}}KG_{\text{R}} \frac{1}{||\mathbf{x}_j - \mathbf{x}_{\text{R}}||_2^{n_{\text{C}_j}}} \ , \qquad (5.3)$$

where n_{C_j} is the PLE for the wireless link ($C_j \rightarrow$ R). However, in real environments, the RSS values are not exactly equal to Eq. 5.2 and Eq. 5.3 due to shadow fading, the time variant noise floor (i.e. time variant environmental conditions), imperfect electronics etc. The RSS is modelled (see section 3.1.1) as a random variable that follows the log-normal distri-

---

[2]A_{eff}^{R} is a measure of how effective an antenna is at receiving the power of radio waves.

bution [27], i.e. Gaussian distributed in dBm. Eq. 5.2 and Eq. 5.3 yield the mean value in mW, therefore the mean values are easily expressed in dBm: $\overline{P_{[\mathrm{T}_j]}^{(t_k^j)}}(\mathrm{dBm}) = 10\log_{10}\left(P_{[\mathrm{T}_j]}^{(t_k^j)}\right)$ and $\overline{P_{[\mathrm{C}_j]}^{(t_k^j)}}(\mathrm{dBm}) = 10\log_{10}\left(P_{[\mathrm{C}_j]}^{(t_k^j)}\right)$ for the tag and the carrier respectively. Thus, the random variables are:

$$P_{[\mathrm{T}_j]}^{(t_k^j)}(\mathrm{dBm}) = \overline{P_{[\mathrm{T}_j]}^{(t_k^j)}}(\mathrm{dBm}) + w_{\mathrm{T}_j}^{(t_k^j)}, \tag{5.4}$$

$$P_{[\mathrm{C}_j]}^{(t_k^j)}(\mathrm{dBm}) = \overline{P_{[\mathrm{C}_j]}^{(t_k^j)}}(\mathrm{dBm}) + w_{\mathrm{C}_j}^{(t_k^j)}, \tag{5.5}$$

for the tag-to-reader and the carrier-to-reader RSS respectively. Measurements' noise is modelled as a zero-mean Gaussian with variances $\sigma_{\mathrm{T}_j}^2$ and $\sigma_{\mathrm{C}_j}^2$ (expressed in dB) respectively; noise r.v's are assumed independent between the measurements by different emitters. Typically, $w_{\mathrm{T}_j}^{(t_k^j)}$ is already the sum of two normal in dB random variables; i.e. one normal variable for the noise of link $\mathrm{C}_j \to \mathrm{T}$ and one for link $\mathrm{T} \to \mathrm{R}$. Thus, $w_{\mathrm{T}_j}^{(t_k^j)}$ is also normal in dB.

5.1.2 RSS Estimation via Power Spectrum Density on USRPs

The USRP includes an analog RSSI sensor, which measures the RSS of the wideband channel. Nevertheless, this sensor is not appropriate for our case since our goal is to measure distinctively the subcarriers' power and the carrier's power of the received demodulated signal $y(t)$ (Eq. 4.1). However, the power (per frequency region) of a signal of interest $y(t)$ can be calculated via power spectral density (PSD) as explained in [38]. Thus, the total signal's power is given by:

$$P_y \triangleq \int_{-\infty}^{+\infty} S_Y(F)\mathrm{d}F, \tag{5.6}$$

where $S_Y(F)$ is the power spectral density of the received signal $y(t)$.

An estimation $\widehat{S}_Y(F)$ of $S_Y(F)$ can be calculated by the average of L periodograms. Each periodogram is a rough approximation of the power

spectral density and is defined by:

$$\frac{\mathbb{E}[|Y(F)|^2]}{T_{\text{rx}}}, \text{with } Y(F) = \mathscr{F}\{y(t)\},$$

where T_{rx} is the time duration of the signal of interest, $y(t)$. Each periodogram suffers from high noise variance and therefore a good approximation, $\widehat{S}_Y(F)$, of the PSD is given by the average of L different periodograms:

$$\widehat{S}_Y(F) \triangleq \frac{1}{L} \sum_{l=1}^{L} \frac{|Y_l(F)|^2}{T_{\text{rx}}}, \quad \left(\frac{\text{Watt}}{\text{Hz}}\right). \tag{5.7}$$

We assume that the RF tag transmits packets towards the reader continuously and T_{rx} is the signal duration of the captured signal $y(t)$ utilized for the periodogram estimation. The power for each specific subcarrier, as well as for the carrier is calculated at time instance t_k^j, when the tag is illuminated by the emitter j is given by:

$$P_{F_0^-}^{(t_k^j)} \triangleq \int_{F_0^- - \frac{w}{2}}^{F_0^- + \frac{w}{2}} \widehat{S}_Y(F)\mathrm{d}F, \tag{5.8}$$

$$P_{F_1^-}^{(t_k^j)} \triangleq \int_{F_1^- - \frac{w}{2}}^{F_1^- + \frac{w}{2}} \widehat{S}_Y(F)\mathrm{d}F, \tag{5.9}$$

$$P_{F_0^+}^{(t_k^j)} \triangleq \int_{F_0^+ - \frac{w}{2}}^{F_0^+ + \frac{w}{2}} \widehat{S}_Y(F)\mathrm{d}F, \tag{5.10}$$

$$P_{F_1^+}^{(t_k^j)} \triangleq \int_{F_1^+ - \frac{w}{2}}^{F_1^+ + \frac{w}{2}} \widehat{S}_Y(F)\mathrm{d}F, \tag{5.11}$$

$$P_{[\mathrm{C}_j]}^{(t_k^j)} \triangleq \int_{-\frac{w}{2}}^{\frac{w}{2}} \widehat{S}_Y(F)\mathrm{d}F, \tag{5.12}$$

where, w, w_{C} denotes the bandwidth of the subcarriers and the carrier respectively, $\widehat{S}_Y(F)$ is calculated by eq. 5.7 at time moment t_k^j, for L periodograms of $y(t)$, and consequently the time interval between t_k^j and t_{k+1}^j is $L \cdot T_{\text{rx}}$ seconds.

5.1.3 Carrier-to-Subcarrier (CSR) Ratio

The CSR ratio was chosen to be an *observation* variable for localization, since the subcarriers' level $P_{[\mathrm{T}_j]}^{(t_k^j)} \triangleq \left[P_{F_0^-}^{(t_k^j)} \ P_{F_1^-}^{(t_k^j)} \ P_{F_0^+}^{(t_k^j)} \ P_{F_1^+}^{(t_k^j)} \right]$, may be affected by many real world parameters. For instance, $P_{[\mathrm{T}_j]}^{(t_k^j)}$ values were affected by the noise floor level (time variant depending on environmental conditions), the interferences by neighbouring frequency bands, such as the GSM 900 MHz or unexpected behaviour changes of the electronics. For example, sometimes, in high humidity levels the ADC output was significantly attenuated. Most importantly, subcarriers' level may be affected by the carrier clutter. However, CSR ratio is a much more accurate observation, since the influence of the unexpected parameters affect both carrier and subcarrier and therefore the ratio reveals distance information. Subcarrier $P_{F_1^+}^{(t_k^j)}$ was selected, since is was affected the less by the carrier's clutter. The mean value of the CSR is given by:

$$\overline{\mathrm{CSR}_{\mathrm{dB}}^{(t_k^j)}} = 10\log_{10}\left(\frac{P_{[\mathrm{C}_j]}^{(t_k^j)}}{P_{F_1^+}^{(t_k^j)}} \right) \overset{5.2,\ 5.3}{\Longleftrightarrow}$$

$$\overline{\mathrm{CSR}_{\mathrm{dB}}^{(t_k^j)}} = 10\log_{10}\left(\frac{||\mathbf{x}_j - \mathbf{x}_\mathrm{R}||_2^{-n_{\mathrm{C}_j}}}{||\mathbf{x}_j - \mathbf{x}_\mathrm{T}||_2^{-n_j} ||\mathbf{x}_\mathrm{T} - \mathbf{x}_\mathrm{R}||_2^{-n_\mathrm{T}} G_\mathrm{T}\eta_\mathrm{T} \cdot \frac{1}{2}} \right) \Longleftrightarrow$$

$$\overline{\mathrm{CSR}_{\mathrm{dB}}^{(t_k^j)}} = -10 n_{\mathrm{C}_j} \log_{10}\left(||\mathbf{x}_j - \mathbf{x}_\mathrm{R}||_2 \right) + 10 n_j \log_{10}\left(|\mathbf{x}_j - \mathbf{x}_\mathrm{T}||_2 \right)$$
$$+ 10 n_\mathrm{T} \log_{10}\left(||\mathbf{x}_\mathrm{T} - \mathbf{x}_\mathrm{R}||_2 \right) - 10 \log_{10}\left(G_\mathrm{T}\eta_\mathrm{T} \cdot \frac{1}{2} \right) \Longleftrightarrow$$

$$\overline{\mathrm{CSR}_{\mathrm{dB}}^{(t_k^j)}} = -10 n_{\mathrm{C}_j} \log_{10}\left(||\mathbf{x}_j - \mathbf{x}_\mathrm{R}||_2 \right) + 10 n_j \log_{10}\left(|\mathbf{x}_j - \mathbf{x}_\mathrm{T}||_2 \right)$$
$$+ 10 n_\mathrm{T} \log_{10}\left(||\mathbf{x}_\mathrm{T} - \mathbf{x}_\mathrm{R}||_2 \right) - s, \tag{5.13}$$

where s is a scaling term expressed in dB, related to the tag scattering efficiency η_T and the tag gain G_T, and will be estimated.

Considering the random variables in Eq. 5.4 and Eq. 5.5, the CSR defi-

nition yields:

$$P_j^{(t_k^j)} = \text{CSR}_{\text{dB}}^{(t_k^j)} = \left(P_{[\text{C}_j]}^{(t_k^j)}(\text{dBm}) - P_{F_1^+}^{(t_k^j)}(\text{dBm}) \right), \tag{5.14}$$

where, $P_j^{(t_k^j)}$ is the difference of two normal (in dBm) random variables and therefore, $P_j^{(t_k^j)}$ is distributed in a normal manner in dB with mean value given by eq. 5.13 and variance $\sigma_j = \sqrt{\sigma_{\text{T}_j}^2 + \sigma_{\text{C}_j}^2}$. Symbol $P_j^{(t_k^j)}$ is used for simplified notation:

$$P_j^{(t_k^j)} = \overline{P_{[\text{C}_j]}^{(t_k^j)}}(\text{dBm}) - \overline{P_{F_1^+}^{(t_k^j)}}(\text{dBm}) + w_j^{(t_k^j)} \tag{5.15}$$

5.2 Estimation Algorithm

An initial estimation of all PLEs is needed in order to proceed with the estimation algorithm. The PLEs of the links $\text{C}_j \rightarrow \text{T}$ can be estimated, since the locations of the emitters, $\mathbf{x}$, and the reader, $\mathbf{x}_\text{R}$, are known. For the link $\text{C}_j \rightarrow \text{T}$ the mean RSS in dBm is given by:

$$\overline{P_{[\text{C}_j]}^{(t_k^j)}}(\text{dBm}) = P_0 - 10 n_{\text{C}_j} \log_{10} \left(\frac{\|\mathbf{x}_j - \mathbf{x}_\text{R}\|_2}{d_0} \right), \tag{5.16}$$

where P_0 is measured experimentally at $d_0 = 1\text{m}$. Consequently, the estimation of all PLEs for links $\text{C}_j \rightarrow \text{R}$ is given by:

$$\widehat{n}_{\text{C}_j} = \frac{P_0 - (1/\kappa) \sum_{i=1}^{\kappa} P_{[\text{C}_j]}^{(t_i^j)}(\text{dBm})}{10 \log_{10} \|\mathbf{x}_j - \mathbf{x}_\text{R}\|_2}, \forall \, j, \tag{5.17}$$

Moreover, we assume that, $n_j = n_{\text{C}_j}$, therefore:

$$\widehat{n}_j = \widehat{n}_{\text{C}_j}. \tag{5.18}$$

This assumption comes from the fact that links $\text{C}_j \rightarrow \text{T}$ have similar characteristics with the links $\text{C}_j \rightarrow \text{R}$, i.e. similar wireless propagation attenuation at the emitters' locations. Besides, the estimation algorithm will improve the

imperfect initial estimation of $\widehat{n}_j$. Furthermore, s, which is the term related to tag scattering efficiency, is unknown and should be estimated. Finally, we assume that n_{T} is the average value of the links n_{C_j}:

$$\widehat{n}_{\mathrm{T}} = \frac{1}{N} \sum_{i=1}^{N} \widehat{n}_{\mathrm{C}_j} \tag{5.19}$$

The goal is to estimate vector $\boldsymbol{\theta}^{(t)}$, which includes all the unknown parameters, including the unknown tag coordinates $\mathbf{x}_{\mathrm{T}}$ from *real-world measurements* $\mathbf{z}^{[\mathrm{CSR_{dB}}]}$:

$$\boldsymbol{\theta}^{(t)} \triangleq \begin{bmatrix} x_{\mathrm{T}} & y_{\mathrm{T}} & n_1 \cdots n_N & n_{\mathrm{T}} & s \end{bmatrix}^{T}. \tag{5.20}$$

More specifically, probability density $p(\boldsymbol{\theta}|\mathbf{z}^{[\mathrm{CSR_{dB}}]})$ is modeled and estimated with non-parametric procedures based on particle filtering [33], as we described earlier in section 3.2 of this manuscript. Specifically, M particles at time t are considered, with corresponding weights $\{w_t^{[m]}\}$:

$$\left\{ \boldsymbol{\theta}_t^{[m]} = \begin{bmatrix} x_{\mathrm{T}}^{[m]} & y_{\mathrm{T}}^{[m]} n_1^{[m]} \cdots n_N^{[m]} & n_T^{[m]} & s^{[m]} \end{bmatrix}^{T} \right\}.$$

The whole topology, i.e. both the N carrier emitters and the tag, is static. Also, the PLEs are considered constant, for the time window of the utilized experiments. Thus, there is no update operation of particle filtering.

The *correction* phase of each particle weight at time t, when a time frame t_k has finished (i.e. measurements by N different emitters), is given by:

$$w_t^{[m]} = p\left(\mathbf{z}^{(t)}|\boldsymbol{\theta}_t^{[m]}\right) \tag{5.21}$$

$$= p\left(P_1^{(t_k^1)}|\boldsymbol{\theta}_t^{[m]}\right) \cdots p\left(P_j^{(t_k^j)}|\boldsymbol{\theta}_t^{[m]}\right) \cdots p\left(P_N^{(t_k^N)}|\boldsymbol{\theta}_t^{[m]}\right), \tag{5.22}$$

where independence of CSR measurements by different carrier emitters has been exploited. The conditional p.d.f. value of each measurement is based

on the log-normal p.d.f. (Eq. (5.15)):

$$p\left(P_j^{(t_k^j)}|\boldsymbol{\theta}_t^{[m]}\right) = \frac{1}{\sigma_j\sqrt{2\pi}}\exp\left(-\left(P_j^{(t_k^j)} - \overline{P_{j,[m]}^{(t_k^j)}}\right)^2/2\sigma_j^2\right). \tag{5.23}$$

Parameter $\overline{P_{j,[m]}^{(t_k^j)}}=\mathbb{E}\left[P_j^{(t_k^j)}|\boldsymbol{\theta}_t^{[m]}\right]$ is the expected value of the CSR, given $\boldsymbol{\theta}_t^{[m]}$:

$$\overline{P_{j,[m]}^{(t_k^j)}} = \text{CSR}_{\text{dB}}^{(t_k^j)}[m] = -10n_j^{[m]}\log_{10}\left(\|\mathbf{x}_j - \mathbf{x}_{\text{R}}\|_2\right) + 10n_j^{[m]}\log_{10}\left(\|\mathbf{x}_j - \mathbf{x}_{\text{T}}^{[m]}\|_2\right)$$
$$+ 10n_{\text{T}}^{[m]}\log_{10}\left(\|\mathbf{x}_{\text{T}}^{[m]} - \mathbf{x}_{\text{R}}\|_2\right) - s^{[m]} \tag{5.24}$$

Finally, the low-variance sampling procedure of the particles was utilized [33]. The pseudo-code of the PF algorithm follows.

PF Algorithm: Particle Filtering for estimating $p(\boldsymbol{\theta}|\mathbf{z}^s)$

---

(1): **Initialization of Variables:**

(2): Set M (number of Particles),

(3): X, Y (dimensions of area of interest), T (time window).

(4): $s_{\min}, s_{\max}$ (min and max possible tag scattering efficiency)

(5): **Initialization of Particles,** $\forall\, m = 1 : M$

(6): $\quad x_{t=0}^{[m]} \sim \mathcal{U}[0, X],\ y_{t=0}^{[m]} \sim \mathcal{U}[0, Y].$

(7): $\quad n_{j,t=0}^{[m]} \sim \mathcal{N}\left(\widehat{n}_j, \sigma_n^2\right),\ \forall j$ from (5.18).

(8): $\quad n_{\text{T},t=0}^{[m]} \sim \mathcal{N}\left(\widehat{n}_\text{T}, \sigma_n^2\right)$ from (5.19).

(9): $\quad \boldsymbol{\theta}_{t=0}^{[m]} = \begin{bmatrix} x_\text{T}^{[m]} & y_\text{T}^{[m]} n_1^{[m]} \cdots n_N^{[m]} & n_T^{[m]} & s^{[m]} \end{bmatrix}^T.$

(10): $\quad s_{t=0}^{[m]} \sim \mathcal{U}[s_{\min}, s_{\max}].$

(11): $\mathbf{z}^d \leftarrow$ **Select** T consecutive CSR measurements from $\mathbf{z}^{[\text{CSR}_{\text{dB}}]}$

(12): **for** $t = 1 : T$ **do** {*time-step*}

(13): $\quad$ **for** $m = 1 : M$ **do** {*particle index*}

(14): $\quad\quad w_t^{[m]} = p\left(\mathbf{z}^{(t)}|\boldsymbol{\theta}_t^{[m]}\right)$, from (5.22).

(15): $\quad$ **end for**

(16) $\quad$ Normalize weights $\boldsymbol{w}_t^{[1:M]}$.

(17) $\quad \boldsymbol{\theta}_t^{[1:M]} \leftarrow$ Low-VarianceSampler $\left(\boldsymbol{\theta}_t^{[1:M]}, \boldsymbol{w}_t^{[1:M]}\right).$

(18): **end for**

At the end of particle filtering algorithm the final particles $\boldsymbol{\theta}_T^{[1:M]}$ produce an estimate of the conditional density function $p(\boldsymbol{\theta}|\mathbf{z}^s)$ using the histogram approach [33]. With marginalization, an estimate of the conditional density function $p(\mathbf{x}_T|\mathbf{z}^d)$ is immediately available. The estimate of base station location $\widehat{\mathbf{x}}_T$ is offered by the conditional mean:

$$\widehat{\mathbf{x}}_T = [\widehat{x}_T \ \ \widehat{y}_T]^T = \mathbb{E}[\mathbf{x}_T|\mathbf{z}^d]. \tag{5.25}$$

The procedure could be repeated for K different $\mathbf{z}^s$ and the average value of all estimates produces the final outcome:

$$\widehat{\mathbf{x}}_T^{mean} = \sum_{k=1}^{K} \frac{1}{K}[\widehat{x}_T^k \ \ \widehat{y}_T^k]^T. \tag{5.26}$$

5.3 Results

Numerical results are reported for both simulated and real world data. The measurements collection from the bistatic scatter network was performed at the roof garden of the ECE school of Technical University of Crete.

The simulations consider two distinct locations for the tag deployment, as depicted in Fig. 5.2. Our goal is to investigate the effect of the number of utilized emitters to the localization accuracy. Thus, we assume a fixed noise standard deviation, $\sigma_{T_j} = \sigma_{C_j} = 2.8$ dB for the two log-normal random variables in the Eq. 5.15 which yields $\sigma_j = 4$ dB. Standard deviation of 3 dB is a typical value for wireless systems, as discussed in [27].

Results by simulated data are reported for $M = 30.000$, $X = Y = 70$ m, $T = 10$ time samples, $N = [3 \cdots 10]$ emitters and $K = 200$ independent experiments. For line (7) of the algorithm, $\sigma_n = 0.3$ and the PLEs are pre-estimated by the simulated data and equations 5.16 and 5.17, where the transmission power is $P_{TX} = 13$ dBm. Furthermore, $s_{\min} = -15$ dB and $s_{\max} = -25$ dB.

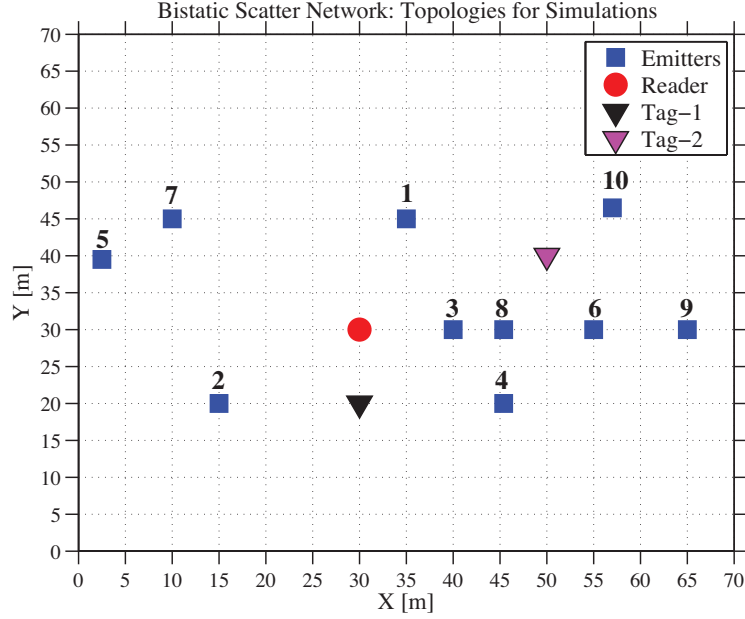The Root mean square error (RMSE) is compared with the different num-

Figure 5.2: Topology utilized in simulations. Emitters' index shows the ordering for the utilization at the simulations.

ber of utilized emitters in Fig. 5.3. The emitters' indexes are illustrated in Fig. 5.2; for $N = i$, in the reported results, it is implied that the emitters $j = \{1 \cdots i\}$ have been used. The emitters' indexes were randomly selected.

Localization error for the Tag-1 converges after the 4-th emitter which is reasonable, since emitters $j = \{1, 2, 3, 4\}$ are very close to the tag and most importantly, emitters $j = \{2, 4\}$ are placed anti-symmetric to the tag, i.e. the likelihood is maximized at the middle of their distance where the tag is. However, localization accuracy of Tag-2 does not converge immediately, but is improved with a larger number of emitters. Thus, the topology may affect the localization accuracy. Nevertheless, the big picture is that there is a clear trend, where localization error is improved while N increases.

Results from real world collected measurements are also reported by a deployment of bistatic scatter network with $N = 7$ emitters at the ECE roof garden. The setup for the bistatic scatter network for the measurement campaign is depicted in Fig. 5.4. For each emitter j, approximately $S = 3000$ measurements were recorded by placing the same emitter at the
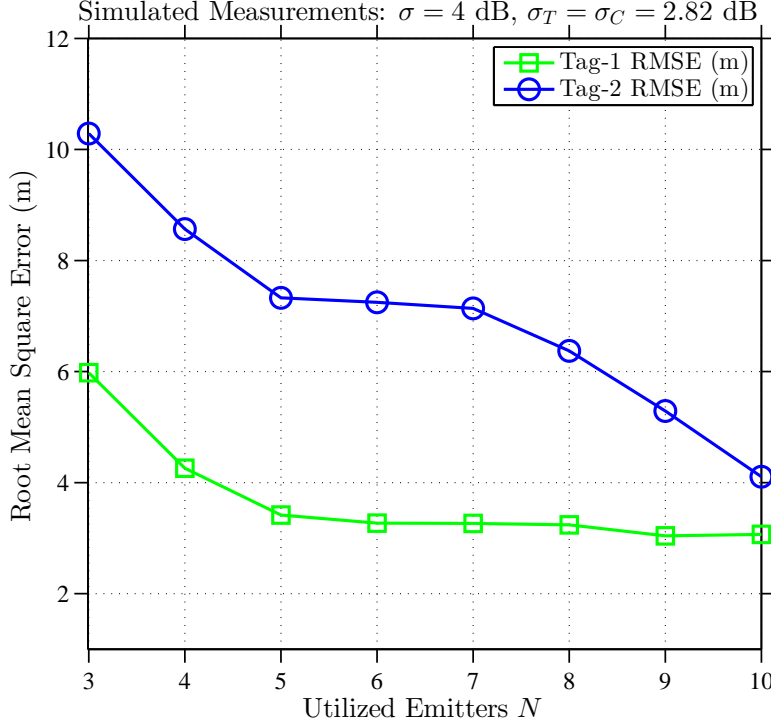
Figure 5.3: The RMSE is compared to the number of utilized emitters for $K = 200$ realizations and $\sigma_{\mathrm{T}_j} = \sigma_{\mathrm{C}_j} = 2.82$ dB (i.e.$\sigma = 4$ dB from Eq. 5.13). The system topology and the index of utilized indexes are depicted in Fig. 5.2.

corresponding location $\mathbf{x}_j$, as demonstrated in Fig. 5.5. One measurement includes tag's RSS $\mathbf{z}^{[\mathrm{T}_j]}$, carrier's RSS $\mathbf{z}^{[\mathrm{C}_j]}$ and consequently $\mathbf{z}_j^{[\mathrm{CSR}_{\mathrm{dB}}]}$), using the equations 5.7 - 5.12 in the reader, with $L = 12$ periodograms, $T_{\mathrm{rx}} = 30$ ms and $w = w_{\mathrm{C}} = 1$ kHz. It should be noted that actually the time interval between two consecutive RSS measurements is 1 second due to the delays of the USRP and MATLAB. The measurement campaign was performed during a specific day in order to have an identical setup for all measurements. Yet, many measurements were collected on different days for system debug and platform disambiguation.

Eq. 4.1 yields that the tag's signal (see term u_0) contributes power to the DC term. Experimentally, the carrier's power was measured when the tag was closed, at each different emitter location $\mathbf{x}_j$, in order to compare it with the carrier's power (i.e. P_{C_j}) while the tag is open. This was found
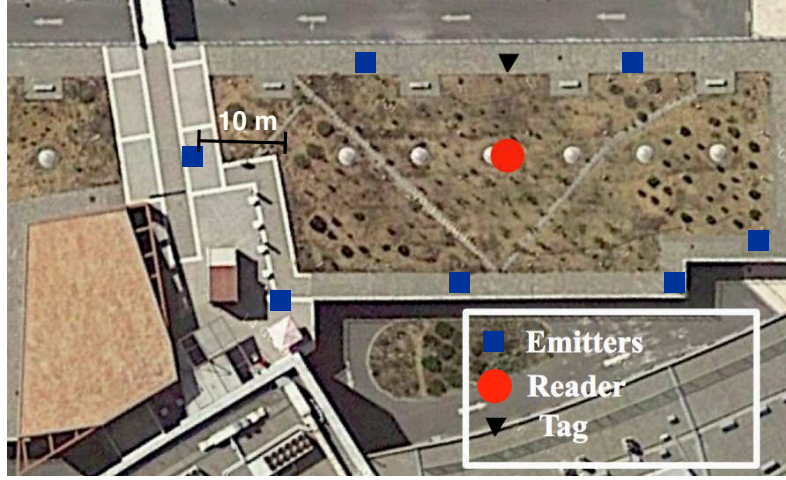
Figure 5.4: Topology of the bistatic scatter radio network setup with multiple emitters for tag localization, deployed at ECE roof garden, TUC, Chania.

approximately $1 - 3\%$, therefore, this effect is ignored.

For experimental validation of the proposed algorithm, measurements were collected from location $\mathbf{x}_T$ as demonstrated in Fig. 5.4. For each specific scenario (fixed subset), numerical results for $M = 100.000$, $X = Y = 70$ m, $K = 100$ independent experiments (i.e. PFs independent runs), $s_{\min} = -20$ dB, $s_{\max} = -30$ dB and $T = 10$ samples are reported. PLEs are pre-estimated by Eq. 5.16 and Eq. 5.17 and in line (7) of the algorithm is used the value $\sigma_n = 0.3$.

Considering the fact that many emitters will result in better estimation, topologies with $N = 6$ and $N = 7$ emitters were tested, as depicted in Fig. 5.6. When all the 7 emitters are considered, the estimation is improved in contrast with the estimation with $N = 6$ emitters where a bias is observed. Most importantly, the K independent estimations by the different runs of PFs forms a parabola, where the majority of the estimations are near the tag. Notably, the 1-mean estimator given by Eq. 5.27 fails to estimate accurately the location of the tag, however, it is clear that there are many outliers and the majority of the estimations are close to the tag.

Thus, an outlier algorithm available from the literature [7] is applied to these estimations. Each estimated position is assigned a score proportional
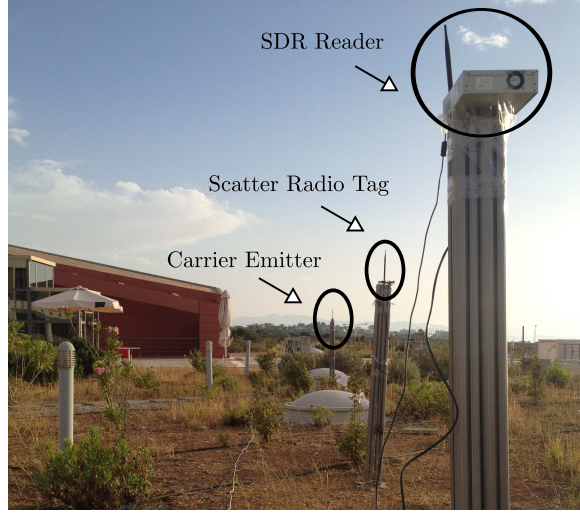
Figure 5.5: Bistatic radio network setup at ECE roof garden, TUC, Chania. Measurements are collected from the N different emitter's locations $\mathbf{x}_j$.
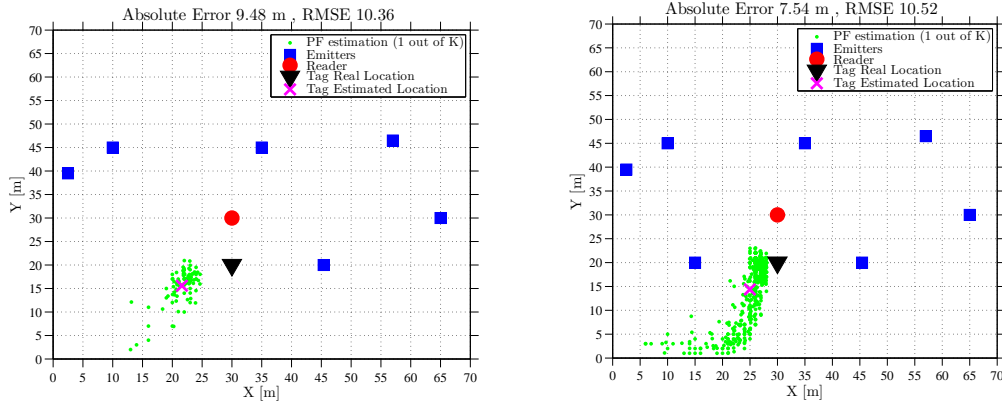
Figure 5.6: Left: Sensor location estimation for real world deployment at ECE roof garden with 6 emitters. A bias in the estimation is observed. Right: One additional emitter is considered and the estimation cloud comes closer to the tag's location.

to the probability of an estimated point being an outlier based on the Kolmogorov distance tes, implemented in [7]. The average value of the 10% locations with the lowest score (to be an outlier) are considered the final estimation:

$$\widehat{\mathbf{x}}_T^{\text{NoOutliers}} = \sum_{l=1}^{L} \frac{1}{L} [\widehat{x}_T^l \ \ \widehat{y}_T^l]^T. \tag{5.27}$$
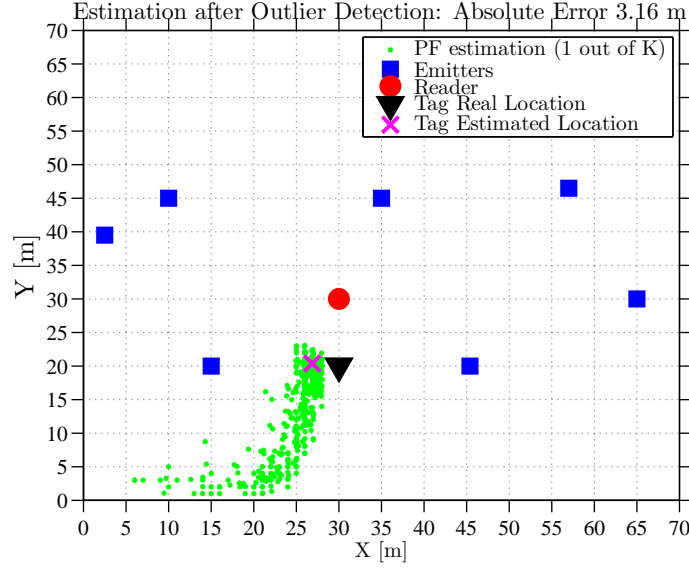
Figure 5.7: Sensor location estimation ($M = 100.000$ particles, $T = 10$ samples, $K = 100$ independent PFs runs) utilizing all the available 7 emitters. The formed curve indicates the existence of outliers, which are removed by outlier detection algorithm in [7].

Fig. 5.7 demonstrates the final estimated location after the outliers' detection.

There are many reasons for the observed errors and for the uncertainty yielded by the observed parabola: Imperfect estimation of the PLEs, constructive or destructive fading which may alter the RSS levels (and it is out of our control), unpredictable interferences from neighbouring GSM bands, USRP non linearities etc. Most importantly, the topology of the emitters affects localization accuracy, since it was experimentally observed that specific topologies such as anti-symmetric emitters by the tag improve the localization error.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

This work aimed at the development of RSS-based localization algorithms for RF devices in real world environments. Our purpose was to demonstrate the universal need for RSS-based localization of *any* RF device. For example, the cellular telephony base stations are unlisted and the knowledge of their location could enable countless applications. Furthermore, RF tag-sensor localization is of tremendous importance to enable ultra-large scale sensing applications in daily life. Thus, this thesis studied both RF-source in cellular telephony and RF tag-sensor in bistatic sensor networks localization.

In this context, RF source localization was considered as the first localization case study, since the unknown and unlisted locations of RF sources are of immense importance for several reasons such as public awareness, to corroborate GPS alternative services for cellular telephony users etc. A vast number of *real world* RSS measurements (over 2.3 million distinct RSS values for the studied cells) was collected through the automated community of users-smartphone network. This thesis incorporated careful modeling of the time-varying source transmission power, source antenna directionality and different path loss exponents among the various users source-user links. The vast number of real world measurements in combination with the careful modeling of real world cellular telephony parameters, resulted in a location estimation error on the order of 50m, outperforming prior art.

Furthermore, the problem of RF tag-sensor localization in bistatic scatter networks was also studied, motivated by the fact that an RF tag cannot be equipped with an expensive and power demanding GPS module. Nevertheless, the accurate location estimation of sensors is a key enabling future for

ultra large scale deployments, where the network must be self-configured and auto-organized. Careful modeling of the RSS was done, taking into account the bistatic scatter radio signal model, which differs from typical point-to-point links. The proposed methodology for localization with multiple low cost carrier emitters offered very promising results both in simulation and real world experimentation. Most importantly a carrier emitter is two order of magnitude cheaper than a conventional reader, therefore, the proposed localization setup is much cheaper than prior art which mainly utilizes multiple readers for RF tag localization.

The simulations demonstrated that the localization accuracy is improved while the number of emitters increases. Finally, experimental results indicated that outlier detection techniques can shrink localization error in the order of 3m in a topology of 70m x 70m, while prior art mainly focus on topologies of few meters. With the proposed localization framework we provide an automated way for RF tag localization, therefore there is no need to record one by one of thousand of sensors; the corresponding database would be automatically updated.

6.2 Future Work

This work was a first step for RSS-based localization considering real world parameters that affect the RSS. Future work could include the following topics:

Firstly, users have provided to community RF sensing platform several millions of RSS measurements from other cells. Thus, these measurements could be exploited for RF-source localization in different cell towers at Chania, if the network carriers provide a few more RF sources locations for validation. In addition, particle filtering should be tested with different resampling algorithms as well as with resampling after several weightings.

The proposed methodology is a concrete example of a crowd-sensing application and the collected data could be used in a wire range of research applications such as the prediction of the volume of wireless throughput utilizing users' RSS [39]. More importantly, the location of the unknown base

stations are important for public awareness for the cellular telephony, therefore, maps which associate low mobile's transmission power with a dense cell tower network are necessary. Finally, the estimated unknown locations could be used for RSS-based localization of the users, providing a GPS alternative to the community.

MISO RF sensing needs further experimental validation. A permanent, water and humidity proofed, setup with multiple emitters and an RF tag to be localized should be installed outdoors. Thus, effects of different fading due to the different setup at each day will be avoided. Different PLEs for carrier-to-tag links and carrier-to-reader links should be considered also. Moreover, several other tag/emitters setups should be tested.

Appendix

The RSS of the user j by the specific serving cell, according [27], is given by:

$$P^{(t)}_{[j,\text{cID}]} \triangleq P^{(t)}_{\text{TX}} G_{\text{TX}} L(d) = P^{(t)}_{\text{TX}} G_{\text{TX}} K G_j \frac{1}{\|\mathbf{x}_{\text{BS}} - \mathbf{x}_j\|_2^{n_j}}, \text{in mW}, \qquad (6.1)$$

where the $L(d)$ is the propagation loss, which is dependent of the receiver and a deterministic function of the distance $d = \|\mathbf{x}_{\text{BS}} - \mathbf{x}_j\|_2$ and represent average path-loss on the given distance. More specifically, G_{TX} is the transmission gain. K depends on the overall antenna efficiency and is necessary to scale $P_{\text{TX}} G_{\text{TX}} \frac{1}{\|\mathbf{x}_{\text{BS}} - \mathbf{x}_j\|_2^{n_j}}$ appropriately in order to offer received values in power, where G_{j} is the receiver gain. The signal attenuates with the inverse PLE law [27]. Moreover, $P^{(t)}_{\text{TX}}$ is the transmitted power at time moment t and n_j is the distinct PLE of the user j.

We consider the received power at the reference distance $d_0 = 1m$, in order to simplify the former equation:

$$P^{(t)}_{[j,\text{cID}]}(d_0 = 1m) = P^{(t)}_{\text{TX}} G_{\text{TX}} K_{eff} G_j \frac{1}{1^{n_j}}, \text{in mW}. \qquad (6.2)$$

If we divide 6.1 with 6.2:

$$\frac{P^{(t)}_{[j,\text{cID}]}}{P^{(t)}_{[j,\text{cID}]}(d_0 = 1m)} = \frac{\|\mathbf{x}_{\text{BS}} - \mathbf{x}_j\|_2^{-n_j}}{d_0^{-n_j}}. \qquad (6.3)$$

where $P^{(t)}_{[j,\text{cID}]}(d_0 = 1m)$ is calculated by the Friss equation according to [9] and [27]. The former equation can be expressed in dBm:

$$10 \log_{10} \left(P_{[j,\text{cID}]}^{(t)} \right) = 10 \log_{10} \left(P_{[j,\text{cID}]}^{(t)}(d_0 = 1m) \frac{\|\mathbf{x}_{\text{BS}} - \mathbf{x}_j\|_2^{-n_j}}{d_0^{-n_j}} \right) \Leftrightarrow$$

$$P_{[j,\text{cID}]}^{(t)}(\text{dBm}) = 10 \log_{10} \left(P_{[j,\text{cID}]}^{(t)}(d_0 = 1m) \right) + 10 \log_{10} \left(\frac{\|\mathbf{x}_{\text{BS}} - \mathbf{x}_j\|_2^{-n_j}}{d_0^{-n_j}} \right) \Leftrightarrow$$

$$P_{[j,\text{cID}]}^{(t)}(\text{dBm}) = P_0^{(t)} - 10 n_j \log_{10} \left(\frac{\|\mathbf{x}_{\text{BS}} - \mathbf{x}_j\|_2}{d_0} \right),$$

where, $P_0^{(t)}$ is expressed in dBm.

Bibliography

[1] M. Sailly, G. Sebire, and E. Riddington, *GSM/EDGE Evolution and Performance.*, Chichester, UK: Wiley, 2011, ch. 13.5.3, Energy Saving Mode on BCCH transceiver. 8, 27, 28, 29

[2] Nokia-Siemens, *Energy saving mode for BCCH TRX*, GSM/EDGE BSS20958 Operating Documentation, Nokia Siemens Networks, 2009, DN70645902, issue 1-2, available online. 8, 27, 28

[3] Ericson, *Boosting Downlink Output Power*, User Description Manual, Ericson AB, 2003, available online. 8, 27, 28

[4] Cisco, "Antenna Patterns and Their Meaning," Cisco Networks, Tech. Rep., 2007, available online. 8, 30, 32

[5] J. Kimionis, "Bistatic Scatter Radio for Increased-range Environmental Sensing," M.Sc. Thesis, School of Electronic and Computer Engineering, Technical Univ. of Crete, Chania, Aug. 2013. 9, 43, 44, 45

[6] J. Kimionis, A. Bletsas, and J. N. Sahalos, "Increased range bistatic scatter radio," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1091–1104, Mar. 2014. 9, 15, 16, 47, 48, 49

[7] M. Kim, "Anomaly Detection," Tech. Rep., Dec. 2012, available online at www.mathworks.com/matlabcentral/fileexchange/39593-anomaly-detection. 10, 62, 63, 64

[8] Y. Zhang, L. Bao, M. Welling, and S.-H. Yang, "Base station localization in search of empty spectrum spaces in cognitive radio networks," in *IEEE Int. Conf. on Mobile Ad-hoc and Sensor Networks, MSN'09.*, Wu Yi Mountain, China, Dec 2009, pp. 94–101. 13, 14

[9] N. Patwari, A. O. Hero III, M. Perkins, N. S. Correal, and R. J. O'Dea, "Relative location estimation in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 51, no. 8, pp. 2137–2148, Aug. 2003. 13, 26, 68

[10] G. Zanca, F. Zorzi, A. Zanella, and M. Zorzi, "Experimental comparison of rssi-based localization algorithms for indoor wireless sensor networks," in *Proc. of the Workshop on Real-world Wireless Sensor Networks (REALWSN).*, Glasgow, Scotland: ACM, 2008, pp. 1–5. [Online]. Available: http://doi.acm.org/10.1145/1435473.1435475 13

[11] Y. Cheng, Y. Chawathe, A. LaMarca, and J. Krumm, "Accuracy characterization for metropolitan-scale Wi-Fi localization," in *ACM Int. Conf. on Mobile Systems, Applications and Services (MobiSys)*, Seattle WA, USA, 2005, pp. 233–245. 14

[12] R. M. Vaghefi, M. R. Gholami, and E. G. Strom, "RSS-based sensor localization with unknown transmit power," in *IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP)*, Prague, Czech Republic, May 2011, pp. 2480–2483. 14

[13] X. Li, "RSS-based location estimation with unknown pathloss model," *IEEE Trans. Wireless Commun.*, vol. 5, no. 12, pp. 3626–3633, Dec. 2006. 14

[14] G. Wang, H. Chen, Y. Li, and M. Jin, "On received-signal-strength based localization with unknown transmit power and path loss exponent," *IEEE Wireless Commun. Lett.*, vol. 1, no. 5, pp. 536–539, Oct 2012. 14

[15] A. A. Gorji and B. D. O. Anderson, "Emitter localization using received-strength-signal data," *Elsevier Signal Process.*, vol. 93, no. 5, pp. 996–1012, May 2013. [Online]. Available: http://dx.doi.org/10.1016/j.sigpro.2012.11.020 14

[16] J. Shirahama and T. Ohtsuki, "RSS-based localization in environments with different path loss exponent for each link," in *IEEE Vehicular Technology Conf. (VTC).*, Singapore, May 2008, pp. 1509–1513. 14

[17] J. Yang, A. Varshavsky, H. Liu, Y. Chen, and M. Gruteser, "Accuracy characterization of cell tower localization," in *ACM Int. Conf. on Ubiquitous Computing (Ubicomp)*, Copenhagen, Denmark, Sep 2010, pp. 223–226. [Online]. Available: http://doi.acm.org/10.1145/1864349. 1864384 15, 39

[18] A. Varshavsky, D. Pankratov, J. Krumm, and E. De Lara, "Calibree: Calibration-free localization using relative distance estimations," in *Springer Pervasive Computing*, May 2008, pp. 146–161. 15, 39

[19] M. Y. Chen, T. Sohn, D. Chmelev, D. Haehnel, J. Hightower, J. Hughes, A. LaMarca, F. Potter, I. Smith, and A. Varshavsky, "Practical metropolitan-scale positioning for GSM phones," in *Int. Conf. on Ubiquitous Computing (Ubicomp)*, Newport Beach, California, Sep 2006, pp. 225–242. 15, 39

[20] M. Dashti, S. Ali-Löytty, L. Wirola, P. Müller, H. Nurminen, and R. Piché, "Robust kalman filter for positioning with wireless BS coverage areas," in *9th Workshop on Positioning Navigation and Communication (WPNC)*, Dresden, Germany, March 2012, pp. 83–88. 15

[21] E. Kampianakis, J. Kimionis, K. Tountas, C. Konstantopoulos, E. Koutroulis, and A. Bletsas, "Wireless environmental sensor networking with analog scatter radio & timer principles," *Sensors Journal, IEEE*, 2014, to appear. 15

[22] P. N. Alevizos, N. Fasarakis-Hilliard, K. Tountas, N. Agadakos, N. Kargas, and A. Bletsas, "Channel coding for increased range bistatic backscatter radio: Experimental results," in *IEEE Int. Conf. on RFID Technologies and Applications (RFID-TA)*, Tampere, Finland, Sep. 2014, accepted. 16

[23] W. Shi and V. Wong, "MDS-Based Localization Algorithm for RFID Systems," in *IEEE International Conference on Communications (ICC)*, June 2011, pp. 1–6. 16

[24] K. Chawla, G. Robins, and L. Zhang, "Object localization using RFID," in *Wireless Pervasive Computing (ISWPC), 2010 5th IEEE International Symposium on*, May 2010, pp. 301–306. 16

[25] A. Povalac, "Spatial Identification Methods and Systems for RFID Tags." Ph.D. Thesis, School of Electrical Engineering and Communication, Department of Radio Electronics, Brno University of Technology, 2012. 16

[26] E. Alimpertis, "Community RF Sensing," Diploma Thesis, School of Electronic and Computer Engineering, Technical Univ. of Crete, Chania, Oct. 2012, available online at www.mysignals.gr/research.php. 18, 21, 22, 23

[27] B. Sklar, "Rayleigh fading channels in mobile digital communication systems. Part I: Characterization," *IEEE Commun. Mag.*, vol. 35, no. 7, pp. 90–100, Jul. 1997. 26, 53, 59, 68

[28] ETSI, *Digital cellular telecommunication system (phase 2+), Radio subsystem link Control*, ETSI, GSM Technical Specification, Jun. 1996, bCCH Carrier, ch. 7.1 ,TS 05.08. 27

[29] S. Bregni, R. Cioffi, and M. Decina, "An empirical study on statistical properties of GSM telephone call arrivals," in *IEEE Global Commun. Conf. (Globecom)*, San Francisco, CA, Nov 2006, pp. 1–5. 28

[30] V. NIŢU and G. LOJEWSKI, "Comparison of the average output power of gsm and umts mobile phones and the impact in exposure to electromagnetic waves," vol. 76, 2014. 29

[31] S. sheet, *900 MHz Sector Antenna, REN 68715 SN-90*, CSG Networks. 31

[32] J. Shirahama and T. Ohtsuki, "RSS-based localization in environments with different path loss exponent for each link," in *IEEE Vehicular Technology Conf. (VTC).*, Singapore, May 2008, pp. 1509–1513. 32, 39

[33] S. Thrun, W. Burgard, and D. Fox, *Probabilistic Robotics.*, Cambridge, MA: The MIT Press, 2006. 34, 36, 37, 57, 58, 59

[34] B. C. Levy, *Principles of Signal Detection and Parameter Estimation.*, New York, USA: Springer, 2008. 36

[35] E. Alimpertis, N. Fasarakis-Hilliard, and A. Bletsas, "Community RF Sensing for Source Localization," *IEEE Wireless Commun. Lett.*, 2014, to appear. 36

[36] R. Vaghefi, M. Gholami, R. Buehrer, and E. Strom, "Cooperative received signal strength-based sensor localization with unknown transmit powers," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1389–1403, March 2013. 40

[37] K. Tountas, "Implementation of Frequency Division Multiple Access Digital Backscatter Sensor Netwok," Diploma Thesis, School of Electronic and Computer Engineering, Technical Univ. of Crete, Chania, Sep. 2014. 42, 44

[38] J. G. Proakis and M. Salehi, *Communication Systems Engineering*, 2nd ed., Prentice-Hall International, Inc., 2002. 53

[39] W. Guo and S. Wang, "Mobile crowd-sensing wireless activity with measured interference power," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 539–542, Oct 2013. 66