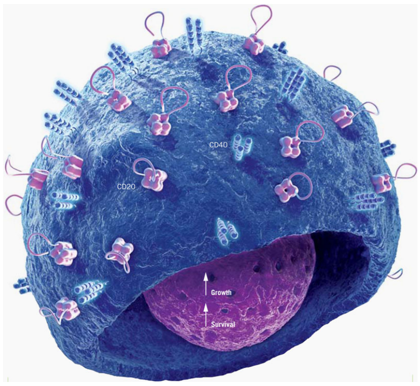

BLE supported indoor location

Subtitle

Ricardo Pacheco Pais Martins

Thesis to obtain the Master of Science Degree in

Elecrical and Computer Engineering

Supervisor(s): Prof./Dr. Lorem Ipsum

Examinatiom Committee

Chairperson: Prof. Lorem
Supervisor: Prof. Lorem Ipsum
Co-Supervisor: Prof. Lorem Ipsum
Members of the Committe: Dr. Lorem Ipsum
Prof. Lorem Ipsum

March 2017

Anyone who has never made a mistake has never tried anything new.

Albert Einstein

Acknowledgments

I would like to thank the Academy,laura, jnos, pais, pais da laura, leal , almeida etc... bla bla bla..

Abstract

The Objective of this Work ... (English)

Keywords

Keywords (English)

Resumo

O objectivo deste trabalho ... (Português)

Palavras Chave

Palavras-Chave (Português)

Contents

List of Figures

List of Tables

Abbreviations

GPS Gloobal Positioning System

LAN Local Area Network

BLE Bluetooth Low Energy

LE Low Energy

RSSI Received Signal Strength Indicator

IoT Internet of Things

SMP Security Manager Protocol

PHY Physical

QoS Quality of Service

L2CAP Logical Link Control and Adaptation Protocol

HCI Host Controller Interface

P2P Peer-to-Peer

ATT Attribute Protocol

GATT Generic Attribute

GAP Generic Access Profile

FDMA Frequency Division Multiple Access

TDMA Time Division Multiple Access

RF Radio Frequency

US Ultrasound

RFID Radio Frequency Identification

WLAN Wireless Local Area Network

CSI Channel State Information

LOS Line-of-Sight

IR Infrared

UWB Ultra-Wideband

ToA Time of Arrival

TDoA Time Difference of Arrival

RToF Roundtrip Time of Flight

AoA Angle of Arrival

FM Frequency Modulation

CoO Cell of Origin

DR Dead Reckoning

List of Symbols

1

Introduction

Contents

The development of navigation systems began in the 1930's with the second world war and opened the door for a continuous research for better and more precise systems capable of providing real-time locations under any circumstances. The most widely known positioning system is the Gloobal Positioning System (GPS), a system whose development begun in the 70's with a military purpose in mind, and is nowadays available and used by everyone with a capable device, be it a smartphone, a portable GPS-device or even a car with incorporated GPS system. This passage occored over the last few years with the advancement of technology and allowed it to become more and more something readily available to anyone, which then allowed for outdoor location to become something of our everyday life in the form of navigation systems, with its most widely used application being google maps.

With the GPS taking the crown in the outdoor location system due to its incomparable success, the research target changed to indoor location but since it's an outdoor position systems based on a network of satellite, when the required scenario for position tracking is the inside a building, new constraints are presented onto the process such as the attenuation and reflection of electromagnetic waves upon collision with building walls and obstacles [7]. As such there was a need to find reliable indoor systems that by nature would already be able to heavily reduce the impact of some of the mentioned constraints.

In order to understand indoor position there is a need to understand the full scope of variables that come to surface when moving from outdoor to indoor. When developing an indoor system there is a need to make sure that it can tackle challenges such as: small space dimension, which reenforces the need for higher precision; a higher probability of non existent line of sight; influence of obstacles such as walls, furniture and moveable objects such as doors and human beings [8]. All of the previously mentioned affect the way electromagnetic waves propagate in an indoor environment leading to problems related to severe multi-path and reflection on existent surfaces [9]. Besides propagation challenges, there are energy consumption, accuracy and deployment costs that play a critical role in deciding the viability of a proposed indoor location technique.

Indoor positioning systems research has been capable of introducing new technologies other than satellites, whose most relevant characteristic is that they are deployed site-wise and as such have a much smaller range and are capable of at least providing a much clearer line of sight between deployed device and target, which was the hardest obstacle to GPS due to the fact that it's a satellite-based system. These smaller scale technologies are meant to be deployed inside building and in much greater number due to their reduced cost. Over the course of the last ten years, the technologies that were indicated as the ones capable of providing a better indoor location system have been ever-changing as with time the technologies themselves have evolved as well. One of the biggest factors for it has been the evolution of mobile devices which have greatly evolved and have now available a far superior range of different sensors, higher processing capacity and different technologies such as Bluetooth Low Energy (BLE), Wi-FI or Radio Frequency Identification (RFID). As such smartphones have made introduced new possibilities to the world of indoor location such as GPS-based technologies, using high sensitivity antennas to overcome GPS's indoor issues, RFID , Wireless Local

Area Network (LAN) and Bluetooth among others, allowing even for hybrid systems which make use of more than one of the technologies mentioned above. [7, 9, 10].

This chapter provides an overview of the Thesis. Section 1.1 lays out the motivation and the context of the problem being analysed and section 1.2 presents the current state of indoor location systems. The contributions of this work are presented on section 1.3 and 1.4 outlines the rest of the work.

1.1 Motivation

The success of GPS as an outdoor location system and its difficulties to have the same success in the indoor location system's environment sparkled the research for different technologies capable of filling the hole. As such in the last fifteen years many indoor system's have been created which attempted to solve the problem using one or more technologies, each with their strengths and weaknesses.

With the advancement of smartphones they are now capable of providing many more tools that can be useful for indoor location such as GPS, Wi-Fi, GSM, camera, FM radio, Bluetooth and microphone. Beside these tools, nowadays they even have inertial sensors such as accelerometers, gyroscopes or digital compasses which ,together with ones that were previously mentioned, provide a wide variety of possibilities. Since this field is still in development and there is a big amount of different scenarios in which it has to be applied that consequently brings onto the table different objectives and requirements, every existent solution can be useful for a certain amount of cases due to the nature of each of them. As such there is a huge quantity of existent solutions that have been researched for each technology which then can even branch out according to all the possible optimisations that have to be applied in order to achieved the project's requirements.

This occurrence has led to a need to registrate the state of the indoor location which has been fulfilled by all the existing surveys on the existent technologies [10, 11], which gather up all the existent technologies in the field and analyse them according to their cost, precision, energy efficiency, scalability, privacy, among others criteria. Other surveys analyse technologies on a more specific level by focusing on existent projects to compare their performances [9]. Another relevant aspect that has been surveyed is the existent techniques utilised [7, 8, 12] by analysing the different metrics utilised to calculate a user's position and comparing their strengths and weaknesses according to coverage, line-of-sight and multi-path problems and cost.

With the situation as is there is big majority of the attention focused on the improving and creating new means to achieve better positioning results, as it is possible to notice from the vast number of existing methods and algorithms available to infer someone's location. Although this part is of great importance, as the success of a location system in the present day is highly dependant on its accuracy levels, another extremely relevant concern for any system is their energetic consumption. With smartphone being the traditional means in any current system, due to its available technologies, it is important to interiorise that it's a personal device with a limited amount of resources, such as battery.

Another important factor is that an indoor system needs to be scalable, be in function of number of users in the same indoor building or in terms of being capable of working with different deployments/buildings. Systems created with the purpose of being used in multiple different environments need to provide an architecture capable of working seamlessly when transferring between buildings. As such it is required that the one smartphone (mobile agent) capable of working with the system is able to obtaining its own location wherever the system is deployed.

The objective of this work is to present and implement a generic architectural framework whose intent is to provide an architecture where the previously present requirements are followed. A system implemented on this framework should be capable of bringing the energetic costs of the smartphone to a minimum while allowing itself to be scalable, deployed in multiple sites and reducing the required smartphone space to a minimum.

The previously mentioned generic architecture framework can be visualised in figure 1.1. This architecture makes use of the technologic advancements on mobile phones to use them as the central point of communication of the architecture. This decision may make it seem so that the energetic cost on the smartphone takes a big impact due to the extra effort required for all the communication but it is the opposite as with it being the central piece, i.e. every other element is capable of reaching the smartphone, the data storage and location processing can be externalised onto servers. On this architecture the beacons are responsible for providing the smartphone information about its surroundings, information that is later on passed onto the location server. This server is responsible of computing the user's location and send it back to him. Once the smartphone is aware of its position, he can request the map server and present the result of the whole process visually to the user.

In order test the idealised architecture, it was necessary to implement a system on it. The chosen technology was the bluetooth low energy, a recent technology that is trying to improve its core in order to be usable on Internet of Things (IoT) and it was capable of providing room-based accuracy without much effort on the algorithm department. The beacon component of the architecture was implement by making use of ble beacon. Each of the used beacons is uniquely identified by its identification and also knows to which location server he belongs to. Whenever a mobile user is nearby an environment where these beacons are present, the mobile user is capable of establishing with them a connection in order to confirm that they do indeed belong to the indoor location system and to access the beacon's data in order to collect information on its owner server.

Once the mobile user has all the data from surrounding devices, i.e. he has data associated to the signals collected from each beacon and the address of their server, he can forward it to the location server. The location server is in possession of a database of all of its associated devices and it is against it that he will compare any data received from mobile users. Upon confirming that the devices belong to it, he can apply its location algorithm to the received data, compute the user's location and send it back to him.

Upon receiving the user's location, the smartphone is just missing the visual representation of the same location. To do so it sends its location into the map server. The map server in the generic architecture framework represents a server which has a database of all the maps for a certain location server. For this implementation the map server utilised was google maps since its indoor maps feature was available in the testing place. As such, the location of the mobile user is requested to google maps through its API and presented to the user on its smartphone's screen.

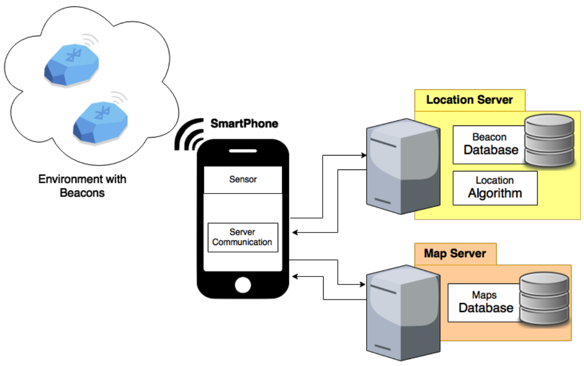

Figure 1.1: Generic Architecture Framework

1.2 State of The Art

State of The Art Section.

1.2.1 Dummy Subsection A

State of Art Subsection A

1.2.2 Dummy Subsection B

State of Art Subsection B

1.3 Original Contributions

Contributions Section.

1.4 Thesis Outline

Chapter 2 of this thesis analyzes the technology that's utilized in the implemented solution,bluetooth low energy's architecture and functionality. The different manners of obtain the metrics utilized to obtain an object's position as well as some location algorithms are also reviewed in this chapter, which is finalized by overview existant related work, from the older ones that functioned as reference in the field to more recent work using BLE. Chapter 3 presents the architecture of the projected generic indoor system by analyzing each component according to its responsabilities while chapter 4 demonstrates the implemented BLE solution based on the previously presented generic architecture.

2

Indoor positioning

Contents

This chapter gives an overview of the state of the art of Indoor positioning solutions. The Bluetooth Low Energy (BLE)'s architecture and functionality is analysed in section 2.4, while section 2.1 overviews the other existing technologies. The most common techniques utilised for position computation along side examples which make use of them are explained in section 2.2. Finally on section 2.3 analyses the most projects that had the most relevance in the field and the existing work related to BLE.

2.1 Indoor location support technologies

When looking at the state of indoor positioning systems, it's clear that there isn't one technology that is better than all of the others. As so it's important to look at each of the possible technologies individually and assess its benefits and drawbacks as well as their performance.

In this chapter many existent indoor positioning technologies are analysed. The most pertinent ones, RFID, Wi-Fi, Infrared and UWB, are explained in a more detailed manner in subsections 2.1.1, 2.1.2, 2.1.3 and 2.1.4 respectively, while less utilised technologies are described in subsection 2.1.5. For each of the present technologies a description is provided about their nature, tags and pros and cons, all of which is complemented with at least one existent system that makes use of the specific technology being described.

2.1.1 RFID

RFID is a technology for storing and retrieving data through electromagnetic transmission to an RF compatible integrated circuit. A RFID system is composed by three components: readers, tags and the communication between both. The reader is capable of reading the data that is being emitted from RFID tags via radio waves and the data usually consists of the tag's unique identification number which can be related to the tag's available position information in order to obtain the user's position. This communication is achieved by having a well-defined radio frequency and protocol which allows for reading and transmitting data. The RFID tags can be of two types: active or passive.

Active tags are small transceivers equipped with an internal battery, which makes them heavier and more costly while allowing for longer detection ranges when compared to their counter-parts. These tags are suited for identification of important units moving through rough processes or positioning in system where location estimation is often carried out through fingerprinting on Received Signal Strength Indicator (RSSI). Passive tags are operated without the need of a battery since they are capable of receiving enough energy in the form of radio frequency waves from nearby RFID scanners in order to transmit back the answers. These tags are used to replace the barcode technology since they are much lighter, smaller and less expensive than the active tags which allows for a relative inexpensive installation and low maintenance caused by not having batteries. One of its drawbacks is that their range is very limited, circa 2 meters, which demands for higher density of tag deployment.

RFID's biggest advantages are the non required Line-of-Sight (LOS) characteristics, their capability of working at high speeds and their relative low cost. As such this technology is often used for tracking objects in automobile assembly industry or warehouse management and tracking of people or animals. One of its most relevant projects is the SpotON [13], a tagging technology for three dimensional location sensing based on radio signal strength analysis. The tags used are custom devices that operate either standalone or as a plug in card enabling larger devices to take advantage of location-sensing technology. They are low power, small and capable of being accurate while having the computing capacity for relevant tasks such as caching, authentication, among others. SpotON tags utilise the received RSSI as a metric for obtaining inter-tag distance. Another important project using RFID is LANDMARC[1] which utilises active tags to produce a location sensing system for locating objects inside buildings. Its objective was to demonstrate that active tags can in fact be viable and cost-efficient for indoor location sensing. One of the problems found was that the hardware wasn't capable of providing RSSI readings, as such the used readers scan through eight discrete power levels in order to estimate the RSSI. This scanning coma at the cost of a significant time period. By placing the readers in known positions, the area that is being analysed can be divided into sub-regions with each being identified by the subset of readers that cover it, which can be visualised in figure 2.1. Given an RFID tag, based on the subset of readers that can detect it, the system is capable of associating the tag with a known sub-region. LANDMARC increased the accuracy without placing more readers by employing extra fixed location reference tags for location calibration.

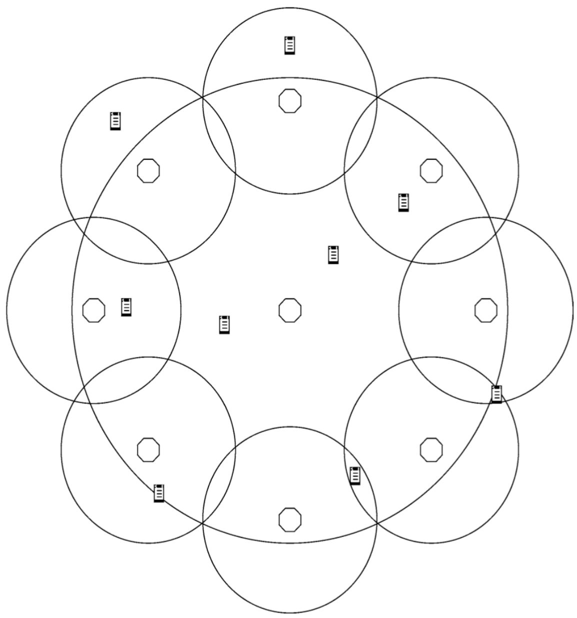

Figure 2.1: Landmarc deployment showing sub-regions (Ref [1])

2.1.2 WLAN / Wi-Fi

Wireless Local Area Network (WLAN)is a technology that can be used to estimate the location of a mobile user that resides inside the network. Nowadays Wi-Fi positioning systems have become the most widespread approach for indoor location systems since WLAN access points are readily available in many indoor environments and any Wi-Fi compatible device (smartphones, laptops ,tablets) can be located without the need of installing extra software or manipulating the hardware. Its popularity is also due to its range of 100 to 50 meters, which is better than RFID and BLE's range, and since LOS isn't required. One issue of WLAN signals is that they suffer attenuation from static environment such as walls and movement of furniture and doors. In these kind of systems position computation is obtained through TOA, AOA, RSS, and CSI, which are properly analysed in section 2.2, with multiple existing projects for each one of the existent methods. The most widely used is the RSSI, which suffers from severe multi-path effects leading to propagation model failures and as such inaccuracy in distance measurement. With these problems in mind a technique called RSSI-based fingerprinting is often used in order to improve performance. Most recently an alternative to RSSI has been researched called Channel State Information (CSI). CSI is widely available on commercial products and it represents the channel conditions over individual OFDM subcarriers across the Physical (PHY) layer. One of the improvements is that instead of obtaining one RSSI value per packet, multiple CSI values can be obtained from multiple subcarriers at a time. FILA [2] was a project that attempted to use CSI for locating targets in complicated indoor environments where RSSI wasn't reliable due to multi-path. This system is capable of extracting the LOS path for distance calculating through time-domain multi-path mitigation and frequency-domain fading compensation and with a simple trilateration calculation they were able to achieve a much better performance than with RSSI for these kind of scenarios. The performance comparison showing the differences in temporal stability between RSSI and CSI can be seen on figure 2.2.

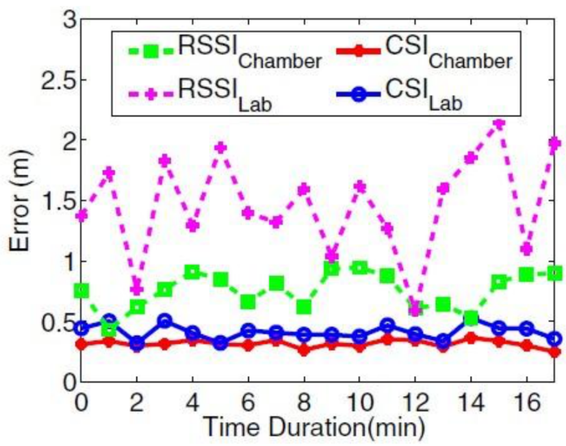

Figure 2.2: Comparison of temporal stability (Ref [2])

2.1.3 Infrared

Infrared (IR) systems are one of the most common position system that utilise wireless technology that has been used to track objects or people. IR wavelengths are invisible to the human eye under most circumstances, making this technology less intrusive than those which are visible. This technology is widely available in various common devices such as mobile phones, PDA's and Tv's and requires LOS communication between receiver and transmitter, preferably without interference from strong light sources. These types of system utilise small, lightweight and easily wearable devices which have the downside of having privacy/security issues. One of the most relevant systems based on IR is the Active Badge system which is described in section 2.3. There are three methods of exploiting infrared signals: Through active beacons, infrared imaging or artificial light sources.

The active beacon's approach is the one utilised by the active badge system and it involves placing fixed IR beacons on known positions. The density of deployment of beacons depends on the objective of the system but if the required is a room-based location, i.e. being able to tell in which room a user is located, a beacon per room should be enough.

Infrared imaging, also known as passive IR systems, makes use of sensors operating in the IR spectrum which are capable of obtaining a complete image of the surrounding from thermal emissions. This approach doesn't require the deployment of any extra hardware or tag for determining the temperature of objects or people but it does get compromised in the presence of strong radiation from the sun. Some known equipments that utilise this approach are thermal cameras, infrared sensors for motion detection or thermocouples used to measure temperature contact free.

IR systems based on artificial light sources are a good alternative to the ones that operate on the visible spectrum. A very well known example is the microsoft Kinect system which uses continuously-projected infrared structured light to capture 3D scene information with an infrared camera. This system is capable of tracking a person's movement up to 3.5 meters with a precision of a few centimetres.

2.1.4 Ultra-Wideband

Ultra-Wideband (UWB) is a radio technology aimed at short-range high-bandwidth communication. Its best characteristics are its capacity of being resistant to multi-path and to some degree being capable of penetrating building materials, such as concrete and wood, with low power consumption. Both these factors allow UWB to achieve high positioning accuracy while the latter enables to address the range in non line-of-sight conditions and makes inter-room ranging possible. Being able to penetrate building material creates precision issues due to the increase in data complexity, making data interpretation one of the biggest challenges to be faced. The usual structure of a UWB system has a stimulus radio wave generator and receivers which capture the propagated and scattered waves and it has four types of methods for position calculation. The first one, passive UWB, attempts to track objects or people through signal reflection. This method doesn't require any sort of tag to be carried by the user or attached to the object and requires only at least on emitter and a few listeners to obtain a location. Since the locations of the antennas as known and it is possible to estimate the distance from user to listener through Time of Arrival (ToA) or Time Difference of Arrival (TDoA) multilateration, the user's location can be computed. The remaining methods are Direct Ranging and Fingerprinting. The first one simply requires the users to wear active tags and uses differente measures based on time to compute distances which are then worked by lateration techniques in order to produce the user's location. The second one works like a regular fingerprinting method except that it utilises Channel Impulse Response (CIR) instead of RSSI. This kind of fingerprinting has the possibility of being more accurate while being usable in non LOS scenarios. On the downside it requires time synchronisation. One commercial example of this technology is Ubisense [3], a system capable of tracking active tags equipped with batteries which have a conventional RF transciever and a UWB transmitter. The system requires a setup deployment of a network of Ubisensors, with fixed positions throughout the area to be covered and networked using Ethernet. Each sensor has a RF transceiver and phased array of UWB receivers. These sensors use a combination of TDoA and Angle of Arrival (AoA) techniques to determine the tags location, achieving an accuracy of 15 cm in a typical open environment. The system's setup can be visualised on figure 2.3.

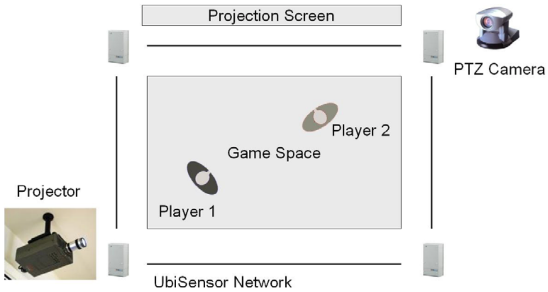

Figure 2.3: Uisense's system setup (Ref [3])

2.1.5 Other systems

Optical Indoor positioning systems are systems that use a camera as their only or main input for position estimation. In recent years these types of systems have found an increase in success due to the improvements and size reduction of the sensors, the improvements in computational capacities and the continuos development of image processing algorithms. Optical systems can be described as a moving sensor, for example a smartphone camera, and often times a set of static sensors which detect movement and which utilise AoA techniques to estimate distances. There are many different types of optical systems, one of them makes use of 3D building models. This approach removes the need for local infrastructure deployment in the building to be monitored since the usually required reference nodes are replaced by a digital reference point. As such they are highly scalable with small increases in cost. In general optical systems are capable of achieving high accuracy but they are vulnerable to light conditions, require LOS propagations and are more computationally expensive than other types of systems.

Frequency Modulation (FM) radio Is a broadcasting technology that has been incorporated for a long time on smartphones with the intent of listening to music or to the news. This technology was originally reserved for frequency modulation to convey information over a carrier wave by varying its frequency but nowadays it just refers to any radio wave in the frequency band 88-108 MHz. This analogue radio signal has amazing advantages for urban/indoor location system such as the ability to be received indoor and outdoor, it has a dense coverage in urban areas, available without installing additional transmitters, low-cost and low-power hardware with simple technology, high received signal power and there are a large number of transmitters which provides good geometry for locating. One crucial part when utilising FM is that it doesn't carry any timing information which is critical in range calculation and the fact that as other radio frequency technologies, it suffers from multi-path effects and non-LOS signals. An example of FM system was created by et al. [14] which implemented an RSSI fingerprint-based system using FM radios in an office environment. The system's test bed obtained 17 FM channels at each point of the fingerprint and it was capable of achieving a mean accuracy of 3 meters.

Zigbee Is an emerging wireless technology standard which provides solution for short and medium range communications and its specially designed for applications which demand low-power consumption and don't require large data throughput. This technology's signal range coverage can go up to 100 meters in open space, while achieving 20 to 30 meters in indoor environments. Most zigbee-based system utilise RSSI for distance calculation and one of its most relevant disadvantage is the its vulnerability to interference from a wide range of signal types using the same frequency which can disrupt radio communication. This is caused by Zigbee operating in the unlicensed ISM (industrial, scientific and medical reserved) bands. An example of a Zigbee-based system is the one created by Larrañaga et al. [15] which attempted to locate a mobile node in an indoor environment. Their system consisted of two phases: The first one, calibration, every existent reference zigbee node transmitted message to each of the remaining. In this ways it was possible to work out the relationship between measured RSSI values and geometric distances, allowing to understand the environment moments before attempting a location. The second phase, location, utilises the data collected and the new data obtained from messages from the mobile user to the reference node to obtain its location. This system was capable of achieved an accuracy with an average error of 3 meters.

Ultrasonic Systems are utilised in indoor positioning by making use of ToA to locate targets. These kind of system make use of ultrasonic transceiver to emit and detect signals while recording times of departure and arrival of the signal. Since the signal medium traveling speed is known, it is possible to use the time difference to compute the distance between emitter and receiver. One of the most famous projects that makes use of this technology is the cricket system which is described in section 2.3.

[Hybrid] Positioning systems are systems which combine several different positioning technologies to determine the location of a user or object. These types of systems make use of different technologies in an attempt to compensate for one's shortcomings through another's strengths. One example of an hybrid system is the solution presented by versus [16] which makes use of Wi-Fi, IR and RF to provide a system capable of displaying real-time locations of people or objects inside a building. By combining these three technologies their were capable of providing a system with different level of accuracy depending on the needs, room-level, bed-level (a fragment of a room) or chair-level (precise positioning).

2.2 Position Techniques

This section's focus is on the available means of obtaining distance measurements from a mobile target to a beacon.

2.2.1 Proximity Detection

Proximity detection is one of the simplest position techniques to implement since its objective isn't to provide a precise position of the target but a symbolic relative location information. The target's position is obtained through the Cell of Origin (CoO) method which relies on a grid of antennas/beacon with a well-known position. When applying this method, if only one beacon is detected by the mobile target then the position provided is equal to the position of the beacon. If more than one beacons are detected by the target, it considers that its position is equal to the position of beacon with the strongest associated signal. In this project, since the objective wasn't to be capable of providing a bluetooth low energy with the best accuracy possible but to prove that the presented architecture was applicable to this type, the CoO method was the chosen one. As such in order to apply room-based accuracy the minimum requirement would be to place a beacon in each existent room. This method can be applied with a better accuracy in mind and doing so depends only on the deployed beacon density. This technique is often implemented in system running IR , RFID and Bluetooth.

2.2.2 Triangulation

The Triangulation techniques makes use of the geometric properties of triangles to determine the location of a mobile target. It can be of two types: lateration, which estimates a target's position by measuring its distance to multiple reference points, and angulation, which obtains the target's position by computing angles relative to multiple reference points. Lateration makes use of ToA, TDoA, Roundtrip Time of Flight (RToF) and RSSI, while angulation utilises the AoA technique. All the previously mentioned techniques are individually analysed in sections 2.2.2.A, 2.2.2.B, 2.2.2.C, 2.2.2.D and 2.2.2.E.

2.2.2.A Time of Arrival (ToA)

ToA-based systems rely on accurate clock synchronisation and signal message sent from a mobile target to several receiving beacons. The distance that is to be used in the calculation of the target's position is proportional to the propagation time. As such the message sent from the mobile target is timestamped with its departure time allowing for the receiving beacons to obtained their distance to the target through the transmission time and the associated signal propagation speed. One of the consequences of requiring precise knowledge of transmission start times is that every single device, beacon and mobile target, need to be accurately synchronised with a precise time source which causes this technique to be the most accurate one in indoor environments since it's capable of filtering multi-path effects. On the others hand the disadvantages of using this technique is the synchronisation requirements and the additional information that needs to be contained in the sent messages, i.e. timestamps.

2.2.2.B Time Difference of Arrival (TDoA)

TDoA systems attempt to determine the relative position of a mobile target by examining the differences in time at which the signal arrives at multiple beacons. This technique doesn't require clock synchronisation with the sender as there is no need for timestamps to obtain its location, making this requirement only present on the receivers. The location is obtain from a transmission with unknown starting time that is received in multiple synchronised receivers which produces multiple TDoA measurements. Each difference in arrival times produces a TDoA and consequently a hyperbolic curve on which the target is located. Each intersection of multiple hyperbolic curves represents a possible location of the target, requiring two or more measurements in order to obtain the location on a two dimensional plane. One example that makes use of this technique is the cricket system which is explained on section 2.3.

2.2.2.C Roundtrip Time of Flight (RToF)

This technique obtains distances by measuring the time-of-flight of the signal pulse traveling from the transmitter to the receiver (measuring unit) and back. This solution solves some of the synchronisation issues presented by ToA since only the only one of the two nodes records the transmission and arrival times, with the conversion from time to distance being equal to the one applied with ToA. The mechanism of obtaining a time reading is similar to that of a radar, i.e. a signal is sent to which the receiving node replies back to the transmitter. When the response signal is received the roundtrip time is obtained. One issue presented by using this technique is the incapability of knowing the time delay on the receiver between receiving the first signal and sending the response. This unknown delay can be ignore in medium to long-ranged systems if its value is relatively small when compared to the transmission time. In short-ranged system this situation can't be applied and as such this technique isn't suited to be applied.

2.2.2.D RSSI

Received Signal Strength Information (RSSI) is a non-linear signal strength indicator based on signal attenuation that is only usable with radio signals. The conversion of this value to distance is often achieved through estimates of signal path loss due to propagation, although this approach doesn't hold is scenarios where severe multi-path effects and shadowing are present.

A technique that is often used with RSSI is the fingerprint method which is the process of computing the location of a user by matching its location-dependent signal characteristics to an existing fingerprint database. This method doesn't required any additional hardware on the mobile device or the beacons as well as no time synchronisation. This process is divided in two stages: an offline and an online phase. In the offline stage, also called calibration phase, the maps for the fingerprint are set up either empirically in measurement operations or computed analytically through a signal propagation model. For the first option multiple positions are defined on the map. On each of this positions a mobile user captures the signal strengths received from each of the existent beacons. An example of this method's data collection setup can be seen on figure 2.4. With the fingerprint concluded, begins the online phase, where mobile users are already capable of being tracked. In order to obtain a user's position it must measure the existent signal properties, which are then compared with the fingerprint database so that a as close as possible match can be found. Position matching is can be achieved through pattern recognition techniques such as K-nearest-neighbours (KNN), support vector machines (SVM), among others. This approach has the drawbacks of being labour intensive and time consuming on the offline phase and the difficulty to maintain and update the fingerprint database in order for it to be in accordance to the current environment. The second drawback is caused by RSSI's sensibility to changes in the environment such as dynamic factors (people and doors), diffraction and reflection.

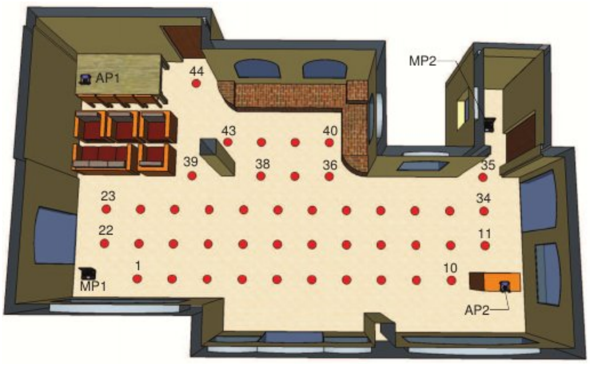

Figure 2.4: Fingerprint example with data collection positions (Ref [4])

2.2.2.E Angle of Arrival (AoA)

The AoA technique finds the location of the target by intersecting several pairs of angle direction lines. Each of this line is part of the circular radius around a beacon which leads to the mobile target. This technique requires only two beacons for two dimensional and three for three dimensional position estimation, with any extra beacon leading to an increase in accuracy while not requiring any time synchronisation. This techniques drawbacks is the increased implementation cost due to the antennas being required to be able to measure angles and its rapid accuracy degradation as the target moves farther away from the existing beacons. This technique is capable of sub-meter accuracy although these types of systems are often limited by shadowing, multi-path reflections arriving from misleading directions or by the directivity of the measuring aperture. One example which attempted to tackle AoA's drawbacks was ArrayTrack [17] which presented a multi-path suppression algorithm capable of removing reflection paths, performance improvements in low density scenarios and parallel processing allowing for faster location estimations. This system was capable of achieving a median accuracy of 23 cm while utilising custom made access points with 16 antennas. Although successful, the hardware complexity remained an issue making this system impractical.

2.2.3 Dead Reckoning

Dead Reckoning (DR) is the process of estimating the target's current position through the last determined position incremented by known or estimated speeds over elapsed time. This technique has the advantage of providing autonomous positioning capacities. DR biggest drawback is that the inaccuracy of the process is cumulative, as such the deviation in the position estimation grows with time. This issue can be aggravated by disruptive motion such as sidestepping, back-stepping or sharp turns which produce scaling errors leading to a bigger accuracy errors. Due to DR's issues it's often accompanied by another technology in order to correct the inertial drift. A common practice is the usage of GPS ,which it doesn't function in indoor environments and as such many different combinations have been created in order to tackle this issue. Fischer et al. [18] made use of Ultrasound beacons as landmarks to provide better accuracy and less heading errors. In their work they stated the existence of two types of errors: heading errors, which are relative to the direction in which the user is heading, and distance errors. The work was targeted for rescue team first responders and required the users to drop ultrasonic beacons as they advance through the building.

2.3 Related work

Active Badge

In 1992 the Active Badge system [19] was presented as an infrared solution capable of provided room-based position tracking. The system has been designed to make use of "active badge" beacons, which can be visualised in figure 2.5 in the form of ID cards, a tag eqquiped with an IR LED that emitted a unique code for approximately a tenth of a second every 15 seconds.

Figure 2.5: Active badge's tags (Ref [5])

The decision to utilise IR was due to how small and cheap the emitters and detectors are, being capable of operating within a 6 meter range and because IR signals aren't capable of traveling through walls. The signal frequency has two major effects of the system, the first being its impact on the energy consumption of the tags, with such a small frequency allowing for long periods of work on a single battery and the second being its impact on user detection. For the used signal duration and frequency there is a chance of 1/150 for two signals to collide, which leads to a good probability that for a small number of beacons, all will be detected. One downside of such a small frequency signal is that the location of a badge can only be known, at best, to a 15 second granularity.

The position of a user is obtained through the implementation of a network of sensors which act as receivers, listening to badge transmissions, and then forward the obtained information to the master station. The master station is responsible for polling all the sensors on the network, store sighted badges into a database with its associated time, position and ID, data processing and data display. The accuracy of the system is room-based by making use of CoO and the properties of IR. A beacon in each room would make it so that each beacon is capable of detecting any badges in its room.

One of the issues that surfaced with this system were privacy issues. Due to the system's nature, the position of each badge is known in a centralised station, with the only available option for people who don't wish to be tracked, to disable their tag. Another privacy issue was the security of the system's data with needed improvements to control access to data [20].

Active Bat

In 2001 the Active bat system [21]was introduced, a system capable of tracking various object, each tagged by attaching small wireless transmitters called bats. The system's architecture is composed of small devices named bats, which are to be carried by the objects or people to be tracked, a network of Ultrasound (US) receiver units and several base stations. The receiver network and a deployed bat can be seen on figure 2.6;

Figure 2.6: Active bat (Ref [6])

A bat, which can be seen in figure 2.6, consisted of a radio transceiver, controlling logic and a ultrasonic transducer, with each having an associated globally unique ID. A Base station periodically transmits a radio message containing a single unique ID, making it so that the ID's associated bat emits a short pulse of US. At the same time, the ultrasound receivers present in the rooms covered by the base station that emitted the radio signal are reset through the wired network. From this point on, the receivers monitor for the expected US signal while recording the time spent waiting in order to obtain the signal's ToA. With a known speed of sound in air, which can be estimated from the ambient temperature, the ToA can be converted into bat-receiver distance.

The mobile target's position can be obtained through multilateration, in the three dimensional space, if three or more non-collinear receivers' distances are known. This method's accuracy is highly dependent on the distance measurement's accuracy. Distance measurement is affected by signal reflections on objects present in the environment, a problem that was correct by the use of a statistical outlier rejection algorithm. One other issue is the reverberations of the initial signal, which are required to die out before initiating another distance measurement in order to ensure that the incoming US signals are from the correct bat. As such the measurement process is divided into time-slots, with each being usable to locate one and only one bat.

The existent system is capable of being improved in order to also provide the target's orientation.

The first option is to place several bats at known points of the rigid object and finding their positions on the 3D space. In cases where multiple bat deployment isn't feasible, if the rigid object is opaque to ultrasound, one single tag might be enough to estimate the objects orientation since any cast signal leaves a shadow on the object [22].

The latest version of the bat included a sensitive motion detector that allowed it to tell the base stations whether it was moving or stationary. Since the base station doesn't require to repeatedly determine the location of a stationary object, the system places these bats into a low-power sleep state which is only removed once the bat stats moving. This implementation allowed for extra power savings while freeing up location-update opportunities for other bats [23].

This system's architecture, much like the Active badge's presented in 2.3, is tightly controlled and centralised. As such it also incurs into the same privacy issues from the active badge system. Another problem created by this system's technique is the requirement of large numbers of receivers across the ceiling and their placements which require sensitive alignments.

Radar

In 2001 the RADAR system was introduced as the first Wi-Fi signal-strength based indoor positioning system [24]. The system is Radio Frequency (RF)-based and its capable of locating and tracking users inside buildings. Radar makes use of signal-strength information obtained through a fingerprint method, presented in subsection 2.2.2.D, to triangulate the user's coordinates. The system's functions in two phases: the data collection phase, where the data is gathered in order to later construct and validate models for signal propagation, which are to be used in the real-time phase to infer user's location. In the offline phase, the type of data collected is the signal strength utilising the methodology already described for the fingerprint method.

Radar's experiments showed RSSI's problems relative to value fluctuation dependent on the user's orientation. This happens due to the existence or not of LOS between antenna and base station depending on the orientation, since the user's body may form an obstruction. As such the user's direction was also recorded in the offline phase.

Data processing involve computing the mean, standard deviation and median of RSSI for each of the used base stations (three in total) and each combination of x,y and direction. In addition, a building layout information was created which included room and base station's coordinates and the number of walls that obstructed the direct line between the base stations and each of the positions where data was collected. With all this information an accurate signal propagation modal was built.

The basic approach used to obtain a user's location was triangulation, which given a set of RSSI measurements at each base station, the user's location is guessed to be the one that best matches the observed data. In addition to this basic strategy, two others approaches were analysed: empirical and signal propagation methods.

For the first method many variations on the data was studied such as: The number of best matching values used (K-nearest neighbours (KNN)), with results showing that the benefits of averaging between multiple neighbours isn't very relevant even for small values of k as in this case it doesn't mean that there aren't k physical distinct points. Other factors were studied such as the impact of the number of samples collected or the number of data points and the impact of the user orientation, with the most relevant being the latter, having shown the relevance of collecting data for multiple directions. In general the empirical method was capable of estimating the user's location with high accuracy, obtaining a median error distance between 2 and 3 meters, and with its main drawback being the required effort for building the data set for each physical area of interest. Another issue is the requirement to remake the data collection phase whenever a base stations is moved or there are heavy changes in the environment.

The signal propagation model comes as an alternative to the empirical method for constructing the fingerprint. This method makes use of a propagation model for the signal to generate a set of theoretically-computed signal strength data, similar to the one physically collected. The performance of this method is correlated to the how well the used model is capable of correctly describe the signal. The system's chosen propagation model was Wall Attenuation Factor model (WAF) which takes into consideration obstacles between transmitter and receiver. This model provides a more reasonable way of obtaining data, since it doesn't require detailed and costly measurements. When compared to the empirical method, it was capable of achieving a mean error distance of 4.5 meters, that although it isn't as accurate it can be considerate as a solution when analysing its benefits.

Cricket

The Cricket system [25]was developed by the Massachusetts Institute of Technology (MIT) in 2005 and managed to tackle some of the problems existent in the previously mentioned systems. The system makes use of nodes, small hardware platforms, consisting of a RF transceiver, a microcontroller and hardware capable of generating and receiving ultrasonic signals. There are two types of nodes: beacons, which are fixed reference points attached to the ceiling or walls of the building, and receivers, called listeners, which are attached to the objects that need to be tracked. Each beacon periodically transmits a RF signal message containing beacon specific information, such as the beacon's unique ID, its coordinates and the physical space associated to the beacon. Whenever a RF signal is transmitted, an ultrasonic pulse, which doesn't contain any data, is also emitted thus enabling listeners to measure their distance to the beacons by using the time difference of arrival times of the RF and ultrasonic signals. Each listener utilises the RF signal's beacon information alongside the obtain distances to beacons to compute their space position and orientation.

When a beacon is deployed it doesn't know its exact position, only a human-readable string which describes its location. In order to compute the recently deployed beacon's position a listener is attached to a roaming device in order to collect distances from the beacons to itself. These distances are used to compute inter-beacon distances, which, when in high enough number, are capable of uniquely define how beacons are located in respect to each other. With this information it is then possible to obtain the beacon's coordinates.

The utilised method for computing distances doesn't require listeners to actively transmit messages which permits cricket to perform well independently to the number of users. This active-beacon passive-listener architecture makes it so that the position of the user isn't tracked by the system thus solving the user privacy that were present in the remaining projects.

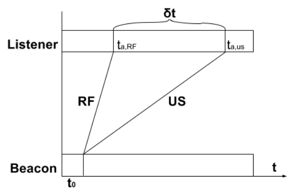

Figure 2.7: Cricket's TDoA representation

Distance measurement is computed through TDoA using both RF and US signals and it can be visualised in figure 2.7. Since the velocity of the RF signal is much higher than that of the US signal and when considering a direction, the US signal lags behind when compared to the other. As such, whenever a listener receives a RF signal, it measures the time is takes until the US signal arrives, denominated $\delta T. Withknowledgeofthespeedsofsoundandlight, thedistancebetweenbeaconandlistenercanbeobtainedfrom:$

$$\delta t = \frac{d}{v_{US}} - \frac{d}{v_{RF}}$$

This approach to distance computation is vulnerable to a certain amount of factors such as: Environmental factors since the velocity of sound depends on factors such as temperature, humidity and atmospheric pressure; Lack of LOS since in these scenarios there is no LOS between the beacon and the listeners, the US signal may reach the listener after it has reflected on a surface. Reflection and refraction cause the signal to travel a longer distance than the direct path; Errors in detecting US due to the threshold-based approach to detect the signal; TDoA associated errors, which are associated to errors from time measurement and errors from detecting the RF signal.

In terms of performance, Cricket was capable of a distance measurement accuracy of 4-5 cm within a 80^o cone from a given beacon, position accuracy of 10-12 cm and an orientation accuracy of 3^o - 5^o.

BLE systems

When looking at what's possible to achieve using the BLE technology there is the example of Apple's creation iBeacon [26] which was presented in 2013 with the purpose of implementing proximity sensing systems. The device is capable of playing on the broadcaster role and as such its objective is to send nearby compatible receivers certain information. Some examples of application are to track customers or trigger location-based actions on devices such as push notifications or checking in on social media, with practical cases such as the usage of iBeacons by McDonalds to offer special offers to their customers in their fast-food stores. An indoor location system utilising this technology was presented by Jingjing Yang et al [27], where these devices were used to indicate a patient of his whereabouts through the proximity sensing proprieties and this information was later transferred *over to a server in order to give clients a variety of different services, from patient counting, to nearby department's information and offer indoor guidance to the nearest available bed.*

When utilising BLE for indoor location the usual metric used to calculate distances is the RSSI. This metric within the context of bluetooth brings to surface several issues such as the fact that RSSI as a metric is very accurate only when the target is within a meter of the beacon, since the value decreases as the inverse of the square of the distance to the beacon . As such when developing solutions for indoor location that require system with high accuracy capable of tracking moving objects, the usage of RSSI can't be utilised without further work. Faragher et al [28] tackled one of the techniques used to improve BLE system's accuracy, fingerprinting, by verifying the effects caused by the device deployment density within the required location. This experiment also puts into evidence one of the downsides of the bluetooth technology being that its scalability is low, besides requiring higher density in order to increase accuracy, due to their low range any need to increase coverage leads to increased costs.

Zonith [29] introduced a bluetooth based location system with the objective of tracking the position of workers in dangerous environments. Any device registered in the zonith implemented network would be continuously tracked and accounted for in each of the system's functionalities such as, sounding an alarm whenever a lone worker doesn't move or respond within a time interval (Lone worker protection) or providing a quick an precise location of any worker that has requested for help. This system's installation requires planing of the best locations to place the beacons and number required of beacons in order to be able to provide enough courage and make sure the system provides the required quality.

2.4 Bluetooth Low Energy

Bluetooth is a wireless technology that was created in 1994 with the objective of replacing cables connecting fixed or portable devices. At this point in time Bluetooth Special Interest Group is in charge of developing and managing this technology characterised by its robustness, low energy consumption and low cost.

The BLE protocol was introduced with the Bluetooth Core Specification version 4 (also called Bluetooth Smart) circa 2010 alongside two other protocols. Out of the three, BLE stood out for its lower power consumption, lower complexity and lower cost, while allowing for device discovery, connection establishment and connection mechanisms. Due to its characteristics, the BLE protocol was utilised in various IoT applications.

2.4.1 BLE's Architecture

Bluetooth's Architecture is ever-changing and can become very complex rather quickly with the introduction of different types of protocols. When working with BLE it's important to understand the key components of its architecture because by doing it's possible to better analyse the role of each component and how they operate and depend on each other. There are two main groups of core *blocks, the Low Energy (LE) Controller and the LE Host, in 2.4.1.A and 2.4.1.B respectively, and most the most relevant of these components will now be looked at.*

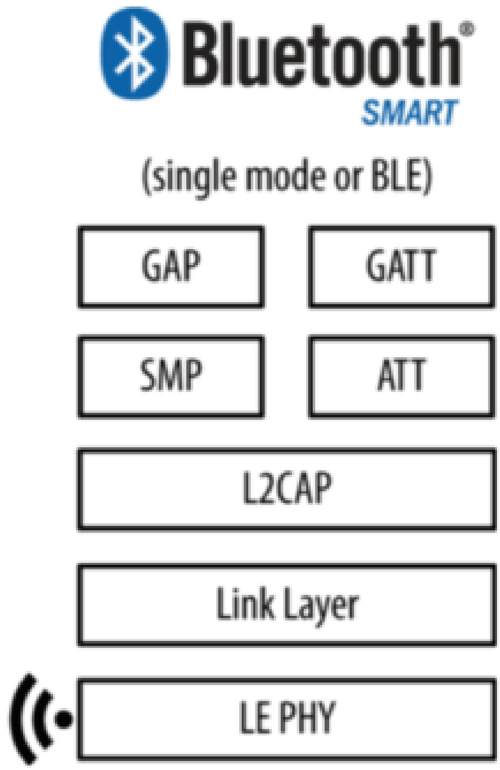

Figure 2.8: BLE architecture

2.4.1.A LE Controller Group

PHY Layer - *Architectural block responsible for all Bluetooth's communication channels on the 2,4GHz radio. Receiving and transmitting packets and supplying information crucial for controlling its timing and frequency through the baseband block.*

Link Layer - *Architectural block responsible for managing logical links between BLE devices. It can create and release connections, update connection parameters related to PHY links. It's responsible for the discovery and consequently connection procedure and also sending and receiving data.*

Device Manager - *Architectural block responsible for controlling the general behaviour of the Bluetooth device. This block is responsible for all operations that aren't directly related to data transportation. Some of its operations are: inquiring for the presence of nearby BLE devices; connecting to a BLE device; setting whether or not its local device is discoverable and/or connectable by the others; controlling device behaviour such as managing own's local name or stored keys.*

Baseband Resource Manager - *Architectural block responsible for all access to the radio medium, this means access to the PHY channels. It has two purposes, first to negotiate contracts with the entities that wish to use the medium and second to act as a scheduler on the same radio medium, granting the entities with said contracts, a time window in which they can utilise the medium. A contract is basically a commitment to deliver a certain Quality of Service (QoS) on the user application.*

Link Controller - *Architectural block responsible for the encoding and decoding of Bluetooth packets from the data payload and parameters related to the physical channel, logical transport and logical link. It also carries out the Link Layer protocol in conjunction with Baseband manager's scheduling function to communicate flow control and acknowledgement and retransmission request signals.*

2.4.1.B LE Host Group

Logical Link Control and Adaptation Protocol (L2CAP) - *Architectural block responsible of transmits packets to the Host Controller Interface (HCI) or directly to the Link Layer in host-less systems. It allows for higher-level protocol multiplexing, packet segmentation and reassembly, and the conveying of QoS information to higher layers.*

Channel Manager - *Architectural block responsible for creating, managing and closing L2CAP channels used in transport of service protocols and application data streams. The local Channel Manager makes use of the L2CAP protocol to communicate with a peer's Channel Manager and together create L2CAP channels and connect their endpoints to the appropriate entities.*

Security Manager Protocol (SMP) - *Architectural block responsible for implementing the Peer-to-Peer (P2P) protocol that operates over its own dedicated L2CAP channel and generates encryption keys and identity keys. This block is also in charge of storing those same keys and making them available to the controller. These keys are later used in the encryption or pairing procedures.*

Generic Access Profile (GAP) - *Architectural block responsible for working in conjunction with Generic Attribute (GATT) to define the base functionality of BLE devices. The available services in this profile are: BLE device discovery, connection modes, security, authentication, association models and service discovery. GAP defines four different roles to describe a device, allowing for the controllers to be optimised in function of the device's desired roles.* ***Broadcaster:*** *This role is optimised for transmitter-only applications. In a scenario in which a device supports this role it will make use of advertising in order to broadcast its data. The broadcaster role doesn't support for connections.*

Observer: *This role is optimised for receiver-only applications and it's complementary to the broadcaster role. It only receives broadcast data included in advertising packets and much like its counterpart, it doesn't support connections.*

Peripheral: *This role is optimised for devices that only want to support a single connection, allowing for a much less complex controller due to the fact that it only needs to support the slave role and not the master one.*

Central: *This role supports multiple connections and functions as the initiator for all of them. These connection are all made with Peripheral devices and its controller must support the master role in a connection and allow for more complex functions, in comparison to the remaining roles.*

Attribute Protocol (ATT) Protocol - *Architectural block responsible for implementing the P2P protocol between an attribute server and client. This client/server communication happens in a dedicated fixed L2CAP channel. A server can send through this channel responses, notifications and indications, while the client can send requests, commands and confirmations. This block allows the clients to read and write values of attributes on a peer device acting as a ATT server.*

GATT Profile - *Architectural block responsible for creating a framework for the ATT, in which it is represented the functionalities of an ATT server. This profile describes the hierarchy of services, characteristics and attributes existent in the server and provides an interface for discovering, reading, writing and indicating service characteristics and profiles. A more thorough description of profiles can be found in 2.4.2. GATT also defines two possible roles, which aren't directly tied to the GAP roles previously presented but can be specified by higher layer profiles.* ***Server:*** *A GATT server is responsible for storing data transported over the ATT and accepts ATT requests, commands and confirmations from a GATT client. It also sends responses to requests and, if implemented, send indication and notification asynchronously to a GATT client when specified events occur on the GATT server.*

Client: *A GATT client has all the functionalities presented in the GATT server description.*

2.4.2 BLE Profiles

Bluetooth profiles defines the required functionalities of each layer, from the PHY to the L2CAP layer, as well as the the vertical interactions between layers and P2P interactions between device and a specific layer. Since a profile also defines application behaviour and data formats, we can say that when two devices comply with all the requirements of a Bluetooth profile, application interoperability is achieved. Each Bluetooth profiles describes its requirements necessary for devices to create a connection, to find available services and connection information required for making application level connections.

The base profile that any Bluetooth system needs to include is the GAP, already presented in 2.4.1.B. From this point, any additional profile implemented will be a superset of GAP, where GATT is included. Among all that was already introduced about GATT in 2.4.1.B, it also specifies the profile hierarchy, or the structure in which profile data is exchanged. 2.9 shows the hierarchy in a Gatt-based profile, with the profile being the top level and services and characteristics below. The last two will now be presented individually:

Service: *A profile is composed by one or more services. A service is a collection of data and associated behaviours to accomplish a particular function or feature of a device or portions of a device. It can be either primary, which provides primary functionalities of a device, or secondary, providing auxiliary functionalities of a device and is referenced from at least one primary service. A service is composed of characteristics and/or references to other services.*

Characteristic: *A Characteristic is a value that is used in a service that has properties and configuration information that descrive how the value should be accessed as well as information on how to display the value. A characteristic is defined by its declaration, its properties, its value and may also be defined by its descriptor, which describes the value or permit configuration of the server relative to the value.*

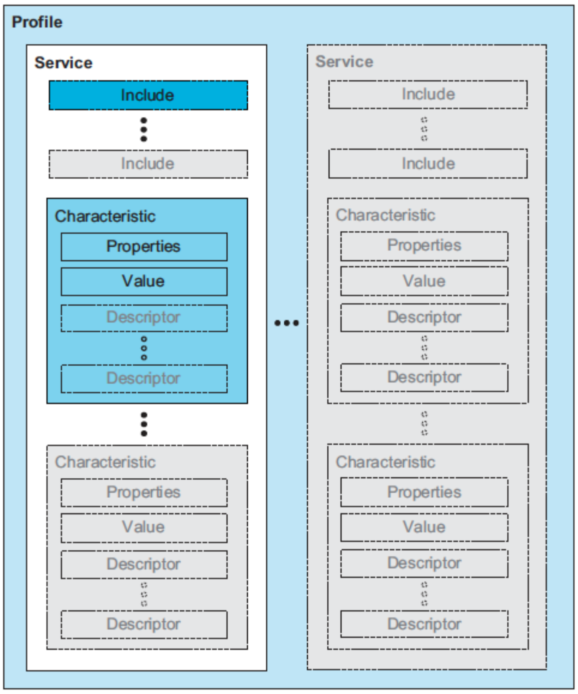

Figure 2.9: Gatt-based profile hierarchy

2.4.3 Communication Topology and Operation

The LE radio operates at the 2.4GHz band and employs a frequency hopping transceiver to combat interference and fading. LE also employs two multiple access schemes: Frequency Division Multiple Access (FDMA) used to separate the 40 available PHY channels, 37 of them are used as data channels and the remaining as advertising channels and Time Division Multiple Access (TDMA) in a polling scheme that is used when one device transmits a packet at a predetermined time and a corresponding device responds with a packet after a predetermined interval.

The PHY channels are sub-divided into time units known as events and these can be of two types according to which type of channel they belong, either advertising events or data events.

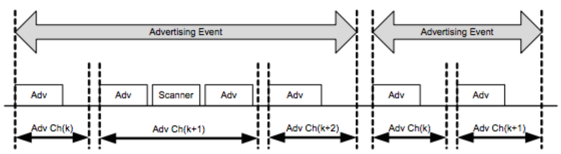

Figure 2.10: Advertising event

Advertising events: *There are three roles that can be used to describe a device in function of their utilisation of the channel:* ***advertisers****, are those that transmit advertising packets;* ***scanners*** *are devices that receive advertising packets without the intention of connecting with the advertising device;* ***initiators*** *are devices that listen for connectable advertising packets in order to later initiate a connection. Transmissions in the advertising channels occur in advertising events which always start with an advertiser sending a packet. Depending on the type of advertising packet, a scanner device may make a request to the advertiser which may be followed by a response from the advertiser, always* *on the same advertising PHY channel. The advertising PHY channel changes when the advertiser sends a new advertising packet. An advertising event can be terminated whenever the advertiser wants and when a new advertising event is created it will occur in the first advertising PHY channel. The whole process can be visualised in 2.10.*

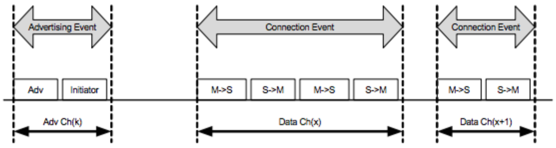

Figure 2.11: Connection event

Connection events: *When an advertiser is using a connectable advertising event an initiator may request a connection on the same PHY channel. If the advertiser accepts the connection request, the advertising event ends and a connection event starts in order to establish the connection. Once it's established the initiator takes the master role and the advertised, the slave role. These events are used to transmit data between each other and they always begin with a message from the master. During a connection event master and slave alternate send data packets on the same packet. The master is responsible for ending the end whenever he pleases and for the creation of new event channel hopping is required. The whole connection event can be visualised in 2.11.*

2.4.3.A LE Piconet Topology

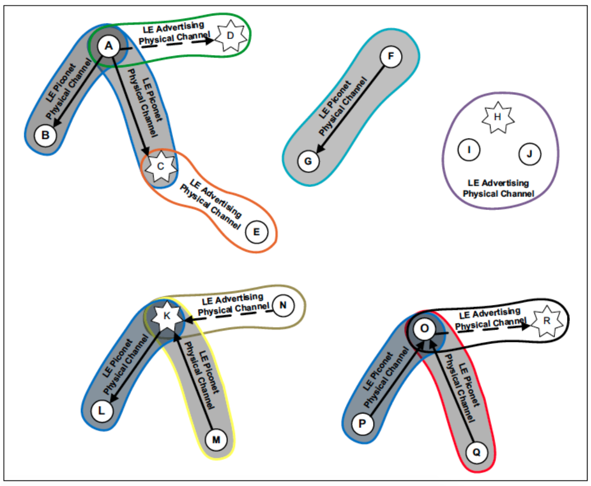

Figure 2.12: Examples of LE topology

As opposed to regular Bluetooth piconet, in LE, slaves can't share a PHY channel and as such each must have his own PHY channel to communicate with a master device. In order to best understand 2.12, solid arrows always point from master to slave, dashed arrows indicate a connection initiation where the arrow points form the initatior to the advertised using a connection event and devices that are advertising are indicated with a star. With these notes the different types of topologies can be analysed:

- *In piconet A, that which contains device A, there are multiple types of topologies such as , device A having connections with multiple slaves and initiating a new one with device D which was advertising. It is also worth noting that the device E is functioning as a scanner listening to the advertiser device C.*
- *In piconet F there is a simple master slave connection with device F as master and G as slave.*
- *In Group H there are more than two devices in a single PHY channel, such thing occurs since multiple devices can listen for advertisements on the same channel. In this case device H is functioning as an advertiser while I and J are scanners.*
- *In scatternet K there is an example where device K functions as master in the connection with device L and as a slave in the connection with device M, at the same time.*
- *In scatternet O there is an example where device O is functioning as a slave in both his connections with devices P and Q but it is still capable of forming a connection with R, where O will be the master.*

2.4.3.B Operational Procedures

The most common operational mode of a Bluetooth device is when he is connected and exchanging data with another Bluetooth device. Since Bluetooth is an ad-hoc wireless communications technology, i.e. decentralised type of wireless network, there are a number of operational procedures that enable piconets to be formed so that the subsequent communications can take place.

Device Filtering Procedure *Method used by controllers to reduce the number of devices requiring communication responses through the use of a "white list" located in the Link Layer that enumerates the devices that are allowed to communicate with the local device. This procedure allows the device reduce power consumption since it reduces the number of transmissions that it needs to make.*

Advertising Procedure *An advertiser utilises this procedure to perform unidirectional broadcasts to devices in the vicinity. The broadcast occurs without any need of connections and can be utilised to establish connections with nearby devices or to simple broadcast information to nearby scanner devices. This procedure includes the operations already described in advertising events in 2.4.3.*

Scanning Procedure *A scanner device utilises this procedure to listen to unidirectional broadcasts of user data sent by advertising devices. It is also capable of requesting additional user data by making a scan request as an answer on the same PHY channel of the first broadcast. This procedure can be utilised while the device is connected to other LE devices for as long as its connections requirements are maintained.*

Discovering Procedure *Bluetooth devices use the advertising procedure and scanning procedure to discover nearby devices, or to be discovered by devices in a given area, as such the discovery* *procedure is asymmetrical. A Bluetooth device that tries to find other devices in the vicinity can be called as a discovering device and will listen for devices advertising scannable advertising events. Devices that are available to be found and actively broadcast scannable advertising events are called discoverable devices.*

Connecting Procedure *The connecting procedure is asymmetrical as it requires one of the devices to be utilise the advertising procedure and the other one the scanning procedure. The advertising procedure has the capability of being targeted which allows only the chosen device to respond. The scanning procedure also has the capability of being target if the device discovers an advertising device and from there on out only listens for its advertisings. Upon receiving a connectable advertising event, it can initiate the connection by answering with a connection request.*

[Connected Mode] Once the Connecting procedure is over the devices are physically connected to each other within a piconet. While in connected mode there is the possibility of changing the connection's properties such as data packet's length and for the device to utilise advertising ,scanning or discovery procedures.

2.5 Critical evaluation

In this section one wants to review all the technologies that have been presented in this section but this time comment and evaluate them with a modern day's vision. It is of relevance to understand which technologies present concepts that can still be easily usable in the present and whether or not they can be adapted to function with state-of-art Smartphones.

Radio Frequency Identification (RFID) *In the current days isn't much of technology for indoor location systems. This is caused by multiple factors such as its incompatibility with smartphone, which by itself is already a critical factor for not being capable of being used in indoor systems other than the ones for research purposes. One recent system using RFID was presented by Han Zou et al. [30] which makes use RFID tags and sensors, a RFID reader and a location server. The general procedure for computing a location is that the tags emitted its ID which is caught by the sensors, the sensors make use of its external power supply to allow the creation of a continuous wireless connection with the reader. Once the reader receives the data he forwards it to the server where the location is obtained. This system introduces one of the issues of RFID which is the high cost of readers. This situation creates a big constraint on the architecture since making the mobile user the central piece of the architecture would require a RFID reader per person. As such nowadays RFID isn't a technology used for indoor location but instead for people or object tracking, since this approach only requires the person/object to have a unique tag.*

WLAN *is a technology that was made for positioning but since it contains Received Signal Strength Indicator (RSSI) information it is possible to use it with that purpose. One of its strongest points* *is its availability, as it's hugely wide spread around the world and it doesn't require any extra infrastructure, other than the already existing one, to function. As such nowadays this technology can be useful when attempting to create an indoor location system capable of being utilised by smartphones in any environment. This is only possible since pretty much every single smartphone is equipped with a WLAN antenna.*

WLAN RSSI-based indoor location systems can be of two types, trilateration or fingerprint. When imagining a scenario for a system implemented in multiple sites, the fingerprint technique raises questions which can be analysed by looking into the RADAR system.

Radar's architecture defines the mobile user as the broadcaster for the whole of its process, be it offline and online phases of the fingerprint method as described in (xXXXX).Despite the choice, P. Bahl et al,(cite radar) comment on their choice consequences, imagining that in a real situation, since the number of mobile users is vastly bigger than that of base stations, the inversion of the roles would be beneficial in order to decrease the complexity and the workload. Passing the broadcast role to the base stations while having the mobile users are listeners would make it so that for a certain floor the complexity would be constant, i.e. equal to the number of stations, instead of being unstable as the number of current mobile users. This change of architecture would allow for much more stable system, while requiring that the mobile users to perform an extra action in the form of a scan, a scan for capture of base station's broadcasts. Radar was design in a way that the collected information by the base stations were forwarded to a central computer, where they were processed in order to obtain a user's location. As such any existing user on the network was capable of being tracked but the information wasn't made available to the mobile user. Device deployment in this system isn't an issue as Wi-Fi is massive deployed technology present in most existent devices. At the time of development this system made use of computer with wi-fi available, as such no system specific devices were required at least for the online phase. Due to the choice of fingerprint as location method, additional measures concerning data collection are always required.

By analysing RADAR its possible to understand the constraints of the fingerprint technique. As such only the trilateration technology could be of use in a large scale environment. With the idea of keeping the smartphone as the central piece of the architecture, it would be on him to capture the RSSI signals from the nearby access points and forward that same information to their associated servers for the rest of the location procedure.

Due to the WLAN characteristics and its worldwide availability, it is often used in hybrid indoor location systems.

Infrared (IR) *In order to analyse the IR technology one can initiate by studying the badge system, which was described in section 2.3.*

The badge system's architecture is considerably different from the one proposed in this work as the role of the beacon(sensor receivers) and the smartphone (badge devices) are exchanged. This exchange in roles allows to reduce the energy cost on the mobile device since it isn't *up to it to communicate with the server and due to the design of the system the energetic balance between scanning and performing a signal broadcast for a tenth of a second each fifteen seconds isn't of relevance. Another aspect of this architecture is the fact that the collected data is sent to the central station, the only place where it will be available, making it only capable of tracking individual users and not providing the users with their location.Since the required building maps are already in the central station there is no need a maps provider. In terms of device distribution, this system makes use of system specific devices, which are already set up and inserted into the system and are distributed to anyone or anything that is to be tracked.*

Due to badge's age, it can't be relied on when making a judgement on the usability of IR in the present time. As such it is of relevance to look at recent works dependent on this technology such as the Epsilon project [31], which makes use of Light-emitting Diode (LED) and light sensors.

Epsilon makes use of LEDs and their capacity to both illuminate, the main reason for it's utilised and wide available il multiple indoor environments, and their capacity to communicate. By making use of the LED's ability to instantaneously change between on and off, it is possible to carry digital data in the visible light carrier through Pulse Width Modulation (PWM). In this system each of the used LEDs was self-contain, i.e. it knew its own location, which was insert into the data transmitted to the mobile user. The mobile user would capture the LED information through its light sensor, and consequently decode the received data from each of the available sources in order to make use of a trilateration system to obtain its position.

Epsilon presents a solution which is easy to use in today's world due to the availability of LED lighting in indoor environments, with the only requirement being the adaption of the existing infrastructure to the required by the system. In order for the system to work, it required the mobile user to carry a device with an incorporated light sensor, which is the case of pretty much any existent smartphone. Epsilon's architecture was created with the intention of having a "plug-and-play" kind of system, made possible through the self-contained LEDs and location calculation made on the smartphone. However in order to be used in a broader environment it could be adaptable to this work's proposed architecture.

Much like the authors already suggest in their work, instead of the self-contained LEDs, they could use a back-end service for mapping the IDs of each LED to their location, by relying on a network connection. The mentioned service would be the equivalent of the location server component on the proposed architecture, with the additional possibility of passing the location computation (which was implemented to occur on the smartphone) to the location service. Since no map component is mention on the work, there wouldn't be any conflict with the addition of the map server, which would rely on the already needed network connection.

Ultra-Wideband (UWB) *Is a technology that isn't very practical for indoor location in today's world. The main reason for it is the incompatibility with the existent modern day smartphones. Existent UWB system are dependent on system specific hardware which invalidates the possibility of* *having a wide scale indoor location systems.*

When analysing recent UWB system, the most common ones are tracking only systems. These systems are found useful in construction environments, where tracking crane's position is of relevance [32]. This position tracking is accomplished by setting up a network of UWB sensors on the construction site and placing UWB tags on the crane or parts of the crane, if the whole position and pose of the vehicle are of relevant, that is to be tracked. If additional objects were to be tracked, it would only be required to add tags to the object in question.

In terms of viability for indoor location, there are commercially available solutions such as the one presented by Decawave [33]. Decawave presents a UWB transceiver in the form of a hardware module. The proposed module makes use of Roundtrip Time of Flight (RToF) to obtain distance between itself and another module of the same kind. This transceiver can be used to implement indoor location systems based on UWB although it won't be compatible with existent smartphones.

Optical *As described in section 2.1.5, optical systems are systems which are dependent on camera as means to obtain input for indoor location. These kind of system are easily usable in today's world due to all the technological improvements of cameras and their integration into every single existent smartphone. Although it was described in section 2.1 as a single technology, nowadays smartphone cameras as used as input receivers in IR systems. One example is the already analysed system, Epsilon, where the camera is used as a mean to capture IR signals from LEDs.*

Other variants of camera-based systems make use of depth cameras with the intention of build dense 3D maps of indoor environments [34], which can be useful in robot navigation. Due to their high cost and incompatibility with modern day smartphone, these variants can't be used for large scale indoor location systems.

FM *This radio technology can be seen as an alternative to WLAN, due to their similarities. Much like WLAN, FM receivers are present in pretty much every single existent smartphone which removes the smartphone component from the list of possible constraints. FM as a technology for indoor location can be used, but often times is discarded in favour of other possibilities. When compared to WLAN, while it has some advantages such as lesser power consumption on smartphones, its bigger range and power, or even the fact that its less prone to interference from human presence or objects due to its bigger frequency band, when compared to WLAN already existent infrastructure and availability, all the positive sides become less meaningful.*

Sungro Yoon et al. [35], proposed an FM system capable of providing indoor location through a fingerprint method and the signals commercial FM radio stations. Since it's a fingerprint-based system, the whole process and its pro's and con's have already been heavily commented on. The big addition with this system is the utilisation of a publicly available signal ,i.e. existent commercial radio stations, which means that there is no need for extra infrastructure. When analysing the possibility of adapting this system onto the proposed generic architecture, i.e.

attempting to make use of this work in order to idealise a higher scale system, one can say that it is feasible. Since the smartphone functions as a receiver, with the radio towers, which include their information ,location and power, functioning as the "beacons", the missing components would be making the fingerprint database on a centralised server, with the same happening to the maps provider.

Zigbee *Is a technology that has been gaining traction due to its low power characteristics, which are very popular in IoT, but as of today hasn't been incorporated into smartphones. As such a smartphone reliant system using zigbee isn't possible only by itself, it would required the addition of a zigbee dongle to allow smartphones to communicate with other zigbee devices. With such restraints, zigbee hasn't been very developed in the indoor location field.*

The few existing zigbee system make use of the fingerprint method for data collection and location computation, such as the example provided in section 2.1.5. With the development of IoT it is possible that one day smartphone will be capable of communicating with other zigbee devices, allow for further development on indoor location.

US *In order to analyse US it is of relevance to review two systems, the bat and cricket systems presented on section 2.3, that make use of this technology and analyse how they could be adapted to todays reality and the generic smartphone centric architecture for an wide scale indoor location system.*

The bat system's architecture is very similar to the one deployed by the badge system, with the big difference being that its location is tracked upon request instead of being periodic. In energetic terms, it is also similar with the increased cost of having an additional operation, listening for central station's messages. Bat deployment is also manually done, with each person or object required to carry a system specific device. Each user's position is tracked and not provided to the user, while being made available through the maps provider extant within the central station.

The cricket system is completely different from the other remaining systems already presented, in terms of architecture. Cricket's Architecture is completely decentralised and the beacons and mobile users have the same roles as the proposed generic architecture of this work. Cricket's beacons broadcast periodically RF and US signals while the mobile user is in charge of listening for both of the signals. Data collection happens entirely on the mobile user's side, as explained on section 2.3, in the form of TDoA. Location computation is obtained directly on the cricket's listeners and this information is made available through this device's API. As such the mobile user's device can inquire the listeners about its position. This design , when compared to the the presented generic framework, reduces a communication step, the one between device and location server. This situation allows the user to keep its privacy intact as no one else has access to the its location. On the other hand, location computational work is passed onto the mobile user, which can make an impact on the performance depending on the algorithms complexity. Another issue is the fact the code deployed on mobile devices can cause issues if needed to *be update, creating a versioning problem that can be solved by having the required code in a centralised station. Cricket's system was created without providing a map based location although as stated by the authors (Add cite to cricket paper), with the deployment of a map server, as in the presented generic framework, by sending the calculated location to this map provider, a location system could be easily provided to the user.*

In order to look at US system's capabilities in today's world one can look into the work of Viacheslav F. et al [36]. Their work presented a location system based on the capability of producing US signals using a smartphone's microphone. The presented system made use of a smartphone as the central piece, which interacted with the system through a mobile application. Although it was a promising approach on indoor location, it falls under the limitations of the technology. Since US signals require an existing LOS between sensor and smartphone, the infrastructural requirements are higher than many of the remaining technologies.

Zonith's architecture was created solely for tracking of people and as such presents inverted roles for beacons and mobile users when compared to the generic framework. The system requires users that need to be tracked to manually insert their device's information, be it system specific or the user's personal device, onto the system. The carried devices should be always in advertising mode so that the existent listeners can capture their signal. This design although similar to the imposed on the mobile devices of the badge or bat systems, since its an always active feature should have a much bigger impact on the energy requirements. The beacon listeners forward their gathered data onto the central station, where all the data of the users to be tracked are kept and the system's functionalities are computed.

They have a indoor location feature for rescuing teams, showing a map with the route to the user in danger's location.

The ibeacon hospital system's architecture is very similar to the presented generic framework. There are beacons which broadcast signals containing location specific information, which are to be capture by nearby mobile user's devices. Upon receiving the beacon's information, they forward it into the central server which analyses the location and gives back to the user information based on it. The maps required for displaying the user's location were deployed on the user's application upon installation of the service. Upon receiving the user's location information back from the server, it is displayed on the local accessible maps. By removing the existence of a map provider server, the scalability of the system is drastically reduced. While it is acceptable for closed environment's service, i.e. app designed for a specific location such as an hospital, when making an indoor location system that is to be used in multiple places, a general exterior map provider server makes it so that a smartphone application doesn't require to have locally all the required maps.

3

Architecture

Contents

3.1 System Requirements

When proposing a generic architecture it is fundamental to define the requirements of any system that intents to implement it. These requirements can be of many different types, from energetic , to functional or scalability, all of which will now be mentioned. Any system capable of complying all the presented minimum requirements can make use of the architecture while being sure that their system will be able to properly function as part of a bigger system and with any other compliant systems.

Functional requirements *The whole architecture revolves around having a smartphone as the central point for communication. As such the existent functional requirements are all based either on technological requirements or compatibility with any smartphone. As such the architecture requires the utilisation of smartphone with network capability in order to be able establish communication between smartphone and location or maps server.*

Another functional requirement is the one concerning the communication between the beacon component, which provides the smartphone with information about its surroundings and take on many shapes and forms depending on the chosen technology, and the smartphone. This requirement limits the number of usable technologies around the existent sensors. The analysis on the communication compatibility with smartphones has been conducted on section 2.5.

Energetic Requirements *It isn't easy to define energetic requirements of an architecture as it is a very volutile parameter. One of the concerns when making use of smartphone as the central node of communication is the fact that the whole system is constraint on the energetic availability of the smartphone. As such it is of major importance to make sure that the energetic impact of the system when it is working is the smallest possible.*

The energetic impact of the system depends on multiple factors such as: Energetic capacity of the smartphone, whose values have been increasing over the years in order to support the higher energetic cost of applications; Cost of the communication between beacon and smartphone, which depends on the size of the messages and the technology; Cost of the communication between smartphone and servers, which depend on the network access available; Cost of the technology's scanning procedure; Cost of map download; Cost of displaying the maps on the smartphone application and finally the overall cost of the application utilisation.

When analysing the costs of each of the previously mentioned factors, the most variable factors are the costs relative to the technology scanning and communication between beacon and smartphone. These cost are dependent on the technology's specific sensor. The remaining communication cost are relatively stable and are independent on the chosen technology. These costs depend mostly on the size of the transmitted messages, which for the ones between smartphone and location server depends on the number of surrounding beacons and for the ones between smartphone and maps server depends on the size of the maps on the maps server.

The mentioned energetic costs are specific to the cost of one complete operation. The overall *cost of the system is dependant on the frequency of the operation. Other than the energy, the used frequency has an impact on the update rate at which the user is capable of knowing its positions. In order to reduce the energetic impact there are algorithms which allow for suspending the process whenever the mobile user is static, i.e. the last location request remains actual without need for update.*

Other that the technology specific costs, the energetic costs are highly dependant on the update frequency...

Interoperability requirements *The concept behind the proposal of a generic architecture framework is that besides multiple system, which use different technologies, being capable of functioning under the same architecture and interface, they also can work together seamlessly.*

In order to support interoperability, i.e. an indoor building attempting to implement multiple different systems, the smartphone needs to be able to identify the type of input data that it's sending to the location server, while the location server needs to be ready to obtain the user's location through the type of data received.

For the data processing, any two technologies that are compatible with smartphones can be used on the same system. In this system, the user needs to be able of obtain a position through any of the chosen technologies, be it passively or actively, in case that the data collection requires user interaction, and the collected data needs to be tagged and sent to the location server. The system's location server needs to be able to distinguish the two tags and its required to be capable of computing the mobile user's location through either of data types. Since the response from the location server is a location, it is independent of the data provided, which means that the rest of the system doesn't require any changes in the presence of multiple sources of location.

Environmental requisites *The environmental requisites are solely dependant on the system's technology. When studying the possibility of deploying a large scale system which has to be capable of functioning in many different indoor environments, the beacon technology needs to be able to be deployed in those same places.*

Another requirement is that the environment where the system is to be deployed needs to have network access, since it is a critical functional requirement. This caution is present in underground environments or other places where mobile network can't be relied upon, which puts the extra requirement of providing another source of network access, such as Wi-Fi.

3.2 Generic Architecture

The solution presented in this paper was made with the objective of creating a generic indoor location system capable of being implemented using any existent indoor system created. Another important concept is the provided capability of allowing multiple different technologies on the same

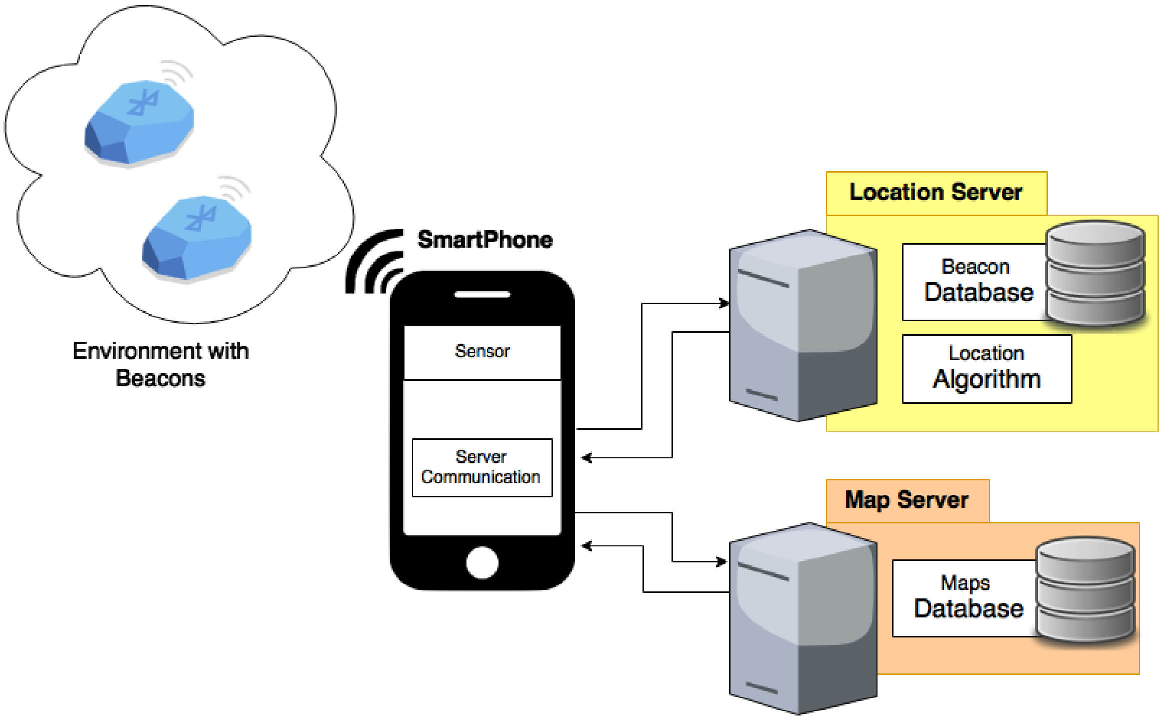

Figure 3.1: Generic System's Architecture

system to work seamlessly and request upon availability. The generic system's architecture is presented in figure 3.1 and it's divided in 4 parts: beacon, location server, map server and smartphone application.

The beacon represents any form of hardware responsible for providing fixed reference points which are fundamental in calculating a user's position. A beacon needs to be be composed of two structural blocks: The Unique ID, which stores any information crucial to identifying a beacon, and the Hardware specific software component, which contains all the necessary software to accomplish communication with a certain technology.

The location server is divided in three: the Communication block, which is responsible for creating, managing and terminating a connection with the mobile application; the location algorithm, architectural block responsible for applying a certain location algorithm to the data received from the application in conjunction with the server's device information in order to obtain a concrete location; and the beacon manager which functions as a database where all the beacon associated with the server are stored.

The map server represents the architectural block responsible for providing the maps associated to the location of user obtained through the location service on the application. As such it requires a communication block which needs to be capable of communication with the map service of the application and takes care of creating, managing and terminating connections, and a map manager which stores the existing maps that are to be transffered to the application.

The smartphone application is divided into three functional blocks: core application, location service and map service. The core application contains the core functionality of the application and is in *charge of communicating with the existing services. Communication with the location service allows for requesting the user's location which is then forwarded to the map service, in order to obtain the associated map. The location service is composed by four blocks: the API component through which it communicates with the core of the application; the tag reader which is the functional block responsible for reading a certain type of tags (beacons) and as such its structure will depend on the type of beacon utilised by the service; the tag decoder, functional block responsible of utilising the information obtained through the tag reader and process it in order to be forwarded to communication block; the communication block which takes care of the creating, managing and terminating connections with a location server.*

It might be relevant to analyse some types of indoor location system that could diverge from this architecture, such as camera or Quick Response (QR) code-based systems. These systems would still follow the proposed architecture except for the beacon component which would not be existent and the location service's tag reader block wouldn't need any sort of communication since it would be responsible of utilising the camera to capture either a photograph or reading a QR core.

Although figure 3.1 is representative of a system utilising a single type of technology, the presented solution is scalable, allowing for insertion of additional indoor location systems onto a single architecture. In this new architecture, the application's core would only communicate with the location manager and the latter would now be responsible of managing through all of the location services and request execution of whichever service would be more suited or available. The location manager would also be required to manage through the existent map services, which may or may not be in same number as the existent location services, and make sure that the data obtained from a certain location service is forwarded to the correct map service which must capable of processing it.

4

Implementation

Contents

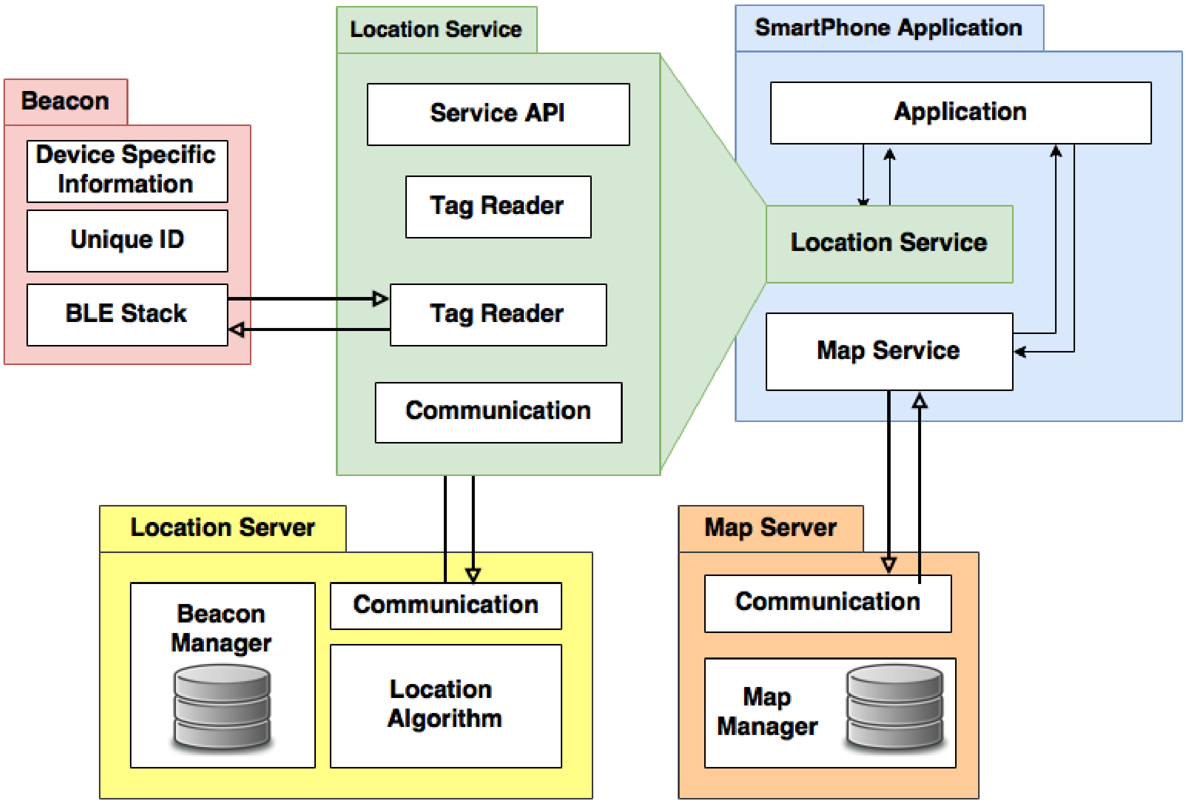

Figure 4.1: BLE system Architecture

The implementation presented in this paper was created by utilising the generic indoor location system presented in section 3 and applying it with bluetooth low energy. The system's architecture is presented in figure 4.1 and is divided three parts: the bluetooth low energy device, in section 4.1 a description of the used technologies and the changes made are present; the server, whose functionalities and stored information are described in section 4.2; and the smartphone application, whose process is described in section 4.3 alongside figures that show the functional prototype. For each of these parts an explanation will be given, containing a description of each of its components specific to the presented system alongside the requirements for each to work.

4.1 BLE beacons

The beacons that were utilised are Texas Instruments CC2650STK devices which can be visualised in figure 4.2. Alongside the device, which comes with a pre-installed bluetooth low energy program capable of giving information on each of its ten sensors through its predefined profiles, there is a texas smartphone application that can connect to a single device and read from its sensors. By using the texas Code Composer Studio (CSS), the pre-defined BLE profile existent on the device could be altered. The initial idea was to insert a new service into the already existing profile making use of the generic files provided by Texas. In order to implement the service, a characteristic containing the device's server IP and port was created and two random 128-bit UUID were generated. When using UUIDs, the Bluetooth SIG defined several UUID, each associated with a certain service,

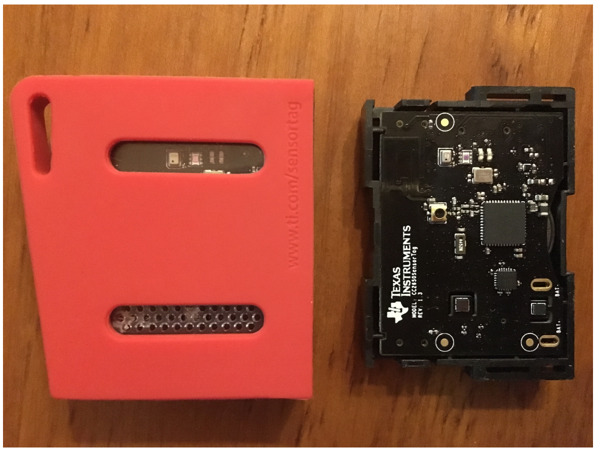

Figure 4.2: TI cc2650stk sensortag

such as heart rate or glucose services [37]. This situation makes it so that whenever someone intents to implements a new service he has to generate a random 128-bit UUID for his service and another one for each of required characteristics. Despite the efforts made, it wasn't possible to alter the existent profile by adding the new service neither by simply attempting to alter it by removing existent services. Due to the low amount of existent information on the technology an alternative was created. The solution found was to store the information into an already functioning service's characteristics as one was capable of altering those kind of parameters. The characteristics available to be used were only the ones from the device information service, a service defined by the bluetooth sig, since the remaining services on the BLE device were meant for reading values of from sensors. The chosen characteristic was the Manufacturer's name due to its relevance and the fact that its UUID was known, while the remaining's weren't.

4.2 Server

The web server was implement in Python 3.5 programming language. The program implements a tcp server capable of receiving multiple request at the same time. Each request starts with information sent from an application which include an undefined amount of pairs of MAC address and associated RSSI value, each corresponding to a BLE device that the same application found and connected. Afterwards the list of pairs is filtered in order to remove any existent devices that are not present in the server's database of devices. Once the list of pairs is composed only devices belonging to the server, the locating algorithm is deployed, in this case a CoO algorithm, which assumes that the location of the device is equal to the location of the closest device. As such the highest RSSI value is found, a new message is composed which includes the device's information on the database and consequently sent back to the user.

Each server has a database that includes only BLE devices. An entry (description of a device) in this database is composed by the device's mac address, its longitude and latitude and its building, floor and room name. In addition to the database, a server when initiated can store additional location info such as the server's street, number, zip-code , city and country, allowing this information to be

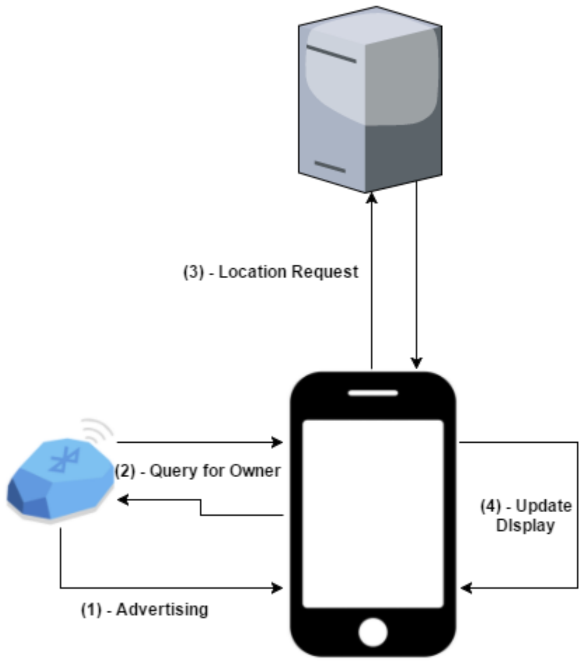

Figure 4.3: Mock Location Provider Workflow

transmitted to the client in order to offer an additional level of location description to the user. The whole location specific information can be visualised in figure 4.5.

4.3 Application

The Smartphone application was developed for Android using the Android Studio IDE. The Application is divided in two primary functional blocks, the Mock location Provider and the Google Maps Integrated Display, as can be visualised in figure 4.1.

The Mock Location Provider is implemented as if it was a Location provider, such as GPS. The application functions works as a listener to a Location provider, in this case it listens to the Mock Provider that was implemented. By implementing the whole process of obtaining a location inside a service (the mock provider) , a new level of abstraction is added to the application. As such, whenever the application is signalled to obtain the user's current location, a request is made to the associated location provider and the application only need to listen for the answer that eventually arrives.

The Mock Location Provider incorporates the first three steps present in figure 4.3, which will now be explored individually. The first step indicates the gathering of information of the surroundings of the user's device. When a request is made to the provider, a scan for nearby bluetooth low energy devices is made which will put the smartphone in a state of listening for incoming BLE advertisement packets for half a second (NEED TO VERIFY VALUE AND JUSTIFY, THERE WAS A PAPER ON THIS TODO). During this scanning period, each time a device is found, the advertisement is registered in a list, which have a duplication prevention mechanism implemented. Once the period is over, the provider has available a list of all the BLE devices within range.

The second step involves taking the created list of devices, obtain a server address and forward *the same list to it. Once the first step is completed, the provider will analyse each entry at a time. For each device the provider will attempt to respond to the caught advertisement packet, resulting in a created connection. Once the connection is created the provider asks for the available services of the paired device. Upon receiving an answer, the list of services is swoop while looking for the service with the wanted UUID. If the device doesn't have the UUID that the provider is looking for, it can assume that the paired BLE is not a beacon of our system, as such the connection is terminated. When the provider identifies that the device has the system's UUID, it requests the device to provide the service's existent characteristics. The provider will receive a list composed of the service's characteristics and it will search in it for the system's characteristics UUID, the one which contains the device's server's address. This search has the objective of confirming that the service existent in this device is indeed the one that was implemented for the system and not a device with another service that happened to have the same UUID. For any service outside those that are documented in the Bluetooth Special Interest Group (SIG), who have a specific UUID attached to them, the UUID is generated randomly and as such there is a small chance of collision. Once the wanted characteristic is found, the provider requests the device to read its value and stores the received value in a list. This list will contain the servers of the devices that were found, and for each address there will be a list corresponding to each device , and their corresponding rssi values, from the same owner. In order to quicken the previously described process, the provider keeps in cache the most recent contacted devices. Before attempting a connection, the provider confirms that the device isn't found in cache and when finishing a process, the associated device is inserted into the cache.*

When every device has been contacted, a voting system is actioned which will decide from the list of servers which one it will send the collected information to. The voting system uses an exponential function in order to attribute a weight to each server.

The voting system was implemented with the objective providing a thin security layer by allowing multiple devices of the same server to overcome a single attacker's device which happened to be close to the user. After obtaining each server's values, the one with the highest value is chosen and sent the list with all the devices.

The Third step involves a simple client/server tcp interaction. The application starts off by formulating the message that it will later on send to the server, this message includes all pairs of device mac address and its associated rssi value captured by the application on the first step. Once the message is computed, the application attempts to create a connection with the server at the chosen address at the end of step two. With the connection established, the message is forwarded to the server and the application is put onto blocked state where it awaits for an answer. Upon arrival, the answer received is checked for valid location, its information is process and the connection is terminated. The information contained inside the received message, which was described in section 4.2, is then processed into the adequate class capable of storing a geographic location and the same is broadcasted from the mock location provider to its listener.

One of the current limitations of the android API that deals with BLE is that the interface on the smartphone that is used to connect with a device has a fixed timeout time.

The Google Maps Integrated display is implemented using the Google Maps Android API. By using Google Maps it was possible to alleviate the weight on application since there wasn't need implement file transfer of indoor building's maps from each dedicated server to each request, which alleviated the servers as well since there was no need to store its associated building's maps on it. Managing the maps was something that was as well fortunately unnecessary and as such all these features were provided by google maps service. By making this development choice, the system as whole became closer to the desired generic approach while making possible for seamless transition between indoor/outdoor maps. The only imposed restriction is related to the addiction of new indoor maps onto the google maps, which is possible and well documented but dependent on a third party.

The Fourth step is called when the application receives a proper location from the request made onto the location provider. With the device's location known, a marker is placed on the map with the obtain coordinates (longitude, latitude), the camera is moved in order to be centralised on the position and fully displaying the indoor level map, and the menu visible on figure 4.5 is updated with the information that is bundled with the received location. In order to show the correct level on a multi level building, the "floor" information present in the menu is utilised. The API allows for obtaining a list of existent levels on which the maps' camera is focused and as such it's possible to find out to which level the provided location belongs and make so that the application shows it.

The pop-up menu was implemented to demonstrate the capacity of providing additional information associated with each location, be it geo-location taxonomy as it is currently implemented or possibly a description of the located room, an hyperlink of some sort or any other type of data that someone implemented this system would like to provide to its users.

The final state of the implemented system can be visualised in figure 4.4 and figure 4.5. The first displays the case of obtaining a location, where the marker has been placed and the camera zoomed

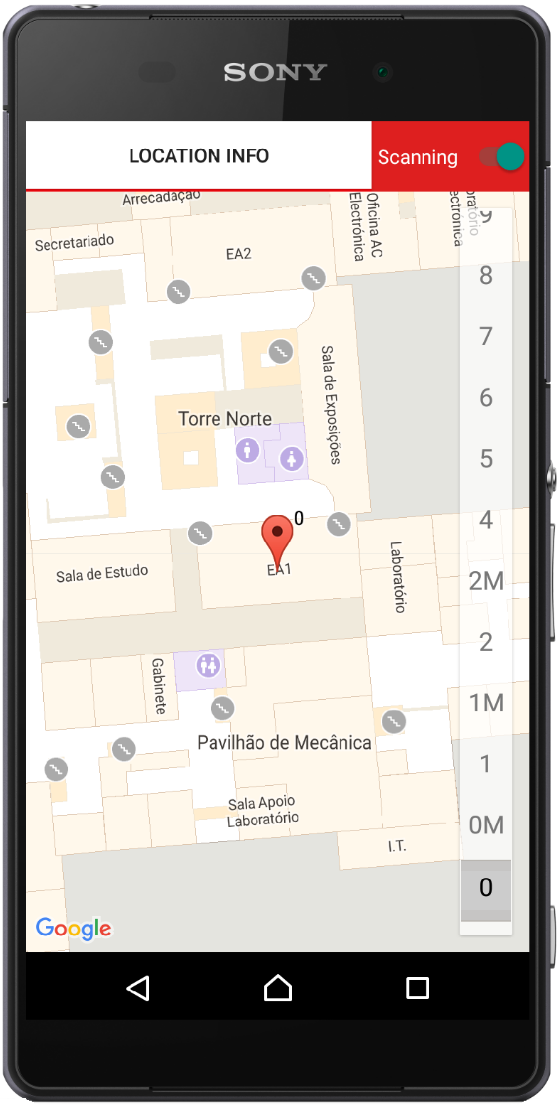

Figure 4.4: Application screen showing a focused location on a room

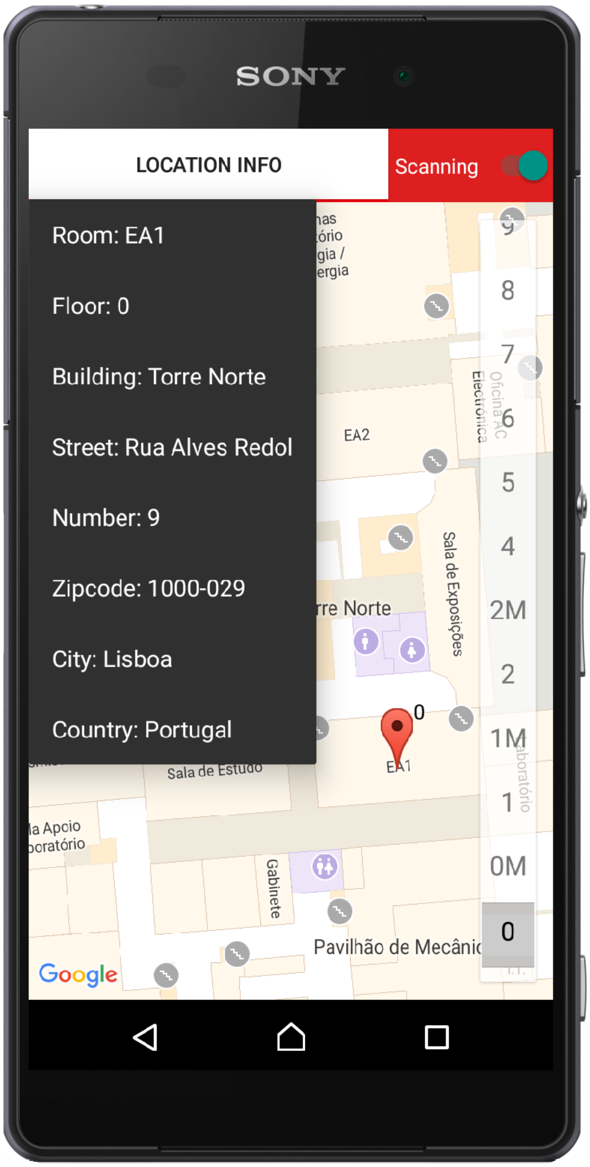

Figure 4.5: Application screen showing additional information of location

5

Conclusions and Future Work

Bibliography

[1] *Y. C. L. LIONEL M. NI, YUNHAO LIU and A. P. PATIL, "Landmarc: Indoor location sensing using active rfid," 2004.*

[2] *Y. Y. M. G. L. M. N. Kaishun Wu, Jiang Xiao, "Fila: Fine-grained indoor localization,"* IEEE 2012 INFOCOM*, 2012.*

[3] *S. G. Pete Steggles, "The ubisense smart space platform."*

[4] *[Online]. Available: http://cosdeo.teco.edu/2013/images/AlyTeaser.jpg*

[5] *[Online]. Available: http://www.cl.cam.ac.uk/research/dtg/attarchive/thebadge.html*

[6] *[Online]. Available: http://www.cl.cam.ac.uk/research/dtg/attarchive/bat/flatBatInside.jpg*

[7] *H. Koyuncu and S. H. Yang, "A survey of indoor positioning and object locating systems."*

[8] *R. N. Zahid Farid and M. Ismail, "Recent advances in wireless indoor localization techniques and system."*

[9] *H. Liu, "Survey of wireless indoor positioning techniques and systems."*

[10] *Y. Y. Jiang Xiao, Zimu Zhou and L. M. Ni, "A survey on wireless indoor localization from the device perspective."*

[11] *R. Mautz, "Indoor positioning technologies," Master's thesis, ETH Zurich, February 2012.*

[12] *K. A. Nuaimi and H. Kamel, "A survey of indoor positioning systems and algorithms,"* Innovations in Information Technology (IIT)*, 2011.*

[13] *G. B. Jeffrey Hightower and R. Want, "Spoton: An indoor 3d location sensing technology based on rf signal strength," 2000.*

[14] *A. G. D. Vahideh Moghtadaiee and S. Lim, "Indoor localization using fm radio signals: A fingerprinting approach," 2011.*

[15] *J.-M. L.-G. Janire Larranaga, Leire Muguira and J.-I. Vazquez, "An environment adaptive zigbee-based indoor positioning algorithm," 2010.*

[16] *[Online]. Available: http://www.versustech.com/rtls-technology/*

[17] *J. Xiong and K. Jamieson, "Arraytrack: A fine-grained indoor location system," 2013.*

[18] *M. H. Carl Fischer, Kavitha Muthukrishnan and H. Gellersen, "Ultrasound-aided pedestrian dead reckoning for indoor navigation," 2008.*

[19] *[Online]. Available: http://www.cl.cam.ac.uk/research/dtg/attarchive/ab.html*

[20] *V. F. Roy Want, Andy Hopper and J. Gibbons, "The active badge location system,"* Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 59–68, August 1992.*

[21] *[Online]. Available: http://www.cl.cam.ac.uk/research/dtg/attarchive/bat/*

[22] *P. S. A. W. Andy Harter, Andy Hopper and P. Webster, "The anatomy of a context-aware application," 199.*

[23] *S. H. J. N. P. S. A. W. A. H. Mike Addlesee, Rupert Curwen, "Implementing a sentient computing system,"* IEEE Computer Magazine*, vol. 34, no. 8, pp. 50–56, August 2001.*

[24] *[Online]. Available: https://www.microsoft.com/en-us/research/project/radar/*

[25] *N. B. Priyantha, "The cricket indoor location system," Ph.D. dissertation, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, June 2005.*

[26] *[Online]. Available: http://www.ibeacon.com/what-is-ibeacon-a-guide-to-beacons/*

[27] *Z. W. Jingjing Yang and X. Zhang, "An ibeacon-based indoor positioning systems for hospitals,"* International Journal of Smart Home*, vol. 9, no. 7, 2015.*

[28] *R. Faragher and R. Harle, "An analysis of the accuracy of bluetooth low energy for indoor positioning applications."*

[29] *[Online]. Available: http://media.teldio.com/pdfs/Teldio_Indoor%20Positioning%20White%20Paper_v2.1a.pdf*

[30] *Z. Han, "An rfid indoor positioning system by using weighted path loss and extreme learning machine,"* IEEE International Conference on Cyber-Physical Systems, Networks and Applications*, 2013.*

[31] *C. P. G. S. F. Z. Liqun Li, Pan Hu, "Epsilon: A visible light based positioning system."*

[32] *M. C. Zhang, A. Hammad and S. Rodriguez, "Crane pose estimation using uwb real-time location system,"* American Society of Civil Engineers.*, 2012.*

[33] *B. K. Y.-S. K. P. P. Bradford Campbell, Prabal Dutta, "Decawave: Exploring state of the art commercial localization,"* Microsoft Indoor Localization Competition*, 2015.*

[34] *E. H. X. R. Peter Henry, Michael Krainin and D. Fox, "Rgb-d mapping: Using depth cameras for dense 3d modeling of indoor environments."*

[35] *K. L. Sungro Yoon and I. Rhee, "Fm-based indoor localization via automatic fingerprint db construction and matching,"* MobiSys'13*, June 2013.*

[36] *C. C. Viacheslav Filonenko and J. D. Carswell, "Indoor positioning for smartphones using asynchronous ultrasound trilateration,"* ISPRS Int. J. Geo-Inf*, vol. 2, pp. 598–620, 2013.*

[37] *[Online]. Available: https:// www.bluetooth.com/ specifications/ gatt/ services*

A

Title of AppendixA