FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Monitoring a mobile ticketing system based on NFC and BLE beacons

Miguel Botelho

Mestrado Integrado em Engenharia Informática e Computação

Supervisor: Teresa Galvão Dias

Second Supervisor: Marta Campos Ferreira

June 27, 2018

Monitoring a mobile ticketing system based on NFC and BLE beacons

Miguel Botelho

Mestrado Integrado em Engenharia Informática e Computação

June 27, 2018

Abstract

Mobile ticketing in public transportation has substantially replaced the old ticket card and its affiliates. This way of interacting with ticketing is not something new and it came to reduce queues and increase commodity for its users. However, as technology rises, there is the need to reduce even further the complexity that is the current public transportation state, which is the biggest problem to its users. It is required to memorize different areas of the city, know the interchange stations locations and the complete schedule for a specific transportation vehicle and know the ins and outs of the ticketing and payment system, so it can be used properly.

Public transportation should be as simple to use as it can be. The end user does not need to understand the system to use it, and could be abstracted of all the complexity that it entails. It could be as simple as grabbing a smart phone, click on a button to start a trip and forget about it entirely, so that public transportation is not a burden anymore.

Given this context, the fact that technology is rising as fast as ever and the public's acceptance of mobile payment solutions, a solution was studied that embodies all of this. Even though solutions already exist, such as the use of NFC (Near Field Communication), BLE (Bluetooth Low Energy) beacons and even QR (Quick Response) Codes, most of them do not focus on simplifying the public transportation system, but rather replacing the old ticketing system only. Through a Check-In/Be-Out system, auxiliated by BLE beacons and NFC technology, the ultimate goal of public transportation should be achieved: no need for the end user to understand the system.

However, implementing an entirely new system on top of an existing one can be prone to flaws. Rather than try and make it flawless, accepting the flaws and solve them as time passes by may be a better solution. To achieve this, a real-time monitoring system was setup on top of the mobile one. The focus is to collect information from different sources and try and gather all kinds of data, so it can be displayed and observed. By way of this observation, errors can be cross checked and identified quicker than just by tackling one problem at a time. There is already information that backs up theories, such as the fact that beacons may be misplaced and not being optimized to each station.

The developed work resulted as well in the writing of a scientific paper, validated and accepted to the 2nd International Conference on Intelligent Traffic and Transportation (ICITT 2018).

Resumo

A emissão de bilhetes móveis nos transportes públicos substituiu substancialmente o cartão antigo, os smart cards e os seus afiliados. Essa forma de interagir com a emissão de bilhetes não é algo novo e veio reduzir as filas e aumentar a comodidade dos seus utilizadores. No entanto, à medida que a tecnologia evolui, existe uma necessidade atual de reduzir ainda mais a complexidade que é o atual estado do transporte público, que é o maior problema para os seus utilizadores. Do ponto de vista do utilizador, há a necessidade de memorizar diferentes áreas da cidade, conhecer os locais de transbordo e o horário completo para um veículo de transporte específico, conhecer os prós e contras do sistema de bilhética e pagamento, para que possa ser usado corretamente .

O transporte público deve ser tão simples de usar quanto possível. O utilizador final não precisa de entender o sistema para usá-lo, e pode ser abstraído de toda a complexidade que vem com ele. Poderia ser tão simples como pegar num smartphone, clicar num botão para iniciar uma viagem e esquecê-lo inteiramente, para que o transporte público deixe de ser visto como um fardo.

Dado esse contexto, o facto de que a tecnologia está a evoluir rapidamente e a aceitação do público às soluções de pagamento móvel, será estudada uma solução que incorpora tudo isso. Mesmo que as soluções já existam, como o uso de NFC (Near Field Communication), BLE (Bluetooth Low Energy) e até códigos QR (Quick Response), a maioria deles não se concentra em simplificar o sistema de transporte público, mas sim substituir o sistema antigo de emissão de bilhetes apenas. Através de um sistema de check-in / be-out, auxiliado por diferentes tecnologias disponíveis, o objetivo final do transporte público deve ser alcançado: não existir a necessidade do utilizador final entender o sistema. O objetivo final é estudar todas essas novas tecnologias e emergentes, relacioná-las com o maior problema de transporte público e tentar explorar todos os caminhos, em conjunto com um sistema de pagamento móvel, para que o melhor dos dois mundos possa ser alcançado: simplificando o transporte público e alterando a emissão da bilhética atual para uma experiência mais agradável.

Acknowledgements

I would like to use this page to thank all the people that made possible for me to complete this dissertation. First of all, I would like to thank my parents for the effort it took to motivate me to pursue my different goals throughout my master's degree, knowing perfectly well that without that motivation and obligation, I would not have wrote this dissertation. Second, I would like to thank my supervisor, Teresa Galvão Dias, and my second supervisor, Marta Campos Ferreira, for making me work hard when I did not want to and to let me rest whenever I needed to. I also know perfectly well that this thesis would not have been written without the constant support of both.
Furthermore, I would like to thank my girlfriend for putting my master's degree above her obligations and for that, I know I will never be able to repay her. I would also like to thank my many friends that, one way or another, helped shape this project but with a special mention to Luís Duarte, that gave his input with his own work and to Gustavo Silva, which decided not to delete the full contents of the dissertation in Overleaf, that would certainly pose me larger challenges to deliver my work on time.
Last, but not least, I would like to thank TIP, Card4B, OPT and Linha Andante for all the information shared and their invaluable input that allowed to correct and fix mistakes that arose during the development of the solution.

Miguel Botelho

"If you cannot do great things, do small things in a great way."

Napoleon Hill

Contents

List of Figures

LIST OF FIGURES

List of Tables

LIST OF TABLES

Abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
ATM	Automated Teller Machine
BLE	Bluetooth Low Energy
CCB	Componente Central de Bilhética
CP	Comboios de Portugal
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSS	Cascade Style Sheets
DBA	Database Administrator
DMZ	Demilitarized Zone
DoS	Denial Of Service
DST	Digital Signature Transponder
ER	Entity Relationship
ES	EcmaScript
ETG	Empresa de Transportes Gondomarense
FEUP	Faculdade de Engenharia da Universidade do Porto
GIS	Geographic Information System
GPRS	General Packet Radio Service
GPS	Global Positioning System
HF	High Frequency
HTML	HyperText Markup Language
ID	IDentification
IE	Internet Explorer
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
JS	JavaScript
LF	Low Frequency
JSON	JavaScript Object Notation
LTK	Long Term Key
MAC	Media Access Control
MAP	Metropolitan Area of Porto
MBTA	Massachusetts Bay Transportation Authority
MGC	Moreira Gomes da Costa
MMI	Man-Machine-Interface
MP	Metro do Porto
NFC	Near Field Communication
NJ Transit	New Jersey Transit

NXWM	National Express West Midlands
PaaS	Platform as a Service
PBV	Pagamento de Baixo Valor
PIN	Personal Identification Number
QR Code	Quick Response Code
RFID	Radio Frequency IDentification
SaaS	Software as a Service
SE	Secure Element
SHF	Super High Frequency
SIBS	Sociedade Interbancária de Serviços
SIG	Bluetooth Special Interest Group
SPA	Single Page Application
SQL	Structured Query Language
SSID	Service Set IDentifier
STCP	Sociedade de Transportes Coletivos do Porto
STK	Small Term Key
TIP	Transportes Intermodais do Porto
TK	Temporary Key
UHF	Ultra High Frequency
UI	User Interface
USA	United States of America
UUID	Universal Unique IDentifier
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WWW	World Wide Web

Chapter 1

Introduction

1.1 Context

The mobile ticketing concept steadily grows as time goes by. There are now companies mass producing solutions in this area (Masabi and Cubic are strong examples) so the smart card can be dropped in favor of the ever more present smartphone, as 88% of the population in South Korea already have one, for example. Israel is behind it with 74%, quickly followed by the USA with 72%. On developing countries, the smartphone is not quite a reality yet, as India stands with 17% and Ethiopia and Uganda with a mere 4%. [Bae16]
As for the smart card, a paper or plastic card with usually a RFID chip embedded, it is used in the majority of public transportation systems, being that the main part of its implementation went from 2007 to 2011. [Sma16] It saves important time on the validation process (as it only requires that the customer presses the card against a validator) and is able to be used multiple times, saving also money and resources on paper. It also provides a level of automation as the customer buys his own tickets by interacting with a machine, significantly reducing queues by eliminating human processing. From this modernization, logs of travels done by different people can be stored, opening the doors to the extraction of knowledge and customization of the public transportation system to each customer.
But the smart cards also brought new problems and did not solve some of the old ones. There are inherent flaws, such as the need to pre-plan and pre-purchase a ticket, when considering a Check-Out system. Smart cards can be easily damaged, hacked, cloned and require that the user travels to a ticketing machine either to buy the card or to buy a ticket, which can be a hassle, as the machines still take a significant amount of time to process the purchase of the ticket. Therefore, queues can also arise from this. The mobile ticketing concept could, potentially, eliminate some of these problems as the user, for example, could buy a ticket anywhere by simply using his smartphone. It can be integrated with other external services that customers usually consult in other places, such as schedules, routes in which the public transport in question travels, real time information or

an overview map of the metropolitan area. By integrating all these different services in the same place, the customer's action is being facilitated and the public transportation system can become more simple to use and understand.

1.2 Motivation

Even though mobile ticketing comes to solve many issues, its implementation also poses new problems and constraints. Smartphones are not as well established around the world, as seen in the section 1.1. Furthermore, smart cards gained a quick adoption due to ease of use and some technologies that are prominent in the mobile ticketing concept are not optimal and others are not 100% reliable, such as BLE and the NFC which are wireless technologies. These techonologies and others will be analyzed in section 2. The combination of all these factors may lead to difficulties in creating and maintaining a mobile ticketing system, either due to inefficiency or to problems in customer adoption.
In Porto, the future mobile ticketing solution is in the final testing phase and some problems still occur frequently, either due to the limitation of the technologies used or other undetected issues. In order to emphasize possible causes and discover unknown problems, this mobile ticketing solution needs a tool to analyze and prevent errors from occurring, to help with customer adoption and its own reliability.

1.3 Goals

BLE is somewhat of a new technology, and its implementation in mobile ticketing systems by way of beacons is quite scarce. NFC is already established but the conjunction of the two technologies is an innovative solution. By monitoring the Anda system and analyzing its flaws, it can be deduced if there is a failure customer-side or at the system side. It can exist incompatibility between devices, technologies, and many other aspects. The goal is to provide a working dashboard that analyzes and aggregates different kind of data based in logs of the mobile application, the system, its communication and in server-side logs as well. By being able to filter data by different search parameters and combine it, the system can acquire a significant level of automation when it comes to the search of the cause of different type of errors. It can save precious time and resources by having all different type of information in one place which becomes manageable.

1.4 Report Structure

In addition to the introductory chapter, where it is explained the context, goals and motivation, this report contains 4 additional chapters. Chapter 2 goes into detail on the state of the art and literature review on mobile ticketing, existing technologies and different approaches throughout the world. There is also a section dedicated presenting the current Porto public transportation landscape, its current solution (Andante) and the future (Anda). Subsequently, Chapter 3 details and explains some problems the future solution in Porto still contains, its overview and summarizes its methods and inner workings. Moreover, in chapter 4 it is exposed an overview of the solution, its idealization, its flaws and a qualitative evaluation, as well as technological testing. Chapter 5 focuses on the results obtained throughout the development of the dashboard and the manual analysis to all types of information. Finally, closing the document, Chapter 6 summarizes the work done until now, what can be concluded by it, as well as the expectations for the future.

Chapter 2

State of The Art

2.1 Technologies used in mobile ticketing

In the context of mobile ticketing, NFC is mainly used for checking in or checking out from a public transportation service. BLE is an emerging technology that can be revolutionary for Be-In/Be-Out types of public transport, as it can accompany and estimate customer's travels. RFID is an older technology that was hotly debated around 2005. [Vio03]

2.1.1 BLE

BLE, Bluetooth Low Energy, is a wireless communication technology for short-range technology operating in the unlicensed 2.4 GHz band, up to one hundred meters. It operates on the same frequency as Classic Bluetooth but differs in the channels used, since BLE divides the 2.4 GHz spectrum into 40 channels, 37 of them are used for connections and the remaining 3 to advertise (broadcast device information and establish communication). This division allows BLE to contain almost no interference from nearly every wireless communication technology. On the connection itself, a BLE connection does not communicate only on one channel, as it hops through various channels (the hop increment) and only sends one packet on one channel. If both the sender and receiver send empty data packets (no data involved and the CRC Init), then they both jump to another channel. Since most smartphones contain bluetooth technology, BLE is rapidly gaining momentum and the Bluetooth Special Interest Group (SIG) predicts that by 2018 over 90 percent of smartphones will support BLE [Jan15]. It is also important to mention that Apple has its own implementation of BLE, called iBeacon.

BLE works by way of a beacon, a small device powered by a battery, that emits a BLE signal. Then, a device within 100 meters can capture the signal and read the information embedded in it. It is not backwards-compatible with the Bluetooth protocol before the version 4 and it has different uses when compared with "Classic" Bluetooth [GOP12]. BLE is often used to transfer, periodically, small amounts of data. Beyond data, it is also useful to figure out where the device is. Not the location of it, but the proximity to the beacon in question, which saves a great amount of energy by not using other technologies such as 802.11 and Global Positioning System (GPS). Bluetooth devices are divided in two implementation modes [Mar18]

- Single Mode: It is only compatible with BLE and it is mainly used by lower power consumption and small size devices.
- Dual Mode: It is compatible with both BLE and "Classic" Bluetooth and it is mainly used by mobile phones and computers.

2.1.1.1 Interference

However, Bluetooth has some issues with signal interference. On 2016, Wolfgang Narzt and Lukas Furtmüller conducted a series of experiments with BLE and its interference, in the course of a research project named Mobility of the Future [NFR16]. They came to the conclusion that, when the antenna of the device was not aligned with the beacon in question, the device could not identify the distance to the beacon reliably. Additionally, the experiment was done with two other devices sending a Bluetooth signal. The distance between two phones was 2.5 centimeters and, according to the Bluetooth signal, it was 16 centimeters. The lowest recorded value was 6 centimeters and the maximum 35.5. They also conducted another experiment, this time with interference from 802.11 signal, because it operates in the same frequency band of Bluetooth, 2.4 GHz. By placing a Cisco Aironet 1250 router next to the BLE receiving smartphone, the results were better. The minimum recorded value was 2.4 centimeters and the highest value was 2.8, which is very close to the real distance, 2.5. Then, they tested the Bluetooth signal near the human body. With a 20 centimeters distance and a smartphone device pressed against the one end of the body and the beacon pressed against the other one, the results varied a lot. It calculated an average of 25 meters, a minimum distance of 1.4 meters and a maximum distance of 3.5 meters. In some occasions, the connection was lost up to 5 seconds, with a 300 ms interval of broadcast. From this, we can conclude that the human body significantly prevents BLE from being used reliably for distance communication. When it comes to wood, the results did not vary either and the conclusion was that it has no shielding effect on the Bluetooth signal. Metal, however, recorded a minimum value of 3.5 meters and a maximum of 4.4 meters, but with no loss of connection. It has a significant shielding effect but, as no loss of connection was detected, it only affects distance calculations, not communication.

2.1.1.2 Security and Privacy

As most wireless technologies, there are some vulnerabilities. Since it happens over the air, the communication can be eavesdropped and any device can be emulated to pass as a legitimate device, from a technological point of view. In 2013, Mike Ryan successfully exploited almost every aspect of the Bluetooth protocol such as eavesdropping on a BLE device, inject data on the sent and received packets and breaking the encryption of BLE. [Rya13]

- Eavesdropping: To eavesdrop a connection, one needs to know four unique values. The hop interval (the time period before hopping to another channel), the hop increment (established during the first connection), the access address (a value that prevents collisions between packets of two different communications) and CRC Init (a random number that is used to verify a specific connection). All the sniffing on the packets is done my modulating a signal generated by any bluetooth device.

- Injection: Packet injection was a proof of concept in which messages were sent undirected, broadcasting a MAC address. Then, a device would receive these messages and would list the sender.

- Breaking encryption: BLE contains encryption and key exchange. However, this key exchange protocol is one invented by Bluetooth SIG, which contains fundamental weaknesses, as opposed to more secure protocols, as Ryan demonstrated. The attack is not exactly on the encryption, that is based on AES-CCM [DW03] (an encryption protocol that contains no known attacks), but on the key exchange protocol. This key exchange protocol is based on no one knowing a shared secret between the sender and the receiver, the LTK, Long Term Key. To generate this LTK, a temporary key is first generated (TK) according to pairing mode, a confirm value and other values that are used to calculate the confirm value. All these values are exchanged over-the-air, in plain text, which means that are easily accessed. Then, the TK is "guessed" by means of a brute-force algorithm. According to Ryan, this algorithm, in practice, takes around one second to "guess" the TK, on a single core of an Intel Core i7 CPU. After this TK is known, the protocol continues normally, and a short term key (STK) is generated, which is the value used to calculate the LTK. So, knowing the TK, one can determine the STK and later the LTK, which means that any eavesdropper that knows the LTK is able to decrypt any communication between the sender and receiver.

2.1.1.3 Energy Consumption

BLE, as the name points out, requires almost no energy consumption. On one hand, in advertisement mode (the mode the beacon operates on), the device requires 274.19 µA, advertising with a broadcast interval of 100 ms. When considering a 2000 mAh battery, working all day (24 hours), the battery lasts 304 days without recharging. On the other hand, considering the connection mode (the mode the normal device operates on), the device requires 19.03 µA, connecting with an interval of 1000 ms. Considering a 3000 mAh battery, which is a normal smartphone, working all day (24 hours), the battery would last 6569 days (18 years, approximately). [UAS]

2.1.2 RFID

RFID, Radio Frequency Identification, is a technology first developed by Mario Cardullo around 1973. However, the first documented exploration of RFID was in 1948, in a paper by Harry Stockman, “Communication by Means of Reflected Power”. [Par15] It is used to communicate information between a stationary device and a mobile device, or even two mobile devices. It is comprised of two different structures: a reader and a tag.

- Reader: It is responsible for powering and communicating with a tag.

- Tag: Tags can be classified as passive or active. If it is an active tag, it requires a power source and it is limited by its lifetime, having the ability to broadcast a read of up to 100 m. Nevertheless, passive tags have the advantage of longer lifespan, as they have no need of a power source or maintenance. The passive tag is the most used one, as the active one has almost no applications, besides asset tracking. [Wan06] Then, the tag is divided in three structures: an antenna, a semiconductor chip and a capsule to protect the whole tag. As there is no power source, the antenna captures the energy that is exposed by the reader and uses it to communicate information between the tag and the reader. [AP10] It can read information from near contact to around 25 m, and it operates in three different frequency ranges: Low Frequency (125 - 134 kHz), High Frequency (13.56 MHz) and Ultra High Frequency (856 - 960 MHz). [Thr13]

RFID has two distinct designs when it comes to the power transfer from the reader to the tag. It can be either by magnetic induction or electromagnetic capture and both designs take advantage of the electromagnetic properties of the antenna: the near field and the far field. Near field is the field around the antenna up to 35 cm and utilizes inductive electromagnetic coupling, which means that it uses a local electromagnetic field to energize the tag, making it perfect for indoor environments and short range applications. In spite of that, far field antennas use capacitive coupling, propagating an electromagnetic field. It can be used for a number of applications, since it can cover more ground than near field antennas. Nevertheless, due to this increased read zone, it can sometimes read unintended RFID tags. [Smi14]

2.1.2.1 Interference

Since RFID is a wireless technology, there is always the possibility of signal interference with other technologies, specially in a workplace environment. There are two types of interference to note, interference in which the system does not respond and prevents data from being even interpreted and the other, a slightly more dangerous one, interference between two systems which can be seen as valid data among them. The most common interference, however, is noted during the deployment of the RFID system. RFID tags mounted on metals or containers of liquids fail to respond to readers. [cor15] Interference between signals can also happen if both coincide in the same range of frequency. For example, 802.11 and Bluetooth can sometimes lead to the bad functioning of a RFID system (Ultra High Frequency), due to the frequency they operate on. HF (High Frequency) RFID and LF (Low Frequency) RFID have almost no interferences, operating on a mostly unused frequency range. [Jou10]

2.1.2.2 Security and Privacy

RFID's privacy was a very debated topic around 2006 [Mal06]. In 2003, a boycott stopped Benetton from using RFID tags for its garments.. [Vio03] Since it is mainly used for tracking and inventorying, problems arise from the applications. As the tags respond to reader interaction without suspicion, unwanted scanning of tags can be a problem. It is used in inventorying and one can establish a link between a person and the items he buys, leading to an unwanted profiling of a customer. If used, for example, in medical prescriptions, one can know the disease of a person by scanning nearby tags. All these problems arise from the fact that there is no authentication and no secure way of communicating, which in turn leads to unwanted eavesdropping by other readers. [Jue06] However, this is not true for all tags. There are RFID tags with increased security capabilities that can compute symmetric key functions. This, in turn, prevents cloning of tags. Yet, due to price and resource constraints, these tags deploy weak cryptographic primitives and vulnerable protocols. In 2004, a team of researchers at John Hopkins University and RSA Laboratories demonstrated the vulnerability of cryptographic primitive used, the Digital Signature Transponder (DST). They started by reverse-engineering the encryption algorithm, cracking the key and finally simulated in the field the results obtained. The team was then able to steal their own vehicle through a simulated DST and purchase gasoline through a clone of their own public transportation ticket. [BGS+05]

2.1.2.3 Energy Consumption

As RFID contains three main frequencies (Low Frequency, High Frequency, Ultra High Frequency), it has different energy consumption levels based on the frequency which is used. High Frequency energy consumption is analyzed in section 2.1.3.3. As for Ultra High Frequency, spend around 2 to 3 A per operation. [ACFM12] Finally, Low Frequency spends even less, as it operates on a much lower frequency. [Smi16]

2.1.3 NFC

NFC, Near Field Communication, is a technology based on short-range, high frequency, wireless communication technology that enables exchange of data between two devices that are close to each other, with a physical separation of 10 centimeters or less. It was developed in 2002 by Philips and Sony and it is a subset of RFID technology, operating on the same frequency as High Frequency RFID, 13.56 MHz frequency [Thr13]. The NFC Standards are based on existing RFID ones and any others created by NFC Forum, an industry association formed in 2004. NFC Protocol varies between two modes of operation, the active and passive mode.

- Passive: Only one of the devices is transmitting information and the other one is only receiving, which leads to devices that do not need electric current, such as NFC Tags or Stickers, which make use of the energy generated by the active device.

- Active: In this mode both the devices are transmitting a signal and exchanging data and, as such, both need electric current

Currently, NFC technology is separated in three execution modes: reader/writer, peer-to-peer, and card emulation. [COO13]

- Reader/Writer: In Reader/Writer mode, the active NFC device, the one transmitting information, initiates wireless communication and can read data stored in a NFC Tag, as well as modify the data.

- Peer-To-Peer: In the Peer-To-Peer mode, the two NFC devices establish a bidirectional connection between them, which allows the devices to exchange any type of data between them.

- Card Emulation: In Card Emulation mode, any NFC device is compatible with a smart card, as long as it is based on the standards created by NFC Forum and RFID existing ones.The user presses his active device to an NFC reader, and the device behaves like a smart card.

2.1.3.1 Interference

As NFC is a subset of RFID, it shares its interferences, which are few. In the case of the active NFC, they are even fewer, as they operate on a very specific range that is not used by many other devices. For passive NFC there are no known interferences. [Jou10]

2.1.3.2 Security and Privacy

Since NFC enables various contactless exchange of sensitive information (such as payment card details and personal information), storing and managing this type of data in the secure area of the NFC device is a requirement for any NFC based system. To solve these kind of situations, these systems need to be saved and executed in a safe environment, the SE (Secure Element) of NFC. An example that safe communication is not always present is that in 2006, Ernst Haselsteiner and Klemens Breitfuß described a series of attacks and exposed how to leverage NFC's resistance to man-in-the-middle attacks to establish a specific key. [HB06] When it comes to NFC technology as a whole, there are some known security vulnerabilities and associated attacks:

- Eavesdropping: Even though NFC communication occurs in close proximity, eavesdropping is still possible. To prevent it, a secure channel of communication needs to be established between the devices, implementing encryption techniques. [Pag13]

- Data Modification: Data modification of the packets sent is done by inhibiting the NFC data exchange for a brief moment, altering the binary coding by via of a RFID jammer. It is a difficult attack to replicate, but it is still possible to, event though it can be prevented by analyzing all incoming signals. [Pag13]

- Relay Attack: This type of attack is an exploit on the NFC protocol compliance with ISO/IEC14443 [fS01]. The attacker, forwarding the request of a reader to its victim, needs to relay back the answer in real time, pretending to be the writer. In a real situation, the attackers holds a reader near the victim's card and relays all the information sent to a second reader, emulating the victim's card. It is also difficult to replicate, as it is very limited by the NFC range (10 cm) and time, meaning the failure of the attack. [FHMM12]

- Data Corruption: This attack can be interpreted as a DoS (Denial of Service) attack, an attack where the victim's machine or system is unavailable due to the flood of request to said system. [McD09] This is accomplished by transmitting radio signals, creating noise, and destroying the information sent by the sender. [Pag13]

- Spoofing: When it comes to NFC Tags, the information that is contained in them can be manipulated by different approaches, such as replace the tag, break the write protection on the original tag and overwrite it or even clone and impersonate them. [Pag13]

2.1.3.3 Energy Consumption

NFC is also a low energy consumption technology. There are now NFC self-sufficient chips. In 2011, STMicroelectronics launched new wireless chips that "harvest the energy generated from NFC and RFID actions to power up small devices so that a battery or other power supply no longer needs to be included" [Cla11]. From the point of view of the device being read, the passive mode, there is no energy consumed. The device that is doing the reading, active mode, uses around 15 mA [Soa12]. However, NFC will only consume energy when it is in fact being used. A smartphone, for example, its NFC can always be on for an entire day and it will spend around 1% of a smartphone's entire battery (provided that the NFC is not being used). For each read done by a normal smartphone (with a 3000 mA battery), only 0.5% of the battery will be used. [Soa12]

2.2 Other Technologies

Besides BLE, RFID and NFC, there are other meaningful technologies being used in the context of mobile ticketing around the world.

2.2.1 QR Codes

QR (Quick Response) codes were created in 1994 by a Japanese company named Denso Corporation. Its initial application was to track vehicles during the manufacturing process, greatly increasing the efficiency of the process of producing to shipping vehicles. QR Codes, being two-dimensional, are an evolution of the simpler barcodes, which are unidimensional and store only up to 20 digits. However, a QR Code can store up to 7089 numeric values, 4296 alphanumeric characters or 2953 bytes. [Inc10] It is also able to be read from any angle and quickly. It works by way of having a reader (usually a smartphone) that reads the encoded information present in a QR

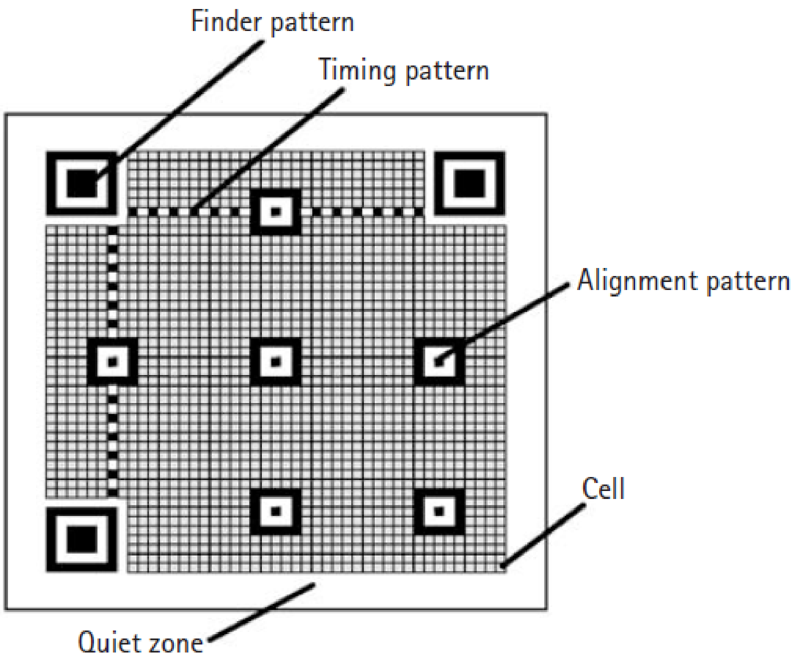


Figure 2.1: Structure of a QR Code [Soo08]

Code symbol. A QR Code can be described by mentioning 5 important items, as seen in figure 2.1.

- Finder Pattern: It is a pattern that allows for the QR Code symbol to be read in all directions, as it allows the detection of its position.
- Alignment Pattern and Timing Pattern: These patterns enable the correction of the distortion on any QR Code symbol.
- Quiet Zone: This area facilitates the detection of the QR Code symbol.
- Cell (Data area): This area contains all of the information that is actually stored in the symbol.

It is also capable of functioning in unideal conditions, such as angled surfaces or tilted readers. QR Code has alignment patterns arranged with a regular interval within the range of the symbol. The variance from the center of the symbol up to its outer shape, allows for distorted and non-linear symbols to be read. [Soo08] When it comes to error correction and adaptability, QR Codes have both. As QR Code is prone to being tear (by being impressed, for example, on a paper) or damaged, it has the ability of correcting itself, depending on the damaged area, up to 30%. This ability is obtained by arranging Reed-Solomon codes in the QR Code area [Bha15]. It is also very adaptive to the environment the symbol is ingrained in and the way it is printed. An inverted signal can be read as easily as a non-inverted one, containing the same information. If the black and white area is also inverted, the outcome is the also the same. Its printing can also be quite modified, as even circular cells can be read, when in comparison with rectangular ones. [Soo08]

2.2.1.1 Security & Privacy

As a security matter, the one that is talked the most and happen the most is the replacement of a QR Code by a malicious or unintended one. [Ley12] Even though QR Codes contain information and data, they can also contain commands to open a browser and redirect the user to malicious websites. This opens the door to browser-based exploits and cross site scripting, for example. Furthermore, some scanning applications keep track of all the scans done in an internal database. SQL Injection can be exploited here also, circumventing authentication mechanisms [KFK+14]. In 2012, Ravi Borgaonkar successfully executed MMI (Man-Machine-Interface) codes on Samsung phones, even going as far as wiping all of a phone's data by scanning a QR Code. [Bor12]

2.2.1.2 Energy Consumption

The QR Code itself has no energy consumption, as it is merely a symbol printed.

2.2.2 WiFi

WiFi is a wireless communication technology that is mainly used for WLAN (Wireless Local Area Network) and its implementation is based on the protocol of 802.11 by the IEEE (Institute of Electrical and Electronics Engineers). [BC13] It operates on two frequency ranges: 2.4 GHz, Ultra High Frequency, and 5.8 GHz, Super High Frequency. Like other communications, its based on radio frequencies and it is communication is done using channels, 2.4 GHz has 11-14 channels available and 5.8 GHz has 30 channels. This difference comes from legal restrictions, as different countries allow different number of channels to be used in the correspondent band. [BC13] When considering WLAN (Wireless Local Area Network), it requires the existence of a computer with a wireless network controller. Then, a router spreads the data available through a frequency range that is captured by the computer, provided they share the same frequency and are connected. After the connection is done, a WiFi signal occupies five different channels during the transmission, working up to a theoretical limit of 100 m. [Gei01]

2.2.2.1 Interference

WiFi contains some known interferences due to the fact that it operates on the 2.4 GHz band, the same band that microwaves, Bluetooth devices, security cameras and ZigBee devices operate on. Besides that, occupying five different channels, means that two channel numbers that differ by five, have no interference. For example, channels 4 and 9 do not overlap. However, many WiFi connections have the same default channel for the initial startup, which may lead to congestion on some channels. [Lud16]

2.2.2.2 Security & Privacy

Being a wireless technology, WiFi has some known vulnerabilities, by, usually, the signal being broadcasted freely. Some counter-measures include hiding the SSID (Service Set IDentifier) broadcast or only allow known MAC (Media Access Control) addresses to connect to the network. WiFi also contains other securing methods. WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2 were used but contain some known vulnerabilities. In 2018 the WiFi Alliance announced WPA3, a replacement for WPA2.
WEP was a security algorithm created in 1997 and discontinued in 2004, due to the appearance of WPA. Later, WEP was considered insecure due to the cyphers used. [BH06] WPA appeared around 2003 and was designed as an intermediate solution between WEP and WPA2. WPA differs from WEP in the encryption keys used. WEP used only an encryption key, where as WPA employed a different key per packet exchanged, preventing the attacks that WEP were vulnerable to. However, in 2005, researchers found that WPA contained a flaw in the hashing of the integrity of the messages exchanged, paving the way for packet injection and spoofing. [HSSB05] Around 2004, WPA2 was developed and created. Even though it was more secure than WPA, it required more processing power from the device using it, failing to gain traction by that time. The main difference between WPA and WPA2 was the use of AES for the cryptography. Then, in October 2017, Mathy Vanhoef discovered a vulnerability in the handshake protocol in WPA2 that leads to the full undesired control of a network. [Van17] In January 2018, the Wi-Fi Alliance announced WPA3, a replacement to WPA2, that will use 192 bit encryption keys individualized for each user. It will also, allegedly, mitigate security issues associated with weak passwords. [All18]

2.2.2.3 Energy Consumption

Routers that use WiFi technology vary their energy consumption between 2 to 20 Watts, being that 6 is the average. For a router consuming 6 Watts and being used 24 hours per day, it will only consume 0.14 kWh, which translates, roughly, to 7 Euros per year. For a router consuming 2 Watts, it would consume 0.05 kWh, 2 Euros per year. Lastly, requiring 20 Watts, consumes 0.48 kWh and it would cost approximately 20 Euros per year. [Cal18]

2.3 Mobile ticketing solutions

2.3.1 Masabi

Masabi is a company that offers a solution for public transportation based on mobile ticketing. It is the first company to prove successfully in the area of mobile ticketing, being the first to take mobile ticketing to volume in 2007 and prove the concept. It was also the first agency mobile ticketing deployment in the USA in 2012 with Boston MBTA (Massachusetts Bay Transportation Authority) [Mas18a]. Masabi's solution has the name of Justride and is implemented as a cloud-based mobility platform and layers its foundations in the concept of Software As A Service (SaaS). It allows for pre-ticketing, meaning that the customer needs to purchase tickets before boarding the public transportation vehicle. Besides the customer point of view, Justride is comprised of 3 different products: Justride Retail, the mobile application used by the end customers, Justride Hub, that allows for companies to have a dashboard that aggregates different kind of data and analyze it, enabling the ticketing agencies to control and maintain their business, and Justride Inspect, a validation system [Mas18b]. Masabi's main customers are New York's Metropolitan Transportation Authority with a ridership of 1.7 billion, National Express West Midlands (NXWM), a bus operator in the West Midlands that operates services in Birmingham, Walsall and Wolverhampton and The Massachusetts Bay Transportation Authority, the United States 5th largest transit agency [Mas18a]. There are around 30-40 deployments of Masabi's product, Justride, around the world [Mas18a] and in 2017 it was deemed as the best Public Transport App of the Year at the Smart Rail Innovation Awards. [Mas18c]

2.3.2 Cubic

Cubic is another company that has a solution in the mobile ticketing area, even though it is not solely focused on that. Cubic's solution is named NextCity. It centers on three core principles, the delivery of an integrated customer experience, one account and integrated operations and analytics. [Cor18b] It also contains a revenue management system, that runs efficiently and reliably, with 24 billion transactions processed per year and also provides financial clearing and settlement, business analytics, device and asset management, prepaid benefits, fare table management, customer service infrastructure, fraud analysis and fare collection engines. The payment, customer-side, is also handled by Cubic, either by contactless smart cards or NFC using smartphones. [Cor18c] It also allows for analytics of all the data collected via Cubic's service. [Cor18a]

2.4 Different Approaches in Different Cities

2.4.1 London

London's public transportation system is based on a Check-In/Check-Out concept, due to the nature of the system (having a significant percentage area underground). To start a journey, one must simply validate his ticket in the validator before entering the public transport vehicle. Later, to finish the journey, there is the need to validate the ticket again, otherwise the max fare will be charged for that journey. [Woo16] However, when traveling by bus, the price charged is the same, regardless of time or distance spent, as it is a flat fare system. London's public transportation service price tickets are based on a zone system and have an extra charge if used during peak hours. It is divided in 9 zones and each have a different price charge. [Woo16] Even though it is still possible to buy a paper ticket, most operators are switching to the Oyster card and respective mobile application. The Oyster system is based on a credit card where it is loaded credit onto and the fare value is subtracted as more travels are done. To fully utilize the application, one needs to buy an Oyster Card, based on NFC, and register it in the Oyster App. Then, the smartphone, running the Oyster App, acts like a smart card and is able to view the journey history, check the balance of the card and, most importantly, load credit onto the card and validate the start and end of a journey. [Oys18]

2.4.2 Shanghai

Shanghai public transportation system aggregates metro, bus, tram, trolleybus, train and rail. Currently, it has the world's largest public transportation system which also handles the largest volume of passengers [Sha18b]. Since 1999, it is possible to travel on the entire system with the Shanghai Public Transportation Card, a contactless card which uses RFID as a communication technology. [SPT18] Its system is similar to London's, as the card is a debit card which is rechargeable and is also a Check-In/Check-Out System. [Sha18a] Nonetheless, the card system is slowly being replaced by mobile ticketing. As of 18 January 2018, Shanghai Metro adopted a mobile ticketing approach based on the use of QR Codes, installing QR Code Readers on all of its stations (389). To fully utilize the new system, the customer needs to install an application created by Shanghai Metro, associate its bank account with the application or charge it, like the contactless card. [Zha18] The decision of utilizing QR Codes as the basis of this mobile ticketing approach as much to do with China's culture, that is very prone to the use of QR Codes throughout restaurants, public transports and clothes stores. Even beggars are now using Alipay and WeChat Pay, two online payment and money transfer systems, to ask for money, as seen in figure 2.2. [Ald18]

Figure 2.2: A beggar in China has come up with an innovative way to collect his handouts. Photo: Handout [Ald18]

2.4.3 New Jersey

New Jersey's public transportation system is managed by NJTransit, a company that covers a service area of 13 791 km^2 square miles, United States of America's third largest provider of bus, rail and light rail transit, linking major points in New Jersey, New York and Philadelphia. It also operates a fleet of 2477 buses, 711 trains and 45 light rail vehicles. It contains 871 bus routes and 14 rail lines statewide, providing nearly 223 million passenger trips per year. [NJT18a] Since April 2013, the company has switched the contactless card for a smartphone, implementing a mobile ticketing approach based on the pre-purchase of tickets through an application developed by NJ Transit. It allows the secure purchase of daily tickets or monthly ones through a credit card or online wallets, such as PayPal, Android Pay or Apple Pay. Then, the ticket is activated in the mobile application and to gain access to the vehicle, the customer only needs to show the activated ticket to the conductor or the bus operator and the fare inspector. [NJT18b]

2.4.4 Porto

Porto has 3 main operators that handle public transportation: STCP (Sociedade de Transportes Coletivos do Porto), handling buses in the city, CP (Comboios de Portugal), handling trains in all of the country and Metro do Porto, that handles the metro in Porto and the surrounding areas. STCP was created in 1946 [STC18b] and currently has 73 bus lines and four different types of vehicles in their fleet. [STC18a] CP has 2179 km of rail roads in Portugal [CPR18], 258 vehicles (trains and locomotives) and was founded in 1856 [CPV18]. In 2017, CP sold 122 million tickets to passengers. On the metro side, Metro do Porto has 6 operating lines, marked with different letters and colors (A to F), 102 vehicles in their fleet, 82 stations and in 2017 alone sold 58 million tickets. [Met18a] It was created in 1994 [Met18b] and is now planned to open one new line and expand an existing one in 2019. [Met18c]
These 3 operators, in 20th December 2002, created a complementary business grouping, by the name of TIP (Transportes Intermodais do Porto). This entity's mission is to promote the use of public transport, allowing an increasing and better mobility of citizens of the MAP. Furthermore, its functions are to define important common business rules in key areas such as zoning, tariffs, ticketing and revenue sharing. [TIP15]

2.4.4.1 Current Solution

The public transport network of the MAP (Metropolitan Area of Porto) covers an area of 1,575 km2 and serves 1.75 million of inhabitants. There is also an initiative to travel around the MAP called Andante, that englobes all of the operators mentioned in the section 2.4.4 and a few more. Currently, the Andante system has 12 operators: Metro do Porto, STCP, CP, Resende, Espírito Santo, Maia Transportes, Valpi, ETG, MGC, A. Nogueira da Costa, Auto-Viação Pacense and Auto-Viação Landim. [And18d] It is an open (ungated) system that divides the Metropolitan Area of Porto in 46 zones through a ring of zones system. This system means that the fare is calculated by the number of ring zones the user traveled, the rings of zones are counted around the zone where the user began its journey, until the limit of rings of zones acquired (Z2 in the case of two rings, Z3 in the case of three rings, ...). [And18e] Figure 2.3 shows an example of this ring of zones if an user enters in the C1 zone.

The system works by way of a RFID smartcard with pre-purchased tickets that range from Z2 to Z12, having a time range of one hour for the minimum fare (Z2) going all the way to two hours and fifteen minutes in the maximum fare (Z12). Besides the pre-purchased tickets, there is also a monthly pass with a subscription plan and in this scenario, areas are counted differently for billing purposes, as the user pays for the zones he will be traveling during the subscription plan, not a ring of zones system. [And18a] There is also another possibility when considering ticketing of the Andante system, the Andante 24, that allows traveling in the defined zones for 24 hours after the first validation.

As for billing prices, there are four price variations, dependent on the social aspect of the passenger: student, pensioner, senior or a child, as seen in tables 2.1 and 2.2.

Table 2.1: Casual Travel Tickets [And18f]

Type Of Ticket	**Andante Simples**	**Andante 24**
Z2	1,20	4.15
Z3	1,60	5,50
Z4	2,00	6,90
Z5	2,40	8,30
Z6	2,80	9,65
Z7	3,20	11,05
Z8	3,60	12,40
Z9	4,00	13,80
Z10	4,40	15,20
Z11	4,80	16,60
Z12	5,20	18,00

Table 2.2: Monthly Passes [And18f]

Type Of Ticket	**Normal**	**Social+ (B), Sub 23 (B)**	**Social+ (A)**	**Sub 23 (A)**
Z2	30,60	22,95	15,30	12,25
Z3	37,75	28,30	18,90	15,10
Z4	48,05	36,05	24,05	19,20
Z5	58,75	44,05	29,40	23,50
Z6	68,25	51,20	34,15	27,30
Z7	77,65	58,25	38,85	31,05
Z8	87,10	65,35	43,55	34,85
Z9	96,55	72,40	48,30	38,60
Z10	106,00	79,50	53,00	42,40
Z11	115,45	86,60	57,75	46,20
Z12	124,90	93,70	62,45	49,95

As for the smartcards, there are two types, Andante Azul and Andante PVC. Table 2.3 shows the difference between both.

Table 2.3: Different Types of Smart Cards [And18b]

Andante Azul	**Andante PVC**
Paper Card	PVC Card
Rechargeable with tickets and Andante 24	Rechargeable with tickets, monthly pass and Andante 24
Validity of 1 year	Validity of 5 years
Can only contain one type of ticket (Z2, Z3, etc)	Can contain multiple types of tickets
Can be shared	Personal and non-transferable
0,60€	6,00€

The Andante system is based on a Check-In/Be-Out approach, as the user pre-purchases the ticket and validates it before starting its journey in the designed vehicle of choice. If there is the need to change vehicle or line, it is necessary for the user to validate its ticket again and when the journey ends, there is no need for the user to check-out. [And18c]

2.4.4.2 Future Solution

As seen in the section 2.4.4.1, the Andante system is quite complex, has many zones, 12 operators integrated and many types of tickets. So, a mobile ticketing project started being thought out and developed around 2013. [FNDC14] At the time, a prototype was developed for the bus operator, STCP, that consisted in the pre-purchase and validation of Andante tickets. In 2015, Leal and Couto [CLCG15] explored the possibility of using QR Codes, NFC and BLE to aid a potential mobile application in the context of mobile ticketing in Porto. Only in 2017, a more robust application started gaining traction, by the name of Anda, a Check-In/Be-Out approach to mobile ticketing that has the main goal of being "a platform that is seamlessly integrated with Porto's intermodal public transportation network, while simultaneously bringing the users a pleasant experience, either by its simplicity of use, or by the many advantages that a service like this can offer" [PM17] The Anda project consists of a mobile application that serves as an interface interacting with the Andante system. The main technology used are BLE beacons that allow for the users to be tracked throughout their journey so that the application is able to deduce the start of the journey. The app captures beacon's signal and asks the user if he is entering the public transportation vehicle, and the end of the journey is deduced when the user's device stops capturing the beacon's signal. For railway operators, the beacons were installed inside the validators that were used for the check-in with the Andante system. For the buses, the beacons were installed inside the vehicles. By the end of 2017, the Anda project switched to a Check-In/Be-Out approach with the aid of the NFC technology for the Check-In, embedded in the validator. [And18g] A very important competitive advantage of the Anda system is the post-billing and tariff optimization.

By tracking the check-in and estimating the end of the journey, the application can keep a record of all the journeys traveled. At the end of the month, the payment for these travels is done and the customer does not need to understand the system or buy any kind of ticket, as the application does it for him. There is also a tariff optimization implemented that charges the customer the minimum fare considering the travels made during the entire month. For example, on the current system relying solely on Andante, a user buying 28 Z2 tickets would spend 33,60 €. However, on the future system, Anda, the application would buy a Z2 monthly pass, only charging 30,60 €. This is a major advantage, as reported by Sofia Tojal and Emília Gomes, participants of the Anda pilot. [Coe18]

2.5 Monitoring of public transportation systems

Most monitoring systems focus on the monitoring the business aspect of mobile ticketing. This includes monitoring of fraud, statistics of use and number of fares purchased. Others focus on the traffic and schedule adherence of the circulating vehicles. Abdalla et al. "integrated buses network management system with poles apart intrusion detection system (IDs) using satellite-based technologies applied" [ARFY11], which in turn provides the passengers with information about bus routes and the location of the buses in real time. This system helps customers choosing their routes and timetables and, besides that, could be an approach on how to increase driver efficiency and routes taken. Hannan et al. [HMHB12] also implemented an intelligent bus monitoring system that focus on tracking the movement of any bus, using RFID, GPS (Global Positioning System), GPRS (General Packet Radio Service) and GIS (Geographic Information System).

2.6 Conclusions

There are many different mobile ticketing systems used worldwide which need electronic systems for monitoring public transportation. Using either Bluetooth, RFID, or even QR codes, these systems are as varied as the cities they are implemented in, changing accordingly to their environment the cultures and people living them. None of these systems is perfect, having flaws still in security and ease-of-use, and there is not, and might never be, an universal system used worldwide or even consistently within a single country. However, in recent years many advances have been made, creating easier and more comfortable ways for commuters to pay for their trips, creating a seamless traveling experience that will only improve over time.

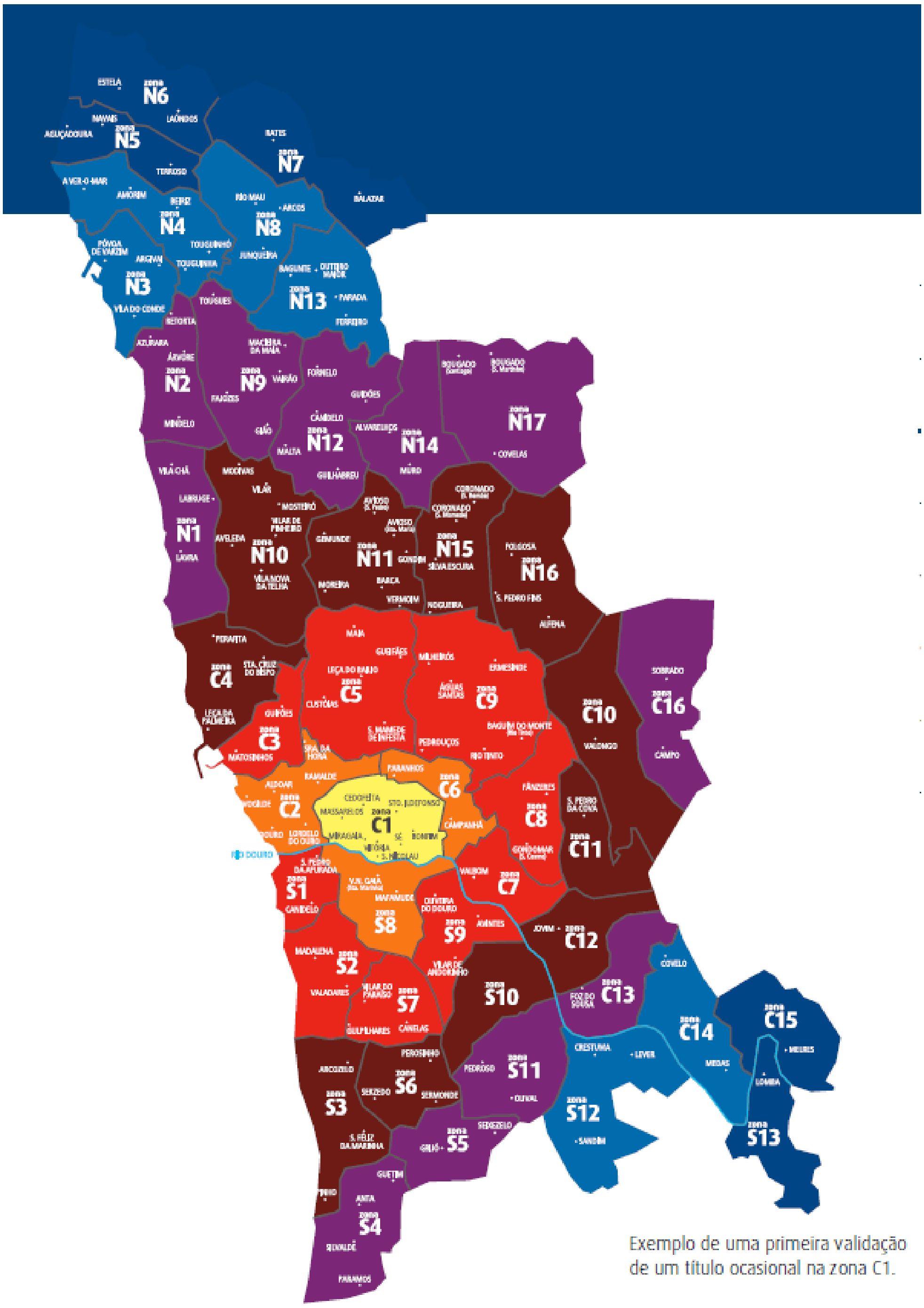


Figure 2.3: Validation in C1 zone. [And18f]

Chapter 3

The Anda mobile ticketing system

Anda is a mobile ticketing system which makes use of an Android application for this purpose. It was developed for the MAP and was the result of a joined project between FEUP (Faculdade de Engenharia da Universidade do Porto) and TIP. This project started in 2016 and is, at the moment, in the final testing phase. It will be available at the end of June 2018 to all MAP users.
This chapter describes Anda's system and identifies some of the portential issues that motivated this work. It is divided in three main topics: the architecture of the system, the way it operates and the identification of current errors and flaws.

3.1 Anda Architecture

3.1.1 Anda Back-End

The Anda back-end encapsulates the majority of the operations that are relevant to the Anda system and is represented in a green rectangle in Figure 3.1. It contains an internal database in which it stores the user's info, as well as the journeys details. Subsequently, these journeys are converted into validations and are then sent to the CCB (Computador Central de Bilhética). The CCB, the blue rectangle in Figure 3.1, is the main database belonging to TIP which stores all of the journeys details of any user, as well as information pertinent to them, such as all of the stations that exist in the MAP, timetables and their respective operator. The CCB also communicates with the Anda Back-End sending information about all the stations and lines. Finally, the most important and innovative aspect of the Anda system also resides in the Anda Back-End, the tariff optimization algorithm that optimizes the user's journey payment, either by buying a different ticket than the one he was supposed to (resorting to the time span that each ticket possesses since its first validations) or even buying a monthly pass, if it is justified. This process is run daily.

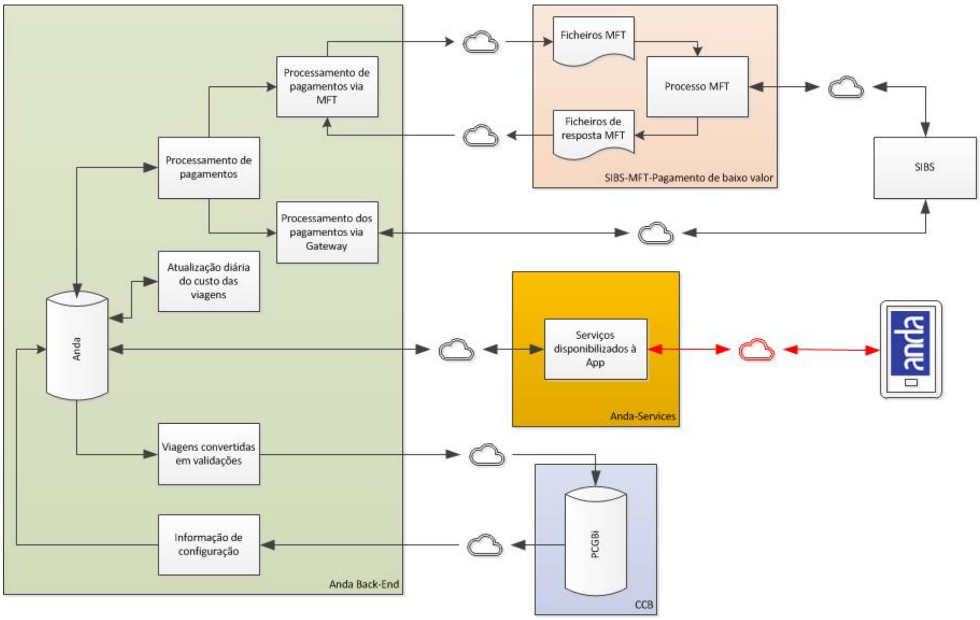


Figure 3.1: The Anda architecture

3.1.2 Payment Gateway

The payment gateway relates mostly to the red rectangle in Figure 3.1 and its communication with the Anda Back-End. All of the transactions are handled by SIBS (Sociedade Interbancária de Serviços). There are currently two possible types of payment:

- PBV (Pagamentos de baixo valor): This type of payment can be compared with the payment of tolls or public phones. A low value payment means that the user has no need to insert his PIN (Personal Identification Number) code to pay his expenses. It is also related with the payment of small amounts. Anda also has this option and any user who wants his payments to be executed this way, only needs to go to an ATM (Automated Teller Machine) of the rede Multibanco, a network of Portuguese ATMs, consisting of almost all retail banking in Portugal, and then associate its personal account with the Anda account. After the validation the amount to pay will be debited in his account twice per month.

- Payment by credit card: In case the user opts for this payment method, he only needs to, at the moment of registration or when updating his personal information, insert its credit card details into the Anda application (which does not store them) which, in turn, will send them to SIBS and the payment is debited in the credit card, at the end of the month.

3.1.3 Anda Services

The Anda Services, represented in an orange rectangle in Figure 3.1, is a DMZ (Demilitarized Zone) that acts as a bridge between the Anda application and its back-end. Only a series of calls, operations and services are open and meant to be called by external services, such as the Anda application. The Anda Services enforces a layer of security to sensitive information.

3.2 How it works

3.2.1 Register a new account

In case of a new user, to use the Anda system it needs to download the application from the Google's Play Store and create a new account. This creation is depicted in figure 3.2 and the main details that the user is obliged to fill are his name, e-mail, password and cell phone number. Furthermore, the user can also add his fiscal information to request invoices, such as his address, postal code, fiscal name and his NIF (Número de Identificação Fiscal), even though this information can be filled out later, after the registration.

3.2.2 Validate account and login

After the registration is done, the user receives an e-mail to validate his account by clicking a given link. If all the process is successful, the user has his account validated and can now log in, after inputting his e-mail and password, as shown in figure 3.3.

3.2.3 Profile

As for the user's profile, there are three main areas: his personal information, shown in figure 3.4, his payment details, displayed in figure 3.5 and lastly, his social profile, presented in figure 3.6.

- Personal information: In this area, it is possible to edit only the user's name, but not the e-mail and phone number, due to business decisions.

- Payment details: In this area, the user can choose his payment method, as depicted in section 3.1.2. Besides that, the user can check his payment information as well as his fiscal information.

- Social profile: This area is related to the user's social information, in case of any monthly pass, given that the user is a student, pensioner, senior or a child, as seen in section 2.4.4.1. It also has the information of start and end of any social profile.

3.2.4 Journey mode

In Figure 3.7 there is an overview of the journey mode within the Anda system. First, the user needs to open the Anda application and press the smartphone against any validator. Then, if successful, a positive response will be seen in the validator's screen and in the smartphone. However, in case of any error, the error will only be displayed in the validator's screen. This comes from a technological impossibility, as the validator does not send any type of message if an error occurs. Afterwards, in case of success, the Anda application starts scanning for Bluetooth signals and tries to decode the key of any signal. If it is a match for an Anda BLE beacon, which is being transmitted from any operational beacon inside the validator, then the application can track the user throughout its journey and know its exact course, as seen in figure 3.8. The key of the beacon identifies it, by sharing its operator, line, vehicle (if the beacon is inside a bus) and station. Consequently, the application continues scanning for beacons until the user's journey ends. This is decided by one of five ways:

- An uninterrupted period of fifteen minutes, in railroad vehicles, or ten minutes, in case of road vehicles, during which no BLE beacon signal is caught.
- The Anda user walks for more than three uninterrupted minutes, with a 70% trust rating in steps.
- The user ends the journey in the first minute after validating if it did not capture any BLE beacon signal.
- By starting a new journey, validating in another validator. This action is valid as in the MAP, the user needs to validate if it is interchanging stations.
- An uninterrupted period of ten minutes catching the same BLE beacon signal.
- Not capturing any beacons' signal besides the first one, for a time interval of more than one hour straight.

Lastly, the user can be supervised by any revisor, as seen in figure 3.9. For this effect, the user has to press his smartphone against the revisor's machine and, then, also show this screen to the revisor. There is information about the user, the operator and line he is travelling, the zone in which he validated and the current zone, and the station he embarked in and the current station.

3.3 Known errors and flaws

Since April 2017, the Anda system is available for a closed testing group of 150 passengers that uses the Anda application daily, as well as the Andante card. The mission of the "testers" is to use both the Anda application and the Andante card and report on it and the problems that arise from its use. The Anda pilot user has the need to validate both the Andante card and the application because, at the moment of testing, the application has no legal value. Besides that, this double validation also allows to verify if the testers are collaborating at the needed demand, since both means of validation are compared daily. The problems of the Anda system vary:

- BLE beacons are not detected.
- The Check-In is malfunctioning with the NFC technology.
- Validators are not uniformed; some beacons issue data that is different from the one sent by the validators.

- The application does not detect the end of the journey in an acceptable amount of time.
- Some users report the app malfunctioning.
- The application does not show correct information at all times.
- BLE beacons emitting erroneous information.
- BLE beacons not synchronized with their NFC counterpart.
- Consistent errors in the process of validation.

The main issue is that, at the time, the resolution of the problems is done as they occur, and it is by a method of trial and error. The Anda system, in terms of actions and sequences, is explained in Figure 3.10. Mostly, a first-time user needs to create a new account and validate it via e-mail. Then, the process is equal to any other user. After logging in, he can then access his account history of journeys, billing history and account definitions. Besides that, it unlocks the journey mode, which can be started by pressing the smartphone against the validator. Many errors occur in the validation stage. However, data related to validations could not be obtained (as none is stored) and, consequently, the proposed solution has almost no information about any problem that may surface in this stage of the Anda interaction. The errors that may surface in this stage are: unknown card, which point to a flaw in the NFC connection, meaning that the NFC's antenna embedded in the validator could not read the NFC card emulated in the smartphone; invalid card, which means that the NFC antenna read the emulated card, but could not validate it; expired card, which means that SpirTech, an external company, has not validated the emulated card and this problem is fixed by clearing the smartphone's cache of the application. There are also reported problems related to the visualization of information in the application, such as incorrect journeys being shown, incorrect dates and UI (User Interface) issues, which are also not contemplated by the dashboard. Sometimes, during a journey, some beacons' signal is not captured by the user's smartphone. Even though this information is available, it was also not contemplated by the dashboard, as this information is only available through the usage of logs, which were not possible to interpret, as explained in section 4.3.2.

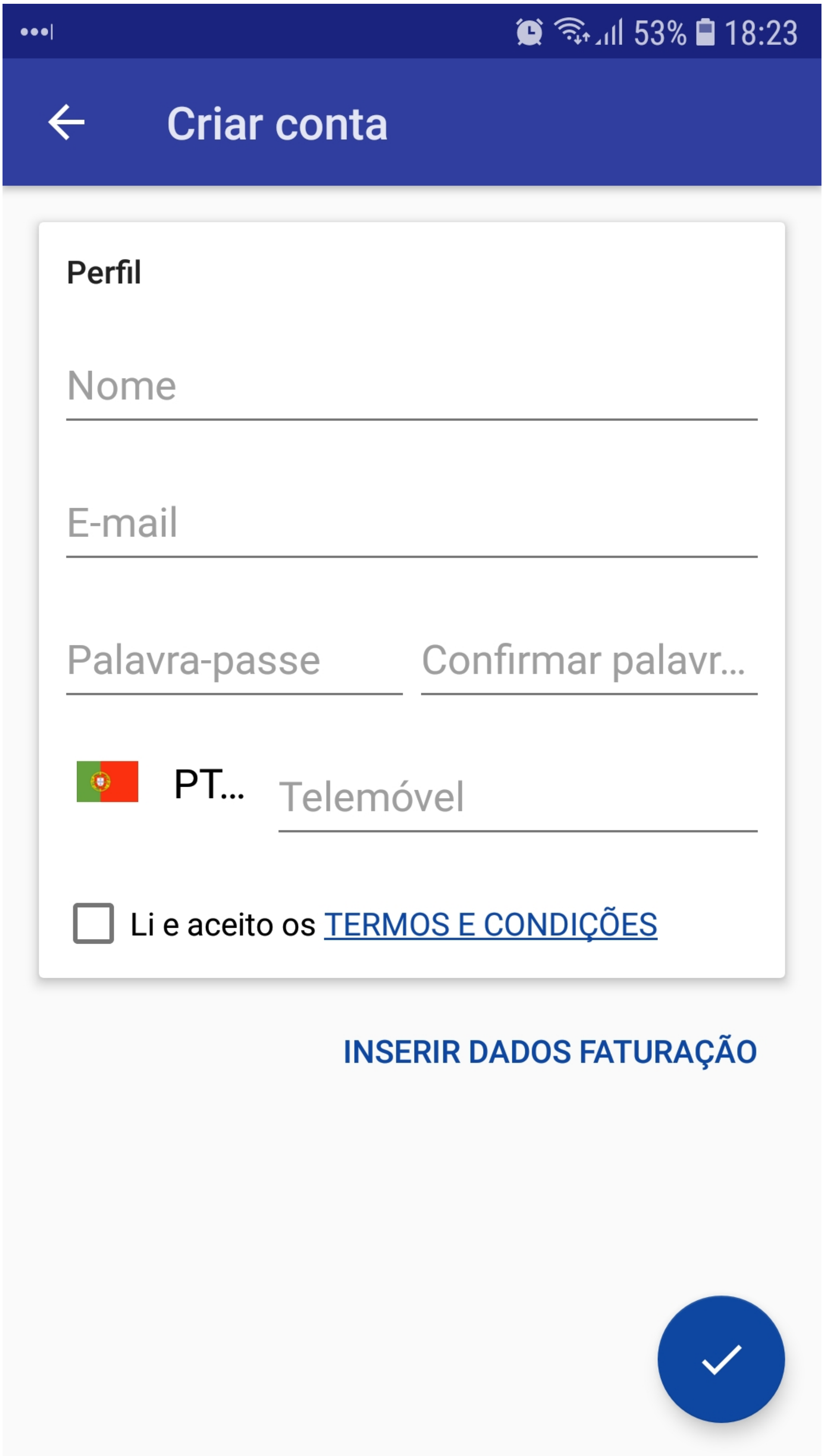


Figure 3.2: Creating a new account

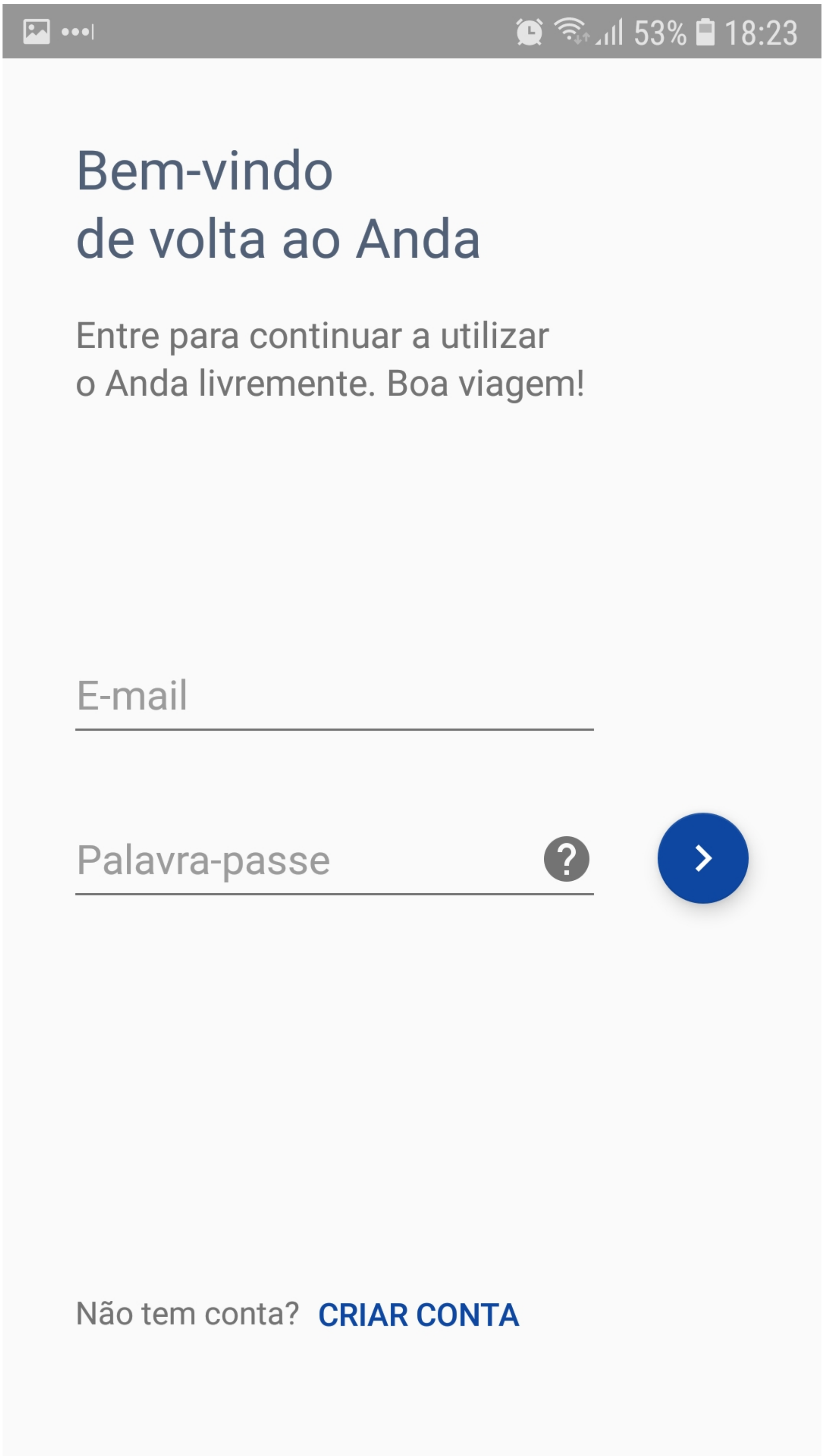


Figure 3.3: Login

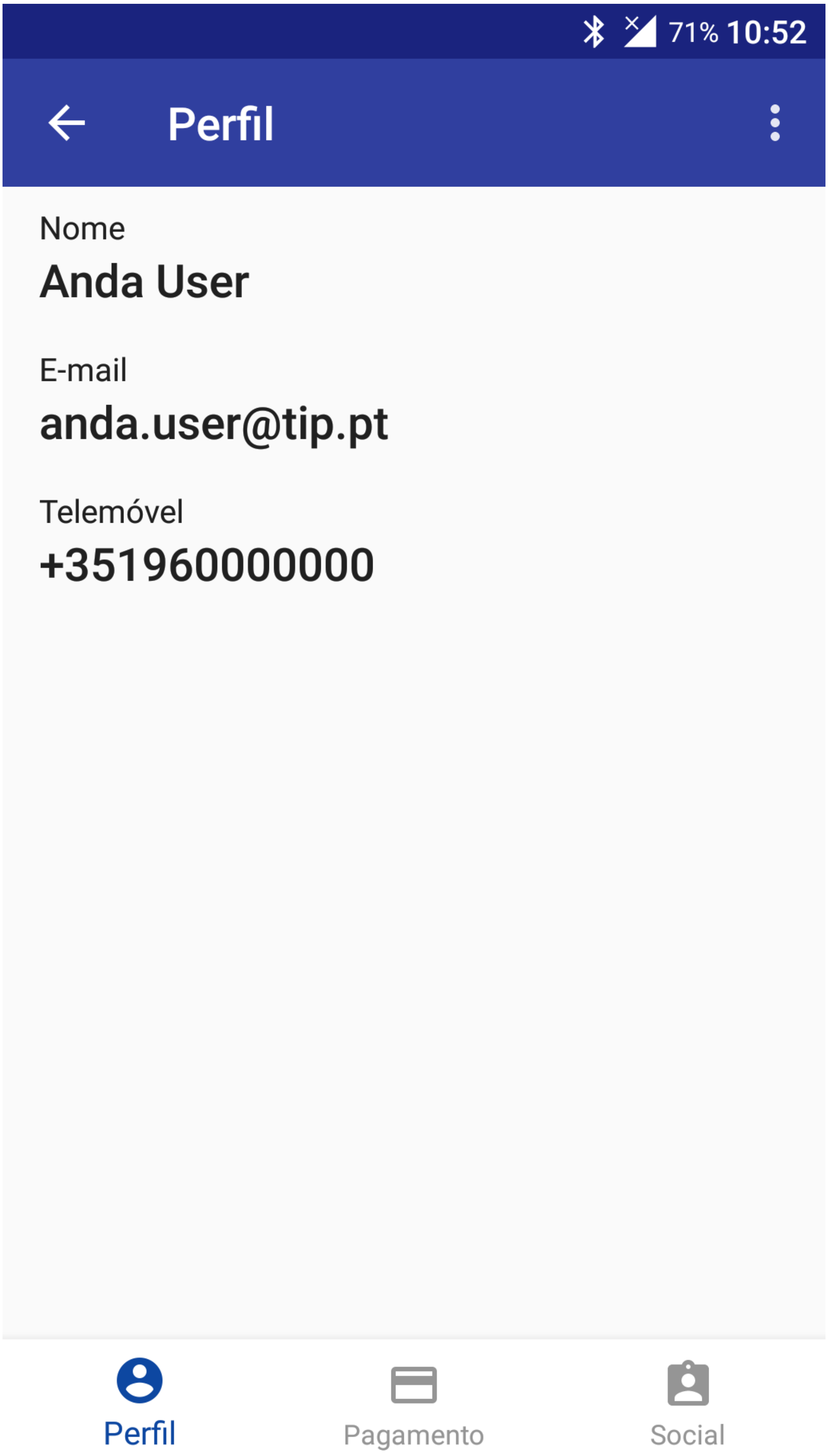


Figure 3.4: Personal information

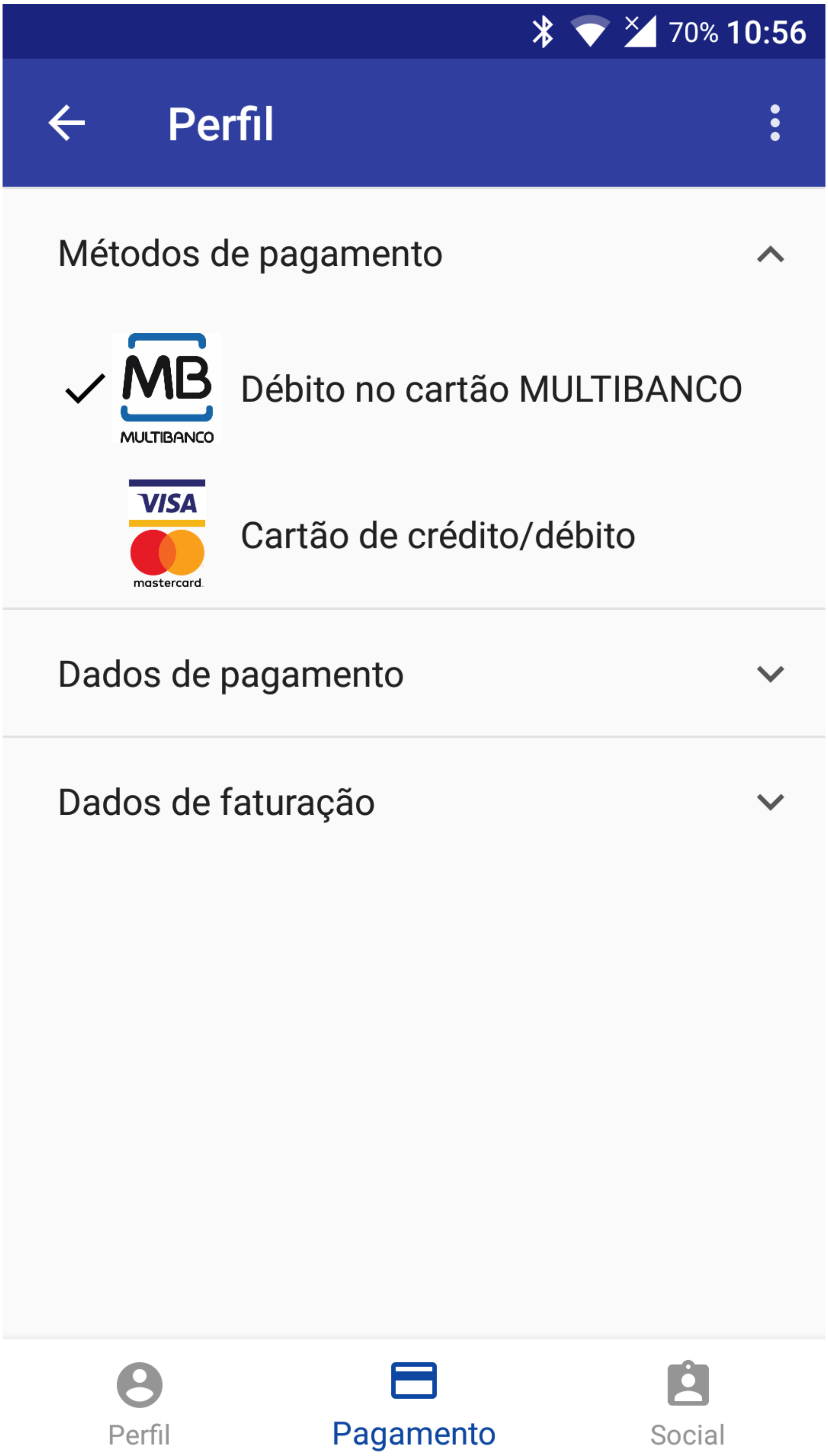


Figure 3.5: Payment details

Figure 3.6: Social profile

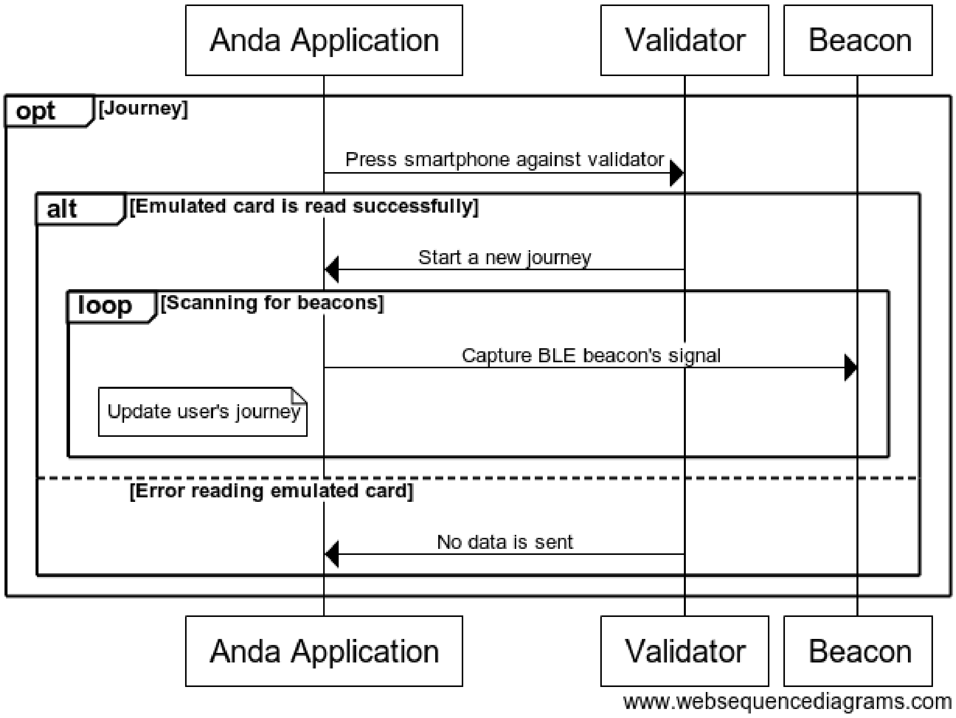


Figure 3.7: The Anda system journey sequence diagram

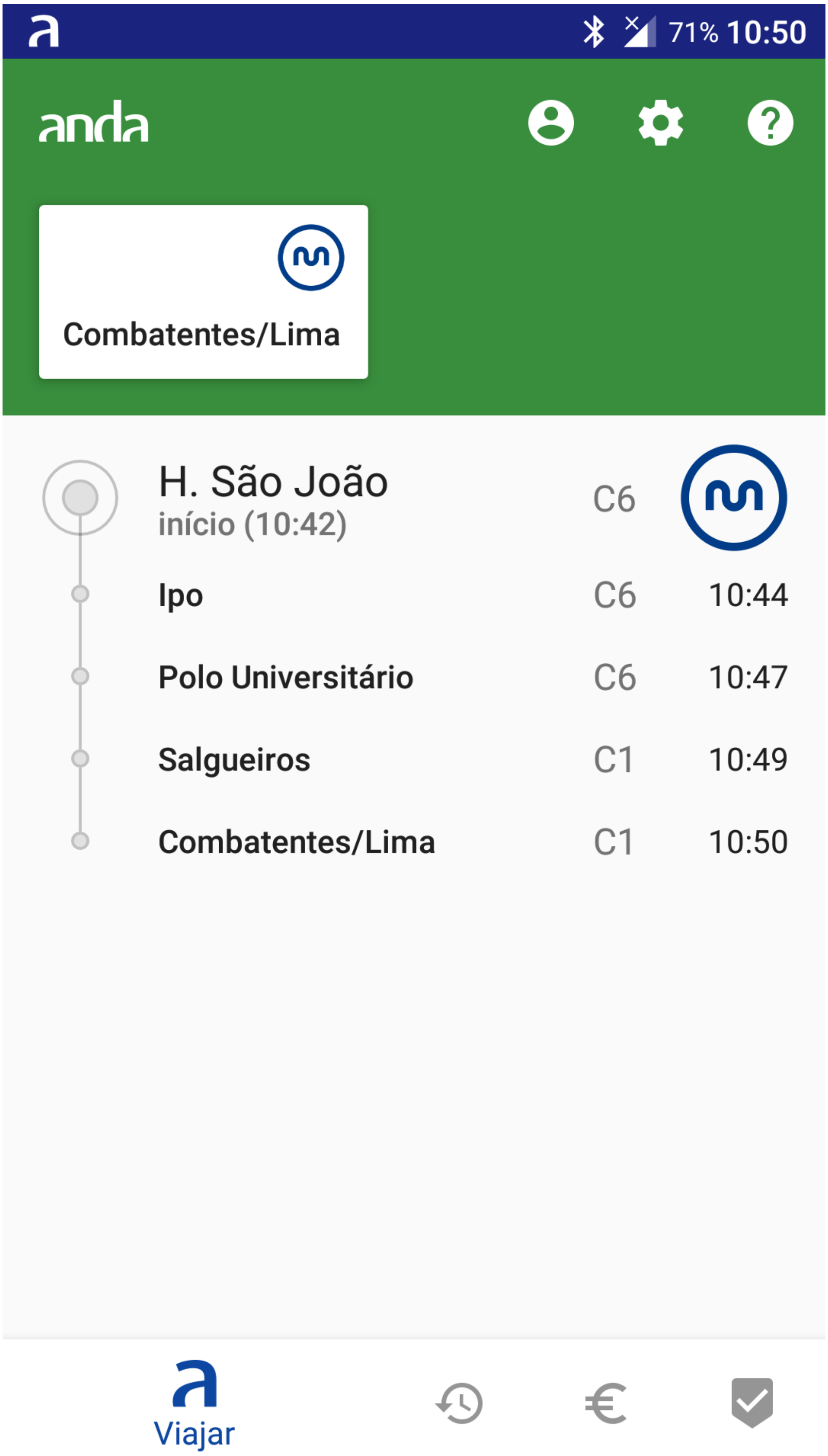


Figure 3.8: The Anda system sequence diagram

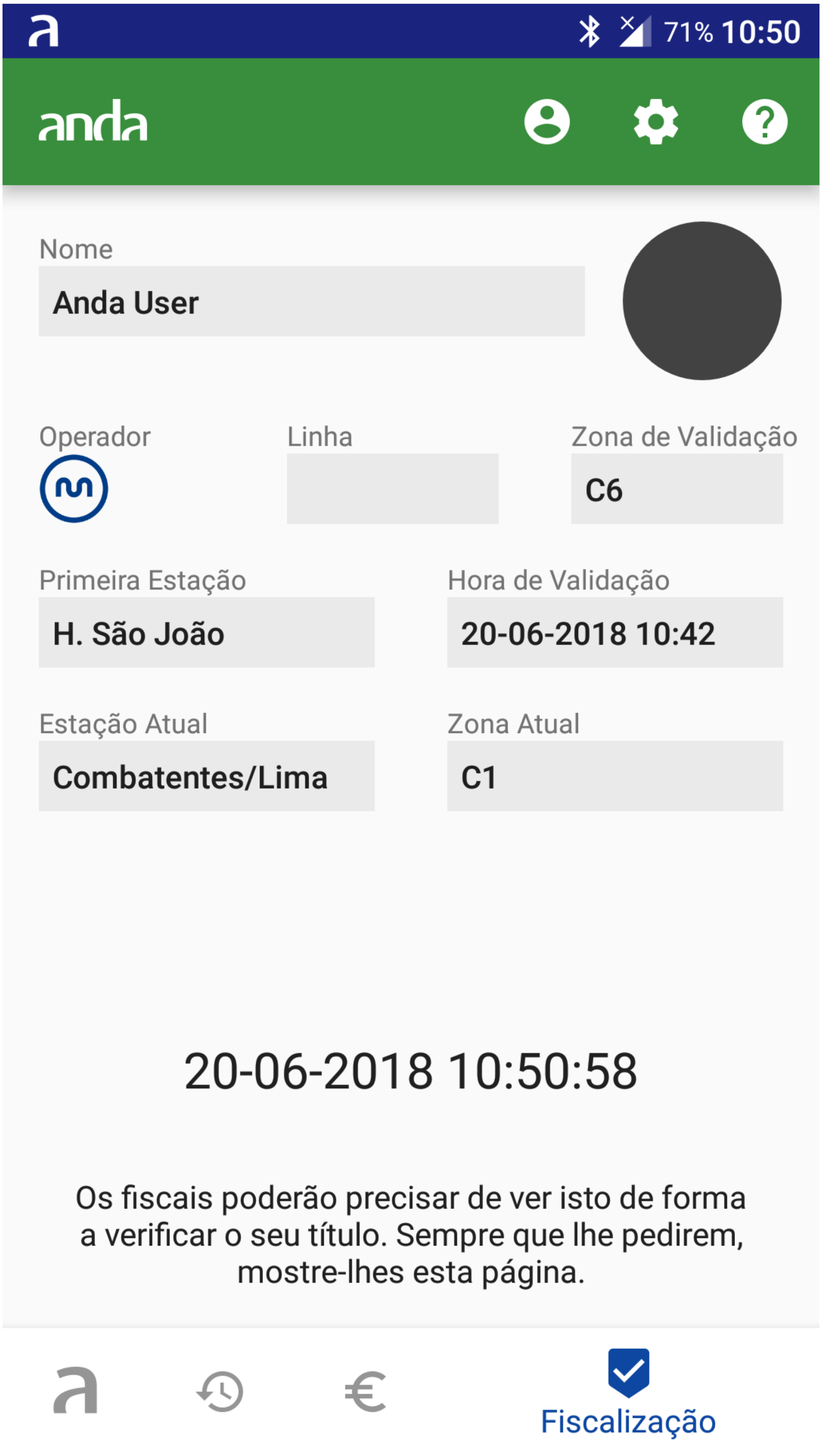


Figure 3.9: Control screen

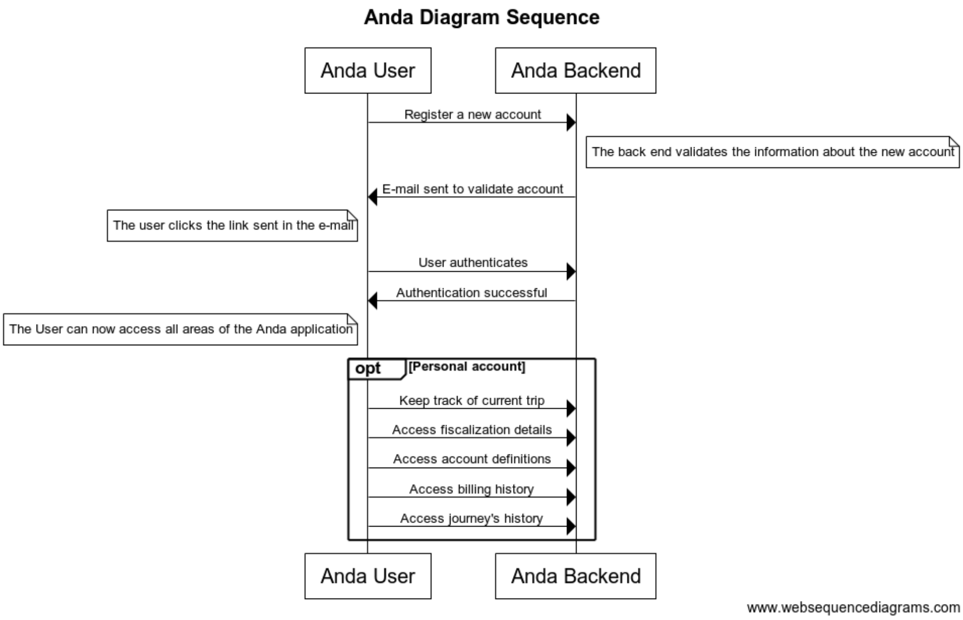


Figure 3.10: The Anda system sequence diagram

Chapter 4

The monitoring system

For a better performance of the Anda system, the ad-hoc approach to problems as they occur is not the most appropriate. Collecting different types of data, known errors and known solutions and display it in a user-friendly capacity may help the process of solving new problems and automate the whole testing system. A dashboard, available through a web browser, is accessible by any operative system and, being user-friendly, is usable by any person who uses it. This monitoring system, in the shape of a dashboard, is the proposed solution to fix and detect Anda's known and unkown issues. This chapter is divided in four main components: architecture, error and data collection, database, web views and automation. Lastly, the testing and evaluation of the solution is addressed.

4.1 Data Collection

Before implementing an online dashboard, there is the need to collect a large number of information. There are currently five data sources to load all of the Anda's relevant material to an external database, which directly feeds the proposed solution.

- A file containing information about the users: This file possesses the name of the user, his e-mail and a UUID (Universal Unique IDentifier). This UUID, "a 128-bit number used to identify information" [UUI18] serves as an identifier for every log that is saved whenever the user shares a report of a situation that happened throughout a travel.
- A file containing the current state of internal database of journeys: This file is updated daily and contains information about the users and their journeys. Regarding the users, it is used to identify any new user that is not present in the previous excel file. Regarding the journeys, the file contains journeys performed by the users registered in a given month, how the journey ended, the time and station the journey started and finished and the operator in which the journey took place.

- File containing information about the users phones: This excel file feeds another subset of the monitoring system that is not directly related to the users, but rather to their phones. It contains each mobile phone specifications, such as operating system, brand, model, manufacturer and Bluetooth version.

- File containing beacons communications: This file is updated daily with information about the BLE beacons being used and active. It contains the serial number to identify each beacon, their last communication date, the operator it belongs to, the station or vehicle it is located in, the intermodal zone and line it operates on, and the number of hits since the beacon went online.

- Logs of the users: These logs are saved whenever a user travels using the Anda system. It contains an internal log of the users' phone developed by an external company, and contains information about BLE signal that is caught, if any, when the travel starts and finishes.

All of this data is collected, refined and sent by an external company by the name of Card4B, one of the companies involved in the development of the Anda system, that is currently developing the Anda system. The information about travels and beacons is fetched daily via the Gmail API [Gma18] and Google Authentication via OAuth2 [Goa18] as it is sent by Card4B through an e-mail. However, the excel files containing information about the Anda users and their smartphones are parsed via "xlsx", a NPM module, which is a "parser and writer for various spreadsheet formats with emphasis on parsing and writing robustness, cross-format feature compatibility with a unified JavaScript representation, and ES3/ES5 browser compatibility back to IE6" [xls18]. This parsing, either via "xslx" and Gmail API, makes it possible for the database to be populated.

4.2 Error collection

The dashboard scans the data mentioned in section 4.1 and detects already known problems. Unknown or new problems need to be reported by users and analyzed by someone with deep knowledge on the Anda system. During the testing of the Anda pilot system, weekly meetings took place at TIP's (Transportes Intermodais do Porto) building. During these meetings, errors reported by the users were discussed, in order to figure out possible causes. In these meetings, the errors and possible causes were collected and then inserted to the dashboard. Status updates were also discussed, which allowed for a global perspective and the implementation of milestones, global statistics and time line in the landing page, as seen in 4.3.3. Currently, there are 8 known errors or misinformation alerts that the dashboard takes into account.

- Not registered ending: This marks an occurrence if the journey ended by an unknown way. Up until this point, it has never happened, but it is checked nonetheless.

- The stations journey's start and end are the same: This is a known problem, but the causes vary immensely. It is only flagged as an occurrence if the journey lasted more than two minutes, to exclude cases in which the user validated by accident or only wanted to test the validators. It generally means that the user's smartphone did not capture any BLE signal that the beacons were emitting or that the application did not enter the state of scanning the BLE beacons.

- No start date and validation date of a journey: Up until now no occurrence like this has been flagged, but it is checked nonetheless.

- The user used the Andante system only: As seen in 3.3 the Anda pilot users use both systems, Andante and Anda. Consequently, if one of the users used the Andante card only, it probably means that he was not able to validate at the station in cause. Users may not validate by lack of time to use the Anda application or simply forgetting. Once again, the causes vary, but it usually means that the NFC antenna is not correctly synchronized in its frequency.

- End of the journey caused by an application crash: This means that the Anda application had an undetected crash and, after the restart done by the operating system, it was the cause of the end of the journey, unintended.

- Ending the journey by exceeding the timeout of the smartphone's Bluetooth disconnection: The journey ended because the user had an ongoing journey and the user's smartphone had the Bluetooth disconnected for more than two minutes straight. This was implemented to prevent fraud from users.

- Ending the journey by exceeding the number of times the user can connect and disconnect the smartphone's Bluetooth: In this case, the journey ended because the user disconnected and connected the smartphone's Bluetooth connection more than ten times. This was also implemented to prevent fraud from users.

- Ending the journey by exceeding the timeout in the first station: This timeout is meant to end a journey in case the user has not caught any BLE beacon signal for more than fifteen minutes (in railroad vehicles) or ten minutes (in road vehicles) straight.

4.3 Architecture

The proposed solution rests on a NodeJS web application, using Handlebars, "an extension to the Mustache templating language created by Chris Wanstrath. It is a logicless templating languages that keep the view and the code separated" [hbs18], as a template engine, Express, a "fast, unopinionated and minimalist web framework" [exp18], as a middleware and MySQL, an open-source relational database management system [MyS18a], for the database. The server has two main responsibilities: 1) daily retrieving all the e-mails and files that populate the database, and 2) feeding the web application. This web application is an interactive dashboard that allows any user to fiddle with different types of information, organize it, compare it and aggregate it. NodeJS and MySQL

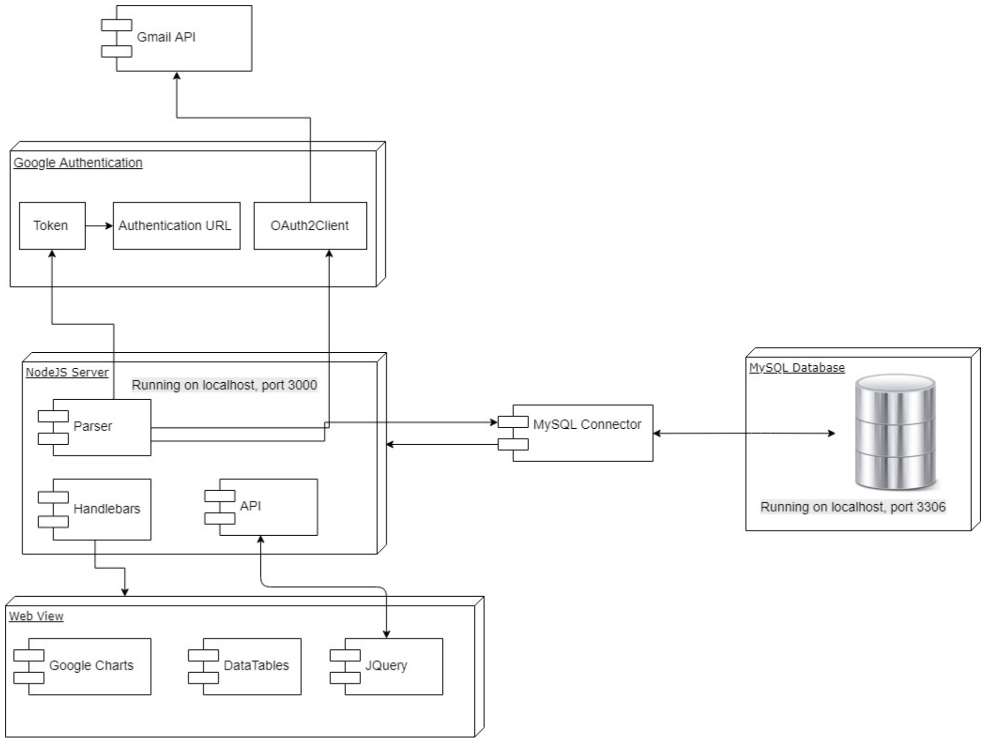


Figure 4.1: Architecture of the dashboard

were used due to their easy setup and because they have vast documentation available online. Angular was considered before a template engine, mostly due to the fact that the dashboard could be implemented as a SPA (Single Page Application) and there were some templates available for free use with multiple functionalities. However, after using it and setting it up, it was apparent that the cost of learning its implementation and documentation was not worth it due to the fact that the dashboard could be implemented using already known technologies, in this case, such as a template engine. This also allowed the whole solution to be contained to a NodeJS project, even though it also acts as a standalone server with daily routines.
MySQL was used as the data pointed to a clear case of a relational database and, considering, for example, PostgreSQL, MySQL and SQLite, MySQL is the one with the most documentation available and most tools to work with and direct integration with NodeJS through "mysql", a NPM module which acts as a driver for mysql, written in JavaScript, not requiring compiling [mys18b]).
Figure 4.1 illustrates the architecture of the proposed solution.

4.3.1 NodeJS Server

The NodeJS server has different levels of functionalities. Firstly, there are some command line calls that can be made to fetch information about the Anda users or their journeys made. These calls take two arguments: a string detailing what operation is related to (Travels or Beacons) and the date of the e-mail. This connects the server to the Gmail API and retrieves the e-mail in the

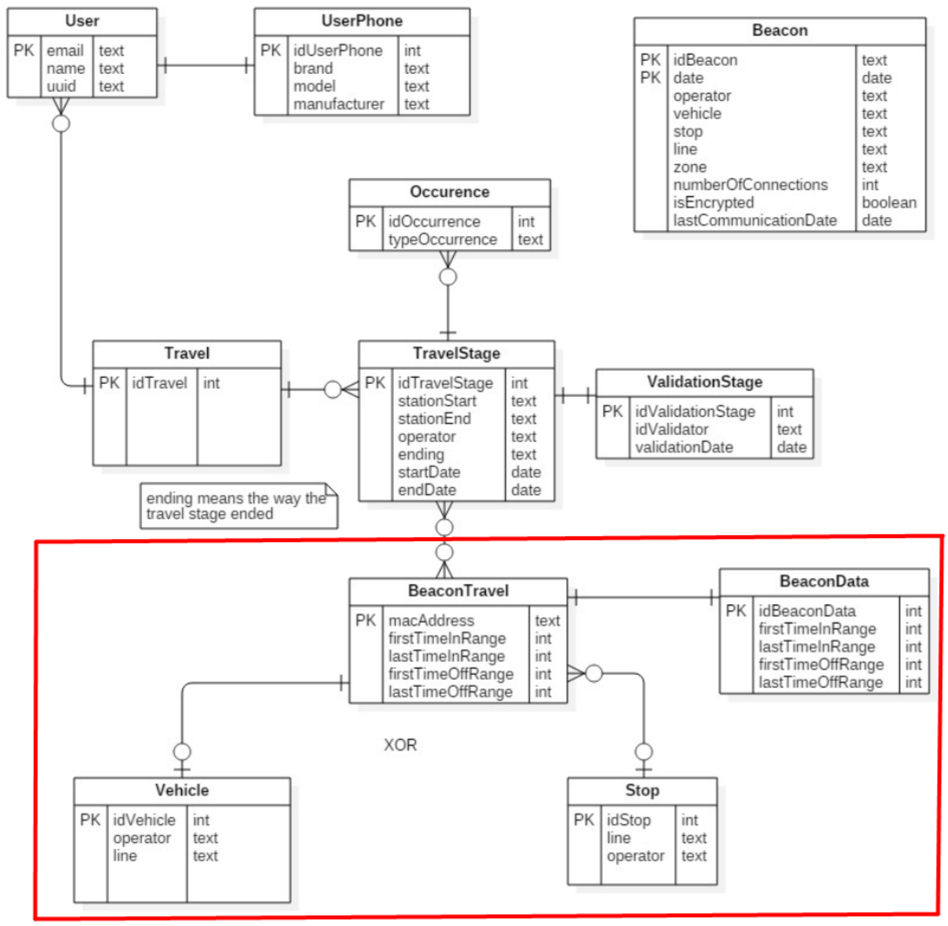


Figure 4.2: ER (Entity Relationship) diagram of the dashboard's database

conditions inserted above, as the structure of the e-mails that are sent daily do not change. Then, the parsing of the e-mail is done taking into account its embedded HTML (HyperText Markup Language). After the correct parsing, the information is inserted into the database, so the dashboard only accesses the database and not the Gmail API, providing faster performance and results. Besides the raw information that is inserted, the server also tries to detect possible errors just by analyzing parameters of the journeys. It scans journeys as occurrences if the type of ending was not registered (it came via e-mail not listed), if the journey started and ended in the same station, if it lasted longer than two minutes and if the user validated with the Andante card and not with the Anda application (meaning the validation was not successful). There are also some endings that signal known occurrences: if the journey ended by a new one at startup, by disconnecting the Bluetooth signal of the smartphone, or if it finished by achieving a timeout. However, this fetching done by command line calls is already automated via a cron job, that is responsible for executing the same call at 15:00 every day.

Secondly, the server opens two types of routes: API routes and web routes. The API routes only return information via JSON (JavaScript Object Notation) Objects and the web routes render web pages to be displayed, via Handlebars.

4.3.2 Database

The database was implemented in MySQL and the ER diagram of it can be observed in Figure 4.2. The diagram is divided in three main groups: users, travels and logs. The User and UserPhone tables belong to the users group. They have the main task of storing data pertained to the Anda pilot users and their smartphones, such as name, e-mail, an UUID that allows the tracking of the smartphone logs, and the brand and model of the smartphone. Afterwards, the travels group subdivides in four distinct tables: Travel, TravelStage, ValidationStage and Occurrence. A travel usually contains multiple travel stages entrances, symbolizing the interchanging of stations that normally occurs in the MAP. This travel table stores information about the station and date in which the journey started and ended, as well as the operator, vehicle and line in which it occurred. Lastly, this table also stores how the Anda system recorded the manner the travel ended. The validation act is stored in a different table, also recording the validator in which the Anda user validated and the date in which it happened. Finally, the table Occurrence stores any occurrences detected by the server, as seen in section 4.3.1.
In Figure 4.2 there are 4 distinct tables inside a red rectangle, that pertains to the last group, the logs. These logs are generated by the users' smartphone and then sent to a back-office database belonging to the Anda system. These logs are currently being sent to a Google account and stored in Google Drive, so it could be stored inside the database. However, after analyzing them thoroughly, the effort to understand, parse and store them would be too complex and time-consuming and the idea was put aside, but the tables in the database were kept in case the idea would be revisited. These logs could potentially detect other flaws, such as beacons not being caught during a specific journey or sudden application crashes.

4.3.3 Web Views

The dashboard accommodates three main web views: the landing page, showcased in Figure 4.3, the beacons' communications, in 4.5 page and the occurrences page, seen in Figure 4.4.

- The landing page is the main web view of the dashboard, enclosing an overview of the entire system, such as the percentage of successful travels and the number of beacons not communicating for over a day. It also possesses a timeline of the Anda system, going through 2014 to late 2018, showcasing important milestones and changes to the system. Finally, two global charts can be seen that detail the manner in which all journeys ended, illustrating the most common endings of users' journeys. Lastly, the second chart shows the number of occurrences since the dashboard's deployment, separated by month.

- The beacons' communications page allows the dashboard user to select a time interval to see the recorded data regarding beacons. Consequently, a "smart" table aggregates all of this information and allows it to be filtered with different intents, such as ordering by the

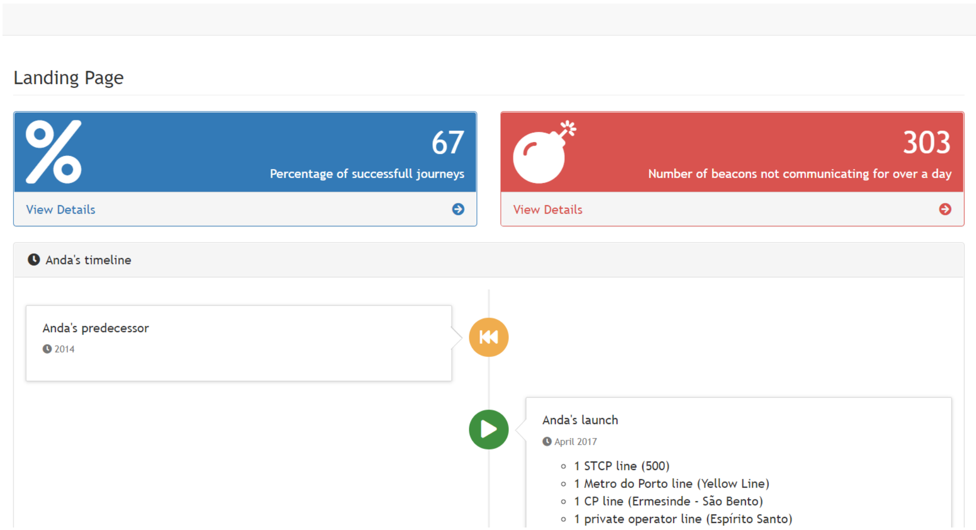
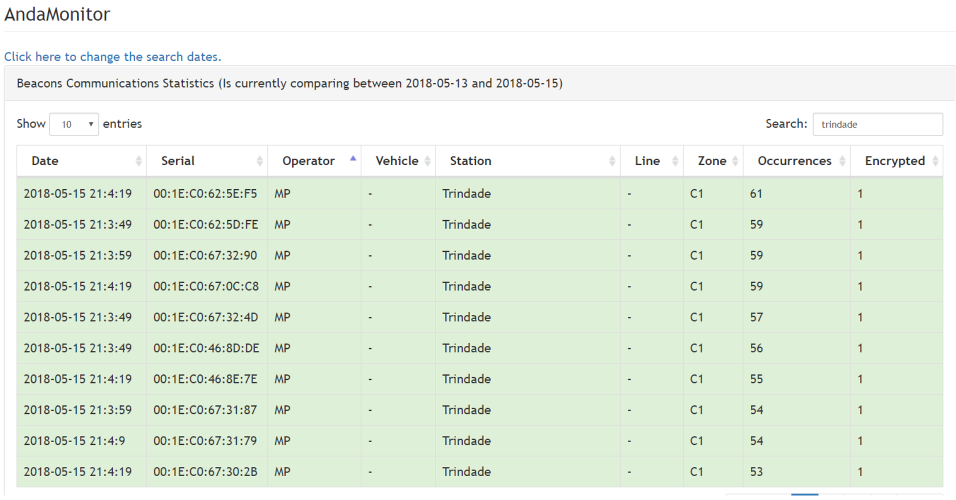


Figure 4.3: The AndaMonitor landing page

beacons' last communication date, its serial number, the operator and line in which the beacon belongs and, finally, the number of hits it got during the chosen time interval. It also allows a search option in any field to quickly detail different beacons and a chosen limit of entries of the table to visualize. Next, a pie chart portrays the percentage of communications of all beacons inside a given station of an operator. Selecting any of the beacons allows the dashboard to present a line chart with the variance of the number of communications it got during each day.

- Just like the beacons' communications page, the occurrences page also allows the dashboard user to choose between two different dates in which to see the recorded data regarding the detected occurrences. There is also a smart table aggregating all the data pertaining to the occurrence, such as the Anda user, his smartphone, details about the journey and why it was flagged as an occurrence. The same filters can be applied, as well as a searching function. Then, a different varieties of charts can be seen, combining different data with different occurrences in order to reveal possible causes. These charts divide the occurrences by the smartphone used, by the station in which the journey initiated and by the Anda user. There is also a column chart that shows the percentage of occurrences detected in relation with the number of journeys concluded in each operator. Afterwards, there are five pivot tables combining the number of occurrences with the smartphone, the start and end station in which the journey happened and the way in which it ended.

The web views are rendered through a template engine, Handlebars, in conjunction with the NodeJS server. Along with it, the design was based on the free bootstrap template: SB Admin 2, a Bootstrap administrator theme, dashboard, or web app UI featuring powerful jQuery plug-ins for extended functionality [sba18], with some posterior alterations. As for the rendering of the tables, a jQuery table plugin was used, DataTables. This plugin is one of the most used by



AndaMonitor

Click here to change the search dates.

Beacons Communications Statistics (Is currently comparing between 2018-05-13 and 2018-05-15)

Show 10 entries Search: trindade

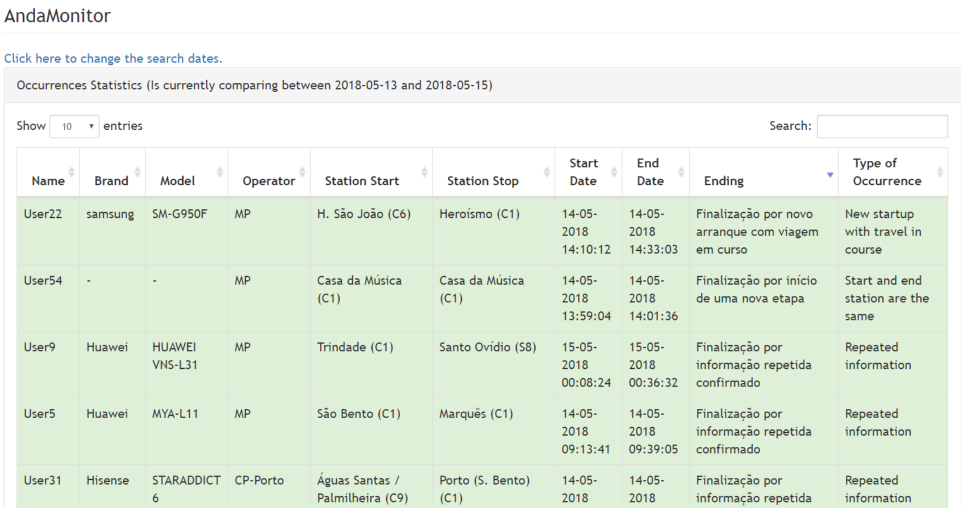
Date	Serial	Operator	Vehicle	Station	Line	Zone	Occurrences	Encrypted
2018-05-15 21:4:19	00:1E:C0:62:5E:F5	MP	-	Trindade	-	C1	61	1
2018-05-15 21:3:49	00:1E:C0:62:5D:FE	MP	-	Trindade	-	C1	59	1
2018-05-15 21:3:59	00:1E:C0:67:32:90	MP	-	Trindade	-	C1	59	1
2018-05-15 21:4:19	00:1E:C0:67:0C:C8	MP	-	Trindade	-	C1	59	1
2018-05-15 21:3:49	00:1E:C0:67:32:4D	MP	-	Trindade	-	C1	57	1
2018-05-15 21:3:49	00:1E:C0:46:8D:DE	MP	-	Trindade	-	C1	56	1
2018-05-15 21:4:19	00:1E:C0:46:8E:7E	MP	-	Trindade	-	C1	55	1
2018-05-15 21:3:59	00:1E:C0:67:31:87	MP	-	Trindade	-	C1	54	1
2018-05-15 21:4:9	00:1E:C0:67:31:79	MP	-	Trindade	-	C1	54	1
2018-05-15 21:4:19	00:1E:C0:67:30:2B	MP	-	Trindade	-	C1	53	1

Figure 4.4: The AndaMonitor beacons' communications page

companies around the globe, such as Adobe, Amazon, SONY, Cisco and Tesla. [dat18] Besides that, it is a jQuery plugin which meant it did not need extra dependencies, besides the source file. PivotTable.js, an open-source JavaScript Pivot Table (also known as Pivot Grid, Pivot Chart, Cross-Tab) implementation with drag'n'drop functionality written by Nicolas Kruchten [piv18], was also used to develop the pivot tables. As for the rendering of the charts, Google Charts [gch18] was the chosen option due to, mostly, the vast availability in terms of types of charts and documentation. Other options were thought out and even implemented, such as Chartist [cha18a] and Chart.js [cha18b], which were far too simplistic. Plotly NodeJS, a graphing library which makes interactive, publication-quality graphs online [plo18], also had many chart options but were not intuitive and D3.js, a JavaScript library for manipulating documents based on data, focusing on data-driven documents [djs18], which was far too complex and not quite the "traditional" charts. Finally, the rest of the design and structure of the dashboard rested upon HTML, CSS (Cascade Style Sheets), Bootstrap as a web framework and Font Awesome as a toolkit of icons and fonts.
To enter the dashboard, the routes opened in the server can be accessed by any modern web browser, with JavaScript enabled. Most of the information to visualize is sent in the rendering of the web view. However, some of it is requested later through the API routes due to user action. These requests are done via jQuery, a fast, small, and feature-rich JavaScript library [jqu18].

4.4 Dashboard

After collecting information of different types, a dashboard can be created and powered by it. The main advantage of a user-friendly dashboard is the ease of use, reducing the burden of associating different types of information mentally. By being able to filter different data with multiple parameters, creating relevant graphics and crossing known problems with probable causes, athe task of solving current problems is much facilitated. Besides what the dashboard user can operate, there



AndaMonitor

Click here to change the search dates.

Occurrences Statistics (Is currently comparing between 2018-05-13 and 2018-05-15)

Show 10 entries Search:

Name	Brand	Model	Operator	Station Start	Station Stop	Start Date	End Date	Ending	Type of Occurrence
User22	samsung	SM-G950F	MP	H. São João (C6)	Heroísmo (C1)	14-05-2018 14:10:12	14-05-2018 14:33:03	Finalização por novo arranque com viagem em curso	New startup with travel in course
User54	-	-	MP	Casa da Música (C1)	Casa da Música (C1)	14-05-2018 13:59:04	14-05-2018 14:01:36	Finalização por início de uma nova etapa	Start and end station are the same
User9	Huawei	HUAWEI VNS-L31	MP	Trindade (C1)	Santo Ovidio (S8)	15-05-2018 00:08:24	15-05-2018 00:36:32	Finalização por informação repetida confirmado	Repeated information
User5	Huawei	MYA-L11	MP	São Bento (C1)	Marquês (C1)	14-05-2018 09:13:41	14-05-2018 09:39:05	Finalização por informação repetida confirmado	Repeated information
User31	Hisense	STARADDICT 6	CP-Porto	Águas Santas / Palmilheira (C9)	Porto (S. Bento) (C1)	14-05-2018	14-05-2018	Finalização por informação repetida	Repeated information

Figure 4.5: The AndaMonitor occurrences page

are also tasks that are already automated and need no inputs or attention. A sequence diagram of the dashboard can be analyzed in Figure 4.6.

4.4.1 Automation

The automation process is achieved as all of the received information is parsed and inserted into a database, allowing easy and simple data manipulation. Even known different types of errors are taken into account and stored, to be cross-checked at a later time. However, there are some processes that are not completely automated, mostly due to technological limitations. During the first few months of the development of the dashboard, the e-mails Card4B sent were not very big in terms of size but, as the number of users increased, so did the travels and, at some point, the information stopped being sent in the body of the e-mail, being sent instead in an attachment. Consequently, the parsing had to be changed and some errors surfaced. The e-mails were parsed, at that time, by their HTML and their unique ID's. After that change, the ID's stopped being unique and so, wrong information was being parsed. To indicate to the server what was the right information, the HTML of the e-mail needs to be changed every time it is read by the server, in order to indicate what is the right information to be read. This change is, currently, manual, and not automated. This only compasses the e-mail detailing the journeys made during a month, as the beacons e-mail is not big enough, so, is currently sent in the body of the e-mail.
Besides that, even though the beacons' communication information is processed daily via a cron job, as seen in section 4.3.1, the journey's information needs a manual process, calling a JavaScript file with certain parameters via terminal line. The reason for this is the fact that the Gmail API has some bugs in its query, which, when trying to retrieve a certain e-mail, would not return the one expected. In order to fix this behaviour, date limits were given in the search and the correct e-mails started being retrieved. However, as the e-mail containing the information about

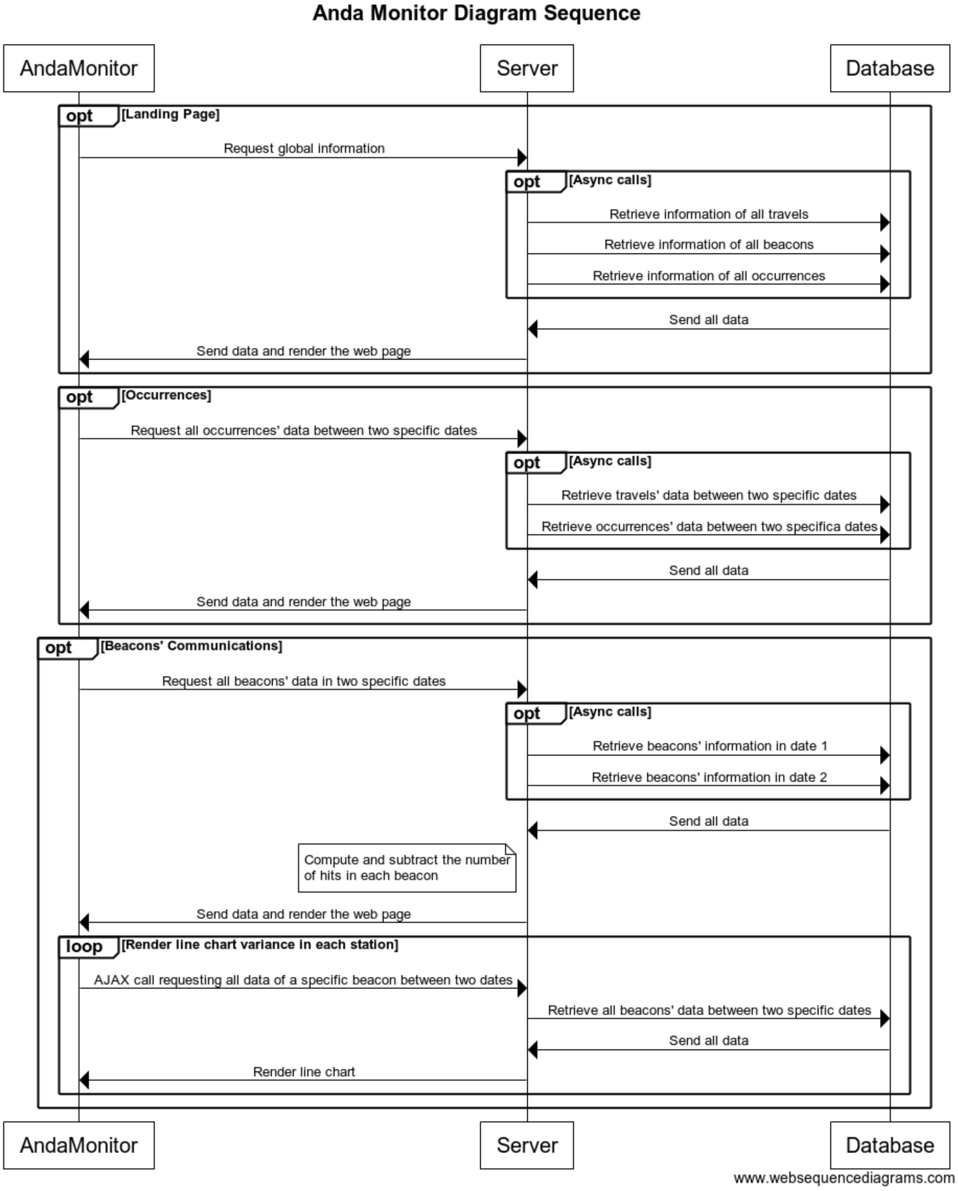


Figure 4.6: The AndaMonitor system sequence diagram

the journeys is not sent exactly at the same date every month, this process is manual. All these details and specifications are explained in Figure 4.7.

4.4.2 Deployment

The deployment of the proposed solution was not fully achieved, but it was thought out. In a testing environment, the server would be uploaded to Heroku, a platform as a service (PaaS) that enables developers to build, run, and operate applications entirely in the cloud [Her18]. However, this platform does not of yet support MySQL integrations and as such, the solution could follow one of two ways: either rent a droplet via Digital Ocean, a easy-to-use cloud computing platform

of virtual servers (Droplets) and object storage (Spaces) [dig18], or migrate the database and its connections to Firebase, Google's mobile platform. Besides this, Heroku also provides a domain name, which facilitates the sharing of the dashboard by eliminating the need to access it via IP (Internet Protocol) address.
Nevertheless, considering that the dashboard would go in a production environment, besides the changes mentioned above, others would have to be made. At the moment, most of the information that is sent by Card4B, as seen in section 4.1, is bound to a personal account, and so do the API keys, authentication accesses and even the information that is sent daily. Thus, this account would also have to be changed to a different one.

4.5 Testing and Evaluation

To validate the solution, the system needs to be used and the data it shows must be significant and enlightening, in order to help solving the issue at hand. The solution should also be able to detect beacons and validators that are malfunctioning or not responding. At the moment, the dashboard can detect malfunctioning beacons but not validators due to external difficulties. Furthermore, the solution facilitates data aggregation and does more than just error checking and seeking, providing useful statistics, such as which cell phones are more prone to errors (and which are not), percentage of successful journeys, which public transport operators are the less prone for errors, for example. Even though it was planned to be mainly a tool to scan problems, it evolved to other areas, such as data analysis and statistics. On account of all of this, all tests and evaluations are not automated and there is no test or function that evaluates the dashboard. This evaluation and testing can only be hand made, preferably by people that are, since the beginning of the deployment of the Anda pilot system, fiddling with comments and suggestions given by the Anda users. For this purpose, a meeting was planned with people which accompanied the process since the beginning. In this meeting, evidenced in figure 4.8, the dashboard was presented and its advantages and usefulness were praised. Errors in the data were also found and flaws in technological areas were discussed, such as the poor usage of the pivot tables and limitations of the information sources itself. It was suggested that the usage of application logs would highly value the monitoring dashboard and that some occurrences may not be occurrences. In conclusion, the reaction was overall positive as a proof of concept that there is the prominent need to monitor a system that has as many details and nuances. It was also acknowledged that it would be useful to work with it as a back-office tool to accompany the state of the Anda system. As for technological testing, there is unit and integration testing, with a 73% test coverage. This tests were run in a completely separated environment, as a different schema and user was created with different access privileges, which means the tests ran can not interfere with the database that is in production. Better results were not possible due to some functions being used one time only, such as Google authentication services to obtain client id and secret or access token and refresh token, and the branch coverage was not always possible, as most of the branches are for error checking. To implement this testing, the chosen tool was Mocha, a feature-rich JavaScript test framework running on NodeJS and in the browser, making asynchronous testing simple. Also, Mocha tests run serially, allowing for flexible and accurate reporting, while mapping uncaught exceptions to the correct test cases [moc18]. Mocha was chosen due to the fact that it is, at the moment, the best test framework to deal with asynchronous tests using promises and the information about the test it shows, such as the duration, number of tests passed and failed and integration with Istanbul. Istanbul is a JavaScript code coverage tool written in JavaScript [ist18], featuring statement, branch and function coverage. Furthermore, Istanbul generates an HTML website where anyone can visualize the details about the test coverage and which lines, functions and statements are not covered, navigating between directories and files. More details about the test coverage of the dashboard can be seen in Figure 4.9.

Lastly, there is generated documentation for all of the code developed, in order for the project to be easily maintained in the future. This generation is made possible using JSDoc 3, an API documentation generator for JavaScript, similar to Javadoc or phpDocumentor. The JSDoc tool will scan the source code and generate an HTML documentation website [jsd18]. This also means all functions and routes are properly documented and commented.

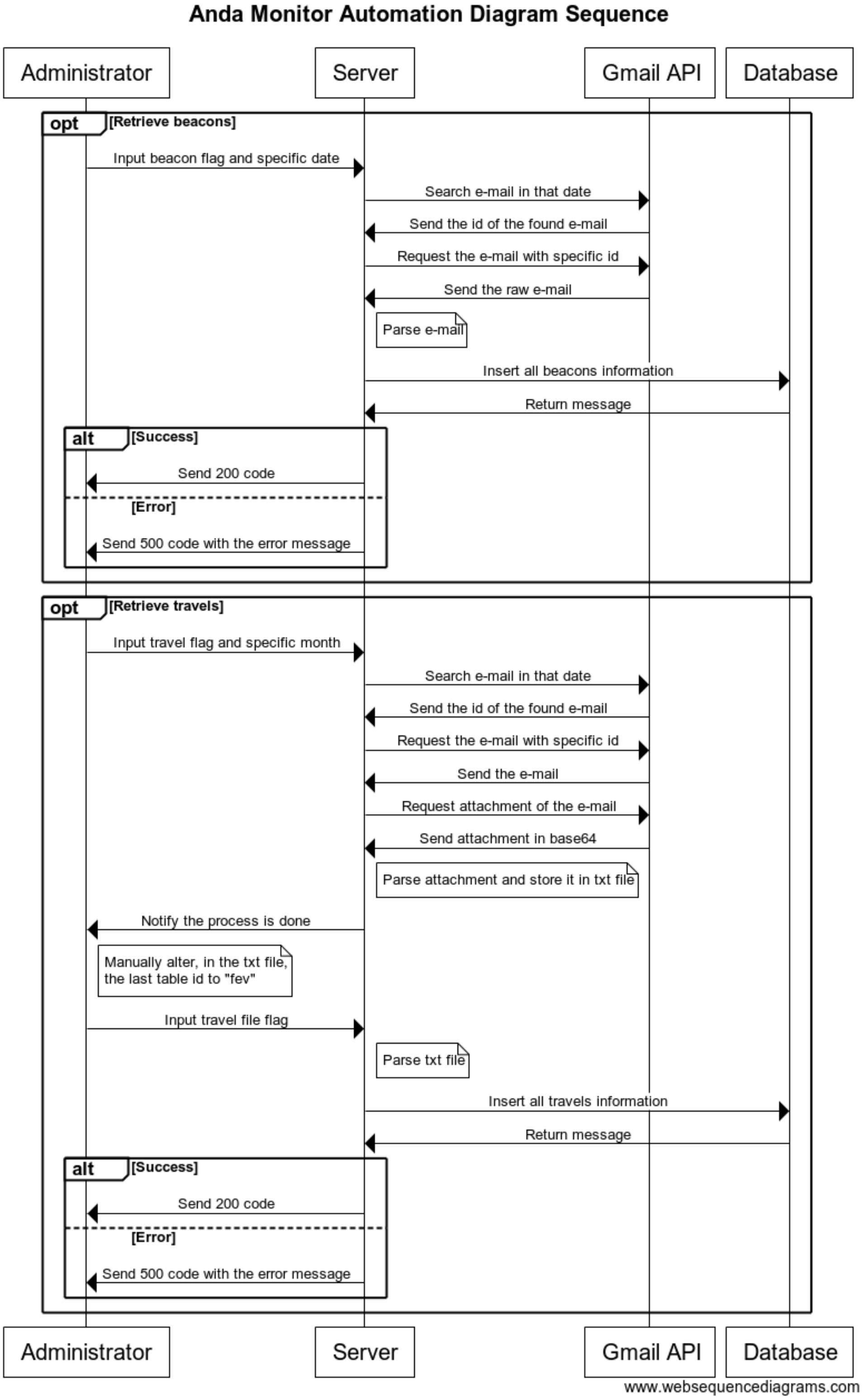


Figure 4.7: The AndaMonitor automation sequence diagram

Figure 4.8: Meeting for qualitative evaluation

73.27% Statements 381/520 **62.45%** Branches 148/237 **88.89%** Functions 32/36 **76.24%** Lines 369/484

File		Statements		Branches		Functions		Lines	
database.js		65.48%	184/281	50.71%	71/140	95.24%	20/21	69.26%	178/257
excel.js		100%	20/20	100%	11/11	100%	1/1	100%	20/20
googleAPI.js		54.79%	40/73	36.36%	8/22	66.67%	4/6	58.82%	40/68
utils.js		93.84%	137/146	90.63%	58/64	87.5%	7/8	94.24%	131/139

Figure 4.9: Test coverage of the solution

Chapter 5

Results

The results shown in this chapter will be thoroughly analyzed and external factors will also be considered, as it is important to conjugate both to validate and make sense of all the information collected. This chapter also aims to demonstrate that the proposed solution does not solely focus on errors and display them, but also exposes and puts into display strong points and statistics of the Anda system.

5.1 BLE beacons

BLE beacons are monitored, mainly in a sole web view that focuses on the communications of each beacon in each station. Figure 5.1 showcases an example of a potential problem with the placement of beacons, in the period between the 13th of April of 2018 until the 15th of May of 2018. As shown, the beacon with the id 00:1E:C0:42:10:03 possesses 44% of the scans that occur in the Aliados station, Metro do Porto. When compared, with for example, the beacon with the id 00:1E:C0:67:31:45, there is a clear discrepancy, as in an ideal scenario, all beacons should be scanned the same number of times, approximately. Even though it may signify that the beacons are miss placed, some external factors need to be taken into account before any conclusion is made. The Aliados station is located in a very populated area in which also buses circulate through. For example, any user travelling in a bus and scanning for beacons, besides capturing the intended signal (the bus he is travelling in), will also capture other existent beacons, such as the Aliados station ones. This difference in the number of hits each beacon has may also be explained with the fact that the Aliados station has two sub levels, and the beacons' signal in the lower one are not captured the same amount of times.
Even though the dashboard can point out potential flaws, it can also do the opposite. In Figure 5.2 the same type of chart is observed with very different values. There are only four active beacons and all of them vary between 24 and 26%. In a perfect scenario, all four would have 25% but the results as they are point to a very good scenario in terms of distribution of the signals caught

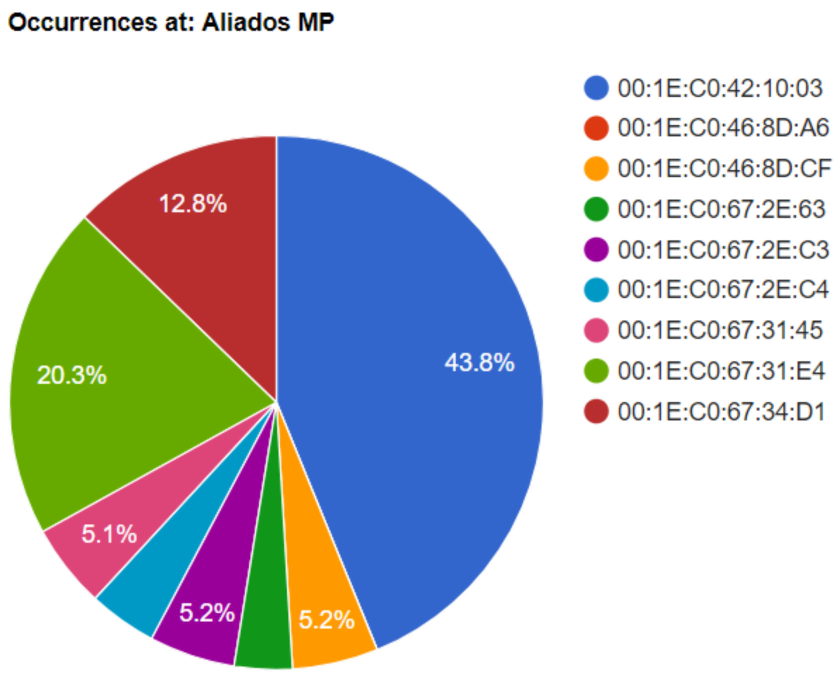


Figure 5.1: The percentage that each beacon is scanned in Aliados, Metro do Porto

by the Anda users. Nonetheless, there are six existent beacons at the Câmara de Gaia station (as seen in the caption of the chart), and only four are active. This is a clear signal that the beacon 00:1E:C0:42:10:D9 and the beacon 00:1E:C0:46:8D:B6 are either malfunctioning, disconnected or badly configured.

5.2 Validators

Validators are not as of yet being monitored, due to technologic limitations. Even though the MySQL database of the dashboard is prepared to host any type of data related to validators, that same data can not be collected at the moment. The only results which could be obtained were the outcome of the manual analysis done to most reports that were submitted by Anda pilot users. Most manifest that the validators have numerous problems when reading the emulated NFC card, as the validators persist on the same errors, as observed in section 3.3. Those errors are still being mended, as most validators are outdated and need to have their antennas either replaced or re-synchronized in their frequency. Besides that, the firmware installed in the validators is legacy and needs to be updated. Nonetheless, there are some validators that have the need to be replaced entirely, mainly in the railroad vehicles, that are as old as 2003.

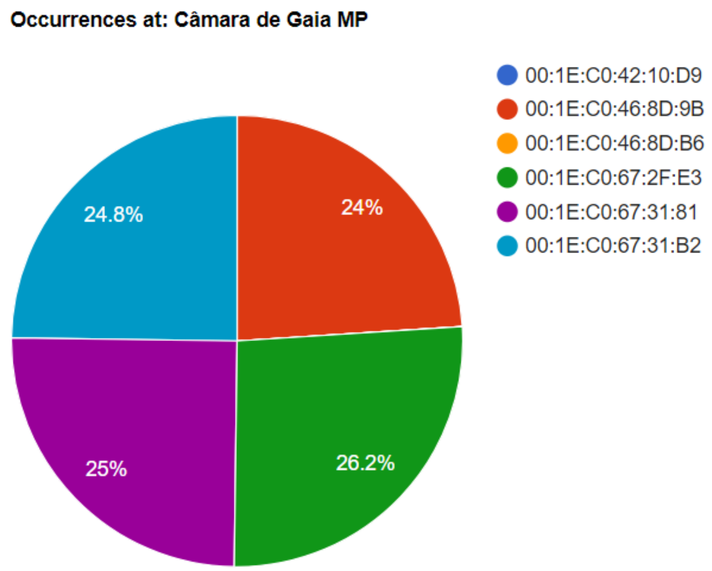


Figure 5.2: The percentage that each beacon is scanned in Câmara de Gaia, Metro do Porto

5.3 Anda system

On one hand, figure 5.3 exhibits the percentage of occurrences in each public transport operator. Metro do Porto contains over half of the flagged occurrences (55%), with Comboios de Portugal and STCP coming second and third with 26 and 13%, respectively. The other three private public transport operators with little over 5% are not relevant enough to be discussed, as they are not tested enough by the Anda pilot users. The fact that it is in percentage shows additional importance as the users tend to report that the operator STCP is the one operator causing the most troubles. However, data does not support that assumption, as Metro do Porto is the one operator with the most occurrences, by far. CP also comes as a surprise but it is also important to notice that, at the moment of analysis, CP did not have all the lines covered and if, any pilot user would visit that line, it would only use the Andante card and the monitoring system would, in turn, flag that action as an occurrence in the assumption that the Anda pilot user did not validate because there were problems with the validators.

On the other hand, figure 5.4 displays the users with the most percentage of occurrences between all users, whose names have been switched to mock ones due to anonimity issues. Besides pointing to some users that may have more problems than others (either due to its smartphone or its incorrect usage, such as not approximating the right distance to the validator or even fiddling with the configurations), it also is a useful feature for a back-office monitoring, as it allows to know which users are having more difficulties with the system and which users have adapted best. Consequently, flaws and anormalities can be picked up by analyzing the worst case users and good methods and techniques can also be discovered by analyzing the best case users.

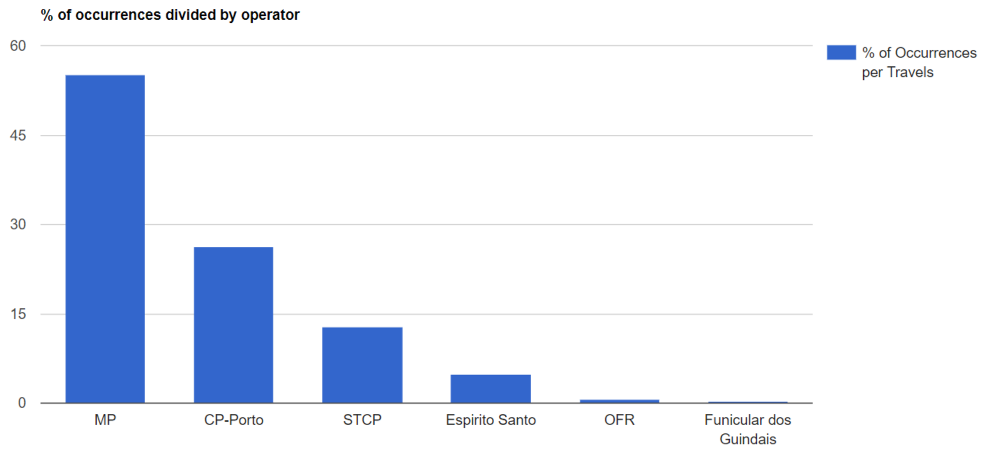


Figure 5.3: The percentage of occurrences in each public transport operator

5.4 Anda users' smartphones

The Anda pilot users' smartphones informations were collected and analyzed, considering the occurrences flagged in each one. Figure 5.5 addresses the percentage of occurrences and this percentage was calculated dividing the number of occurrences detected with each phone brand and dividing by the total number of occurrences. Another approach would be to divide the number of occurrences detected with each phone brand by the total number of journeys done with that same phone's brand. However, the first approach was the one chosen because it demonstrates clearly the success of each smartphone, taking others into account. From this figure, it becomes clear that the ones with the most problems are Samsung, Huawei and Vodafone, with 40%, 28% and 19%, respectively. In spite of that, this chart is not sufficient alone to acess how successful a smartphone is, as noted by the usage of the ZTE, that made only four journeys and recorded four occurrences. In this figure, it is taken as the most succesfull smartphone, when it is clearly not, even though the sample size is small. Sony and Hisense are also in the chart with 5% and 3%, respectively.

5.5 Stations

It is also important to analyze the percentage of occurrences flagged in each station in which all journeys started. As seen in section 5.4, this percentage is also calculated dividing the number of occurrences in each station by the total number of occurrences, as opposed to dividing by the total number of journeys started at that same station. Figure 5.6 shows Trindade at the top of the percentage, with 17%, as opposed to the second station, with 7%. The reason for this is the fact that Trindade is the main starting point for many journeys, as many of the transshipments occur there. Besides that, Trindade is the station in which all of the lines coincide, becoming the main point of entry for most people using the public transportation system. In spite of that, São Bento

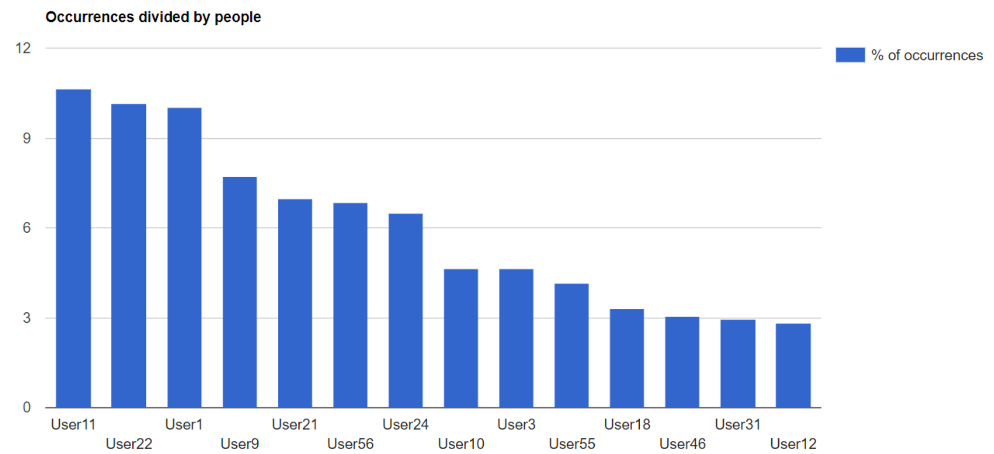


Figure 5.4: The percentage of occurrences divided by person

(CP and MP), Contumil and General Torres fluctuate between 4 and 7%, as these stations are also a point of transshipment between railroad and railway vehicles.

5.6 Automation

The automation of the data collection and error analysis was a vital component of the monitoring dashboard. The main goal was to achieve better and faster results without having the need for someone to execute that some work. This automation was not a process of collecting data directly from each source, but rather collecting different types of information from different sources and analyze them by different parameters. This was mostly achieved via e-mails (as it required the least manual work) and files that could be updated at any time. This process of the automation system was already described in section 4.4.1.

5.7 Statistics

Figure 5.7 demonstrates a clear tendency that people use public transportation vehicles the most during the week, as shown by the peak numbers and rapid decrease during saturdays and sundays. This propensity most likely means that the users of the public transportation system in Porto mainly use the system during work days.

Furthermore, Figure 5.8 showcases a more global view of the Anda system, providing information on the number of beacons that have had no communications for over a day and the percentage of journeys that had no occurrences flagged. Even though three hundred beacons not communicating for over a day may suggest that the beacons are malfunctioning, it is important to take into account that there are, at the moment, seven hundred and fourty seven beacons installed and only sixty six Anda pilot users, which means that most beacons will not be caught due to a lack of testers. Moreover, 67% of success is a very pessimistic number as many occurrences may not be errors and

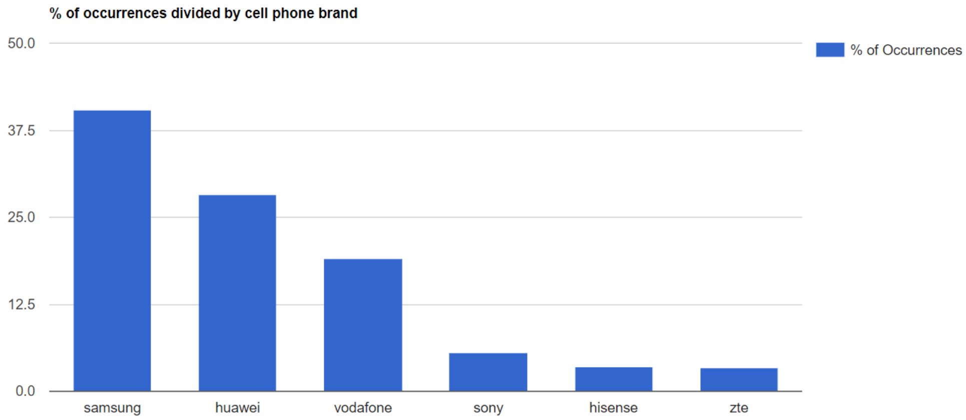


Figure 5.5: The percentage of occurrences in each phone's brand

other occurrences may be flagged wrongly.
Likewise, the dashboard also contemplates statistics for types of endings for all journeys throughout the initial state of development. This statistic, evidenced in Figure 5.9, points to a flaw in the method of terminating a journey. In a perfect system, the Anda application would always terminate any journey by detecting steps. However, the most common ending for a journey is by initiating a new one (as seen in section 3.2.4, it is a normal procedure in the MAP). The second most common ending is unidentified, which means that the Anda pilot user only used the Andante card and not the Anda application. This points to flaws in reading the emulated NFC cards in the validators, as most Anda pilot users will try multiple times to validate their journey with the application when errors occur. Other endings can also be observed in Figure 5.9, as detecting steps and timeouts. Concluding, when observing the different types of endings, it is clear that there are still journeys terminating in unusual ways, either by timeouts or crashes, and there is a great number of journeys in which the Anda pilot user could not validate using the application.
From February to April, the number of occurrences flagged maintain mostly constant (around 500 occurrences per month). It is an unusual high number, but when considering that, for example, four hundred and twenty seven occurrences out of five hundred and sixty two were flagged as occurrences because the Anda pilot user only used the Andante card, meaning that he most likely could not validate. All things considered, when taking into account the other occurrences, the system functions at an acceptable rate. In spite of that, the month of May has a sudden increase due to external factors. In that month, there was an opening of the Anda pilot system to a broader audience (thirty people were added to the pilot) and there are three Anda pilot users that work for Via Porto, a company associated with TIP, and Metro do Porto and Linha Andante (the client support line of the Andante). These users tend to use the system a lot and test it directly, cancelling and starting new journeys a great number of times, opposed to "normal" users, who travel only their normal routes.

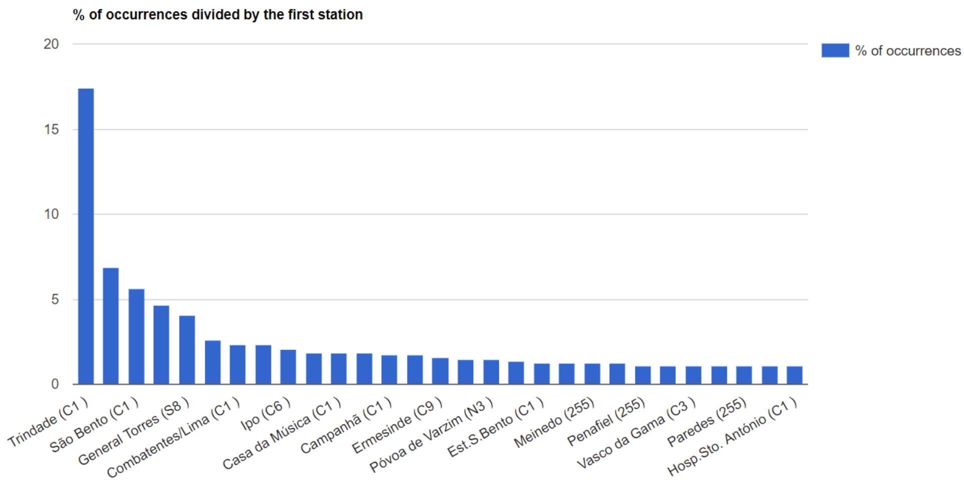


Figure 5.6: The percentage of occurrences in each station the journey started

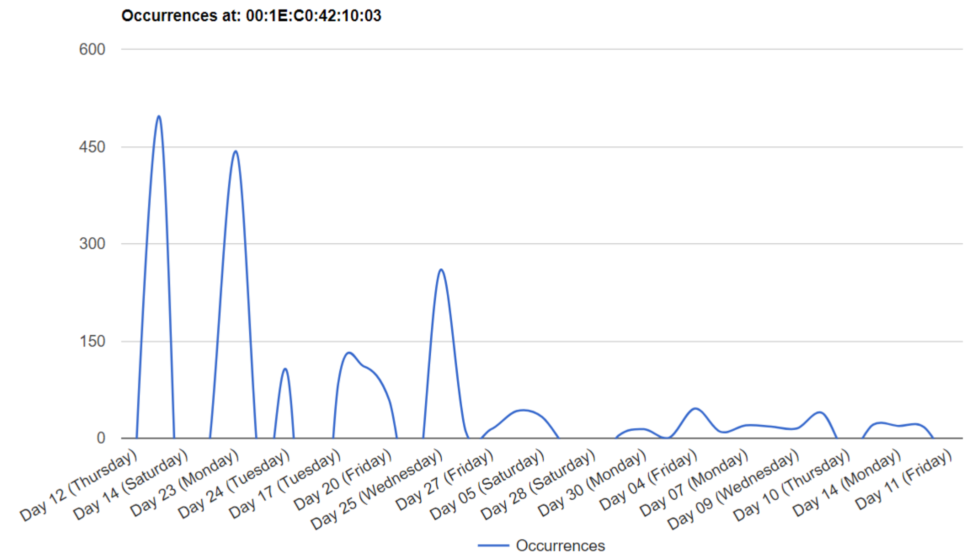


Figure 5.7: The number of hits throughout a month in beacon 00:1E:C0:42:10:03

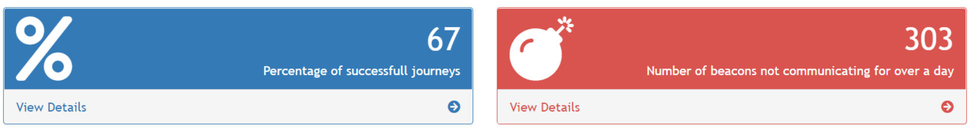


Figure 5.8: Global statistics until 2018-05-31

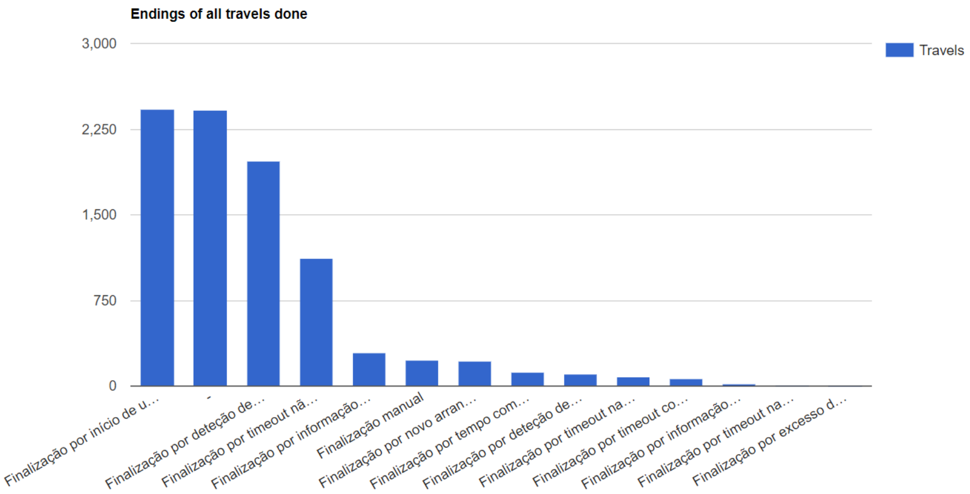


Figure 5.9: Types of different endings of journeys until 2018-05-31

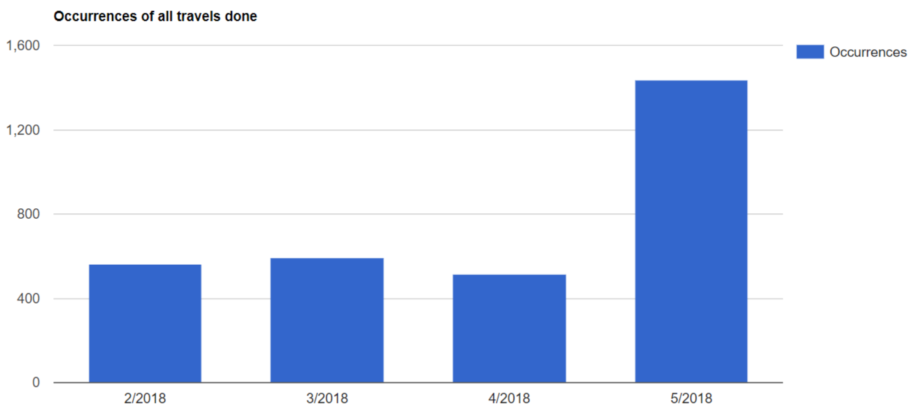


Figure 5.10: The number of occurrences divided by month until 2018-05-31

Chapter 6

Conclusions

Throughout the development of this dissertation, a detailed and thorough analysis of the Anda system was accomplished. This, in turn, allowed for the creation of an interactive dashboard that helps finding and mitigating known errors, as well as undetected ones. This dashboard allowed to visualize which public transport operators were more prone to either success or error, in addition to their respective stations and vehicles. Some beacons may be inadequately located in certain areas, as shown in 4, or even poorly configured. Moving away from the Anda system and into the users' equipment, it was also detected that, perhaps, some errors occurred due to inefficient and low performance smartphones.

This dissertation is a proof of concept that there is the need to monitor any mobile ticketing system, not only to fix and correct errors, but also to discover its strengths. Other results can be deduced by the monitoring system such as the most busiest hours, the least travelled routes, the smartphones with the most success or even plan preventive maintenances for known error prone validators and beacons.

6.1 Future Work

The proposed solution in the shape of a dashboard has room for growth. As discussed in 4, validators' data is not being collected which, consequently, does not allow to collect and identify different types of errors during the validation stage. Besides that, the logs of the Anda application are being stored but not used and parsed, which would prove invaluable to discover which beacons' signal are not being captured during any journey's length. Additionally, by combining the data extracted from the applications logs and the topology of the MAP network, other results could be obtained, such as how much time each journey lasts and should last, theoretically. Furthermore, in order for the dashboard to evolve with the Anda system without requiring major changes, it could be included a space for any administrator using the dashboard to add new parameters to flag new occurrences.

Lastly, the biggest improvement would be to change the entirety of the information collection and the way it is processed. In order to be a completely real-time solution, devices could be installed in each vehicle and station that would be, theoretically, capturing the beacons' signals constantly. This data could then be relayed to the dashboard's database and stored there, allowing the dashboard to flag which beacons were malfunctioning in a short time interval. Furthermore, the e-mails sent by Card4B contain processed information from the users' journeys. This may not be the ideal solution, as the raw information may contain details that could be used to feed the dashboard. Lastly, this data that is collected, processed and then sent, could be obtained directly from each smartphone using the Anda application.

References

[ACFM12] Marinos Argyrou, Matt Calder, Arsham Farshad, and Mahesh K Marina. Understanding Energy Consumption of UHF RFID Readers for Mobile Phone Sensing Applications. 2012.

[Ald18] Zigor Aldama. Going cash free: why china is light years ahead in the online payment revolution. Available at http://www.scmp.com/magazines/post-magazine/long-reads/article/2110118/going-cash-free-why-china-light-years-ahead, last accessed 7th February 2018, 2018.

[All18] Wi-Fi Alliance. Wi-fi alliance® introduces security enhancements. Available at https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements, last accessed 4th February 2018, 2018.

[And18a] Andante: Assinaturas. Available at http://www.linhandante.com/assinaturas.asp, last accessed 7th February 2018, 2018.

[And18b] Andante: Cartões. Available at http://www.linhandante.com/cartoes.asp, last accessed 7th February 2018, 2018.

[And18c] Andante: Como se usa. Available at http://www.linhandante.com/comoseusa.asp, last accessed 7th February 2018, 2018.

[And18d] Andante: Linhas e operadores. Available at http://www.linhandante.com/linhas.asp, last accessed 7th February 2018, 2018.

[And18e] Andante: Ocasionais. Available at http://www.linhandante.com/ocasionais.asp, last accessed 7th February 2018, 2018.

[And18f] Tarifário intermodal andante: Novos preços 2018. Available at http://www.linhandante.com/noticias-det.asp?noticiaid=139, last accessed 7th February 2018, 2018.

[And18g] Vem aí o andante no telemóvel. Available at http://www.linhandante.com/noticias-det.asp?noticiaid=141, last accessed 8th February 2018, 2018.

[AP10] Sanjay Ahuja and Pavan Potti. An introduction to rfid technology. *Communications and Network , 2010, 2, 183-186*, 2010(August):183–186, 2010.

[ARFY11] Ahmed N Abdalla, Muhammad Rauf, Azhar Fakharuddin, and Xiao Yao. Public transport monitoring with route and dispatch management system. *African Journal of Business Management*, 5(22):9106–9115, 2011.

[Bae16] Drake Baer. This map shows the percentage of people around the world who own smartphones. Available at http://www.businessinsider.com/how-many-people-own-smartphones-around-the-world-2016-2, last accessed 9th February 2018, 2016.

[BC13] Sourangsu Banerji and Rahul Singha Chowdhury. On IEEE 802.11: Wireless Lan Technology. *International Journal of Mobile Network Communications & Telematics*, 3(4):45–64, 2013.

[BGS+05] Stephen Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel Rubin, and Michael Szydlo. Security Analysis of a Cryptographically-Enabled RFID Device. *14th USENIX Security Symposium*, pages 1–15, 2005.

[BH06] Andrea Bittau and Mark Handley. The Final Nail in WEP ' s Coffin. 2006.

[Bha15] Ravikant Sharma Bharti. Reed-Solomon Error Correction. *International Journal of Emerging Research in Management &Technology*, 9359(2):19–22, 2015.

[Bor12] Ravi Borgaonkar. Dirty use of ussd codes in cellular network. Available at https://www.youtube.com/watch?v=Q2-0B04HPhs, last accessed 30th January 2018, 2012.

[Cal18] Energy Use Calculator. Electricity usage of a wi-fi router. Available at http://energyusecalculator.com/electricity_wifirouter.htm, last accessed 4th February 2018, 2018.

[cha18a] Chartist.js: Simple responsive charts. Available at http://gionkunz.github.io/chartist-js/, last accessed 6th June 2018, 2018.

[cha18b] Chart.js: Simple yet flexible javascript charting for designers & developers. Available at http://www.chartjs.org/, last accessed 6th June 2018, 2018.

[Cla11] Sarah Clark. Nfc goes green: New st chips use energy harvesting to replace the need for batteries. Available at https://www.nfcworld.com/2011/11/08/311126/nfc-goes-green-new-st-chips-use-energy-harvesting-to-replace-the-need-for- last accessed 26th January 2018, 2011.

[CLCG15] Rui Couto, João Leal, Pedro Mauricio Costa, and Teresa Galvão. Exploring Ticketing Approaches Using Mobile Technologies: QR Codes, NFC and BLE. *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, 2015-Octob:7–12, 2015.

[Coe18] Abel Coentrão. Andante deve estar disponível no telemóvel já em abril. Available at https://www.publico.pt/2018/01/15/local/noticia/andante-deve-estar-disponivel-no-telemovel-ja-em-abril-1799401, last accessed 8th February 2018, 2018.

[COO13] Vedat Coskun, Busra Ozdenizci, and Kerem Ok. A survey on near field communication (NFC) technology. *Wireless Personal Communications*, 71(3):2259–2294, 2013.

[cor15] coreRFID. Rfid - the risks of interference. Available at http://www.corerfid.com/rfid-technology/technology-issues/rfid-and-interference/, last accessed 26th January 2018, 2015.

[Cor18a] Cubic Corporation. Analytics. Available at https://www.cubic.com/Transportation/Solutions/Analytics, last accessed 4th February 2018, 2018.

[Cor18b] Cubic Corporation. Nextcity™ - building a smarter tomorrow. Available at https://www.cubic.com/Transportation/About-CTS/NextCity, last accessed 4th February 2018, 2018.

[Cor18c] Cubic Corporation. Revenue management. Available at https://www.cubic.com/Transportation/Solutions/Revenue-Management, last accessed 4th February 2018, 2018.

[CPR18] Cp: A empresa. Available at https://www.cp.pt/institucional/pt/empresa, last accessed 7th February 2018, 2018.

[CPV18] Cp: Cultura ferroviária. Available at https://www.cp.pt/institucional/pt/cultura-ferroviaria, last accessed 7th February 2018, 2018.

[dat18] Datatables: Add advanced interaction controls to your html tables the free & easy way. Available at https://datatables.net/, last accessed 6th June 2018, 2018.

[dig18] Digital ocean: Simplicity at scale. Available at https://www.digitalocean.com/, last accessed 6th June 2018, 2018.

[djs18] D3: Data-driven documents. Available at https://d3js.org/, last accessed 6th June 2018, 2018.

[DW03] N. Ferguson D. Whiting, R. Housley. Counter with cbc-mac (ccm). rfc 3610, 2003.

[exp18] Express: Fast, unopinionated, minimalist web framework for node.js. Available at https://expressjs.com/, last accessed 6th June 2018, 2018.

[FHMM12] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical relay attack on contactless transactions by using NFC mobile phones. *Cryptology and Information Security Series*, 8:21–32, 2012.

[FNDC14] Marta Campos Ferreira, Henriqueta Nóvoa, Teresa Galvão Dias, and João Falcão e Cunha. A Proposal for a Public Transport Ticketing Solution based on Customers' Mobile Devices. *Procedia - Social and Behavioral Sciences*, 111:232–241, 2014.

[fS01] International Organization for Standardization. ISO/IEC 14443-3. 2001:58, 2001.

[gch18] Google charts: Interactive charts for browsers and mobile devices. Available at https://developers.google.com/chart/, last accessed 6th June 2018, 2018.

[Gei01] Jim Geier. Overview of the ieee 802.11 standard. Available at http://www.informit.com/articles/article.aspx?p=24411&seqNum=7, last accessed 4th February 2018, 2001.

[Gma18] Gmail api. Available at https://developers.google.com/gmail/api/?hl=pt, last accessed 6th June 2018, 2018.

[Goa18] Using oauth 2.0 to access google apis. Available at https://developers.google.com/identity/protocols/OAuth2, last accessed 6th June 2018, 2018.

[GOP12] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors (Switzerland)*, 12(9):11734–11753, 2012.

[HB06] Ernst Haselsteiner and Klemens Breitfuß. Security in Near Field Communication (NFC) Strengths and Weaknesses. *Semiconductors*, 11(71):71, 2006.

[hbs18] Handlebars. Available at http://handlebarsjs.com/, last accessed 6th June 2018, 2018.

[Her18] Heroku. Available at https://www.heroku.com/, last accessed 1st June 2018, 2018.

[HMHB12] M A Hannan, A M Mustapha, A Hussain, and H Basri. Intelligent Bus Monitoring and Management System. II, 2012.

[HSSB05] Jianyong Huang, Jennifer Seberry, Willy Susilo, and Martin Bunder. Security Analysis of Michael: The IEEE 802.11i Message Integrity Code. *DavidHutchisonTakeoKanadeJosefKittlerJon M.KleinbergFriedemannMatternJohn C.MitchellMoniNaorOscarNierstraszC.Pandu RanganBernhardSteffenMadhuSudanDemetriTerzopoulosDoughTygarMoshe Y.VardiGerhardWeikumLecture Notes in Computer Science0302-97431611-3349*, 3823(Chapter 44):423–432, 2005.

[Inc10] Denso Wave Incorporated. Qr codes features. Available at https://web.archive.org/web/20130129064920/http://www.qrcode.com/en/qrfeature.html, last accessed 30th January 2018, 2010.

[ist18] Istanbul: Javascript test coverage made simple. Available at https://istanbul.js.org/, last accessed 7th June 2018, 2018.

[Jan15] Szymon Janiak. Three ways bluetooth smart technology enables innovation for the internet of things. Available at https://blog.bluetooth.com/three-ways-bluetooth-smart-technology-enables-innovation-for-the-internet-o last accessed 21th January 2018, 2015.

[Jou10] RFID Journal. Does rfid interfere with other devices? Available at http://www.rfidjournal.com/blogs/experts/entry?7518, last accessed 30th January 2018, 2010.

[jqu18] jquery: write less, do more. Available at https://jquery.com/, last accessed 6th June 2018, 2018.

[jsd18] Js doc 3. Available at http://usejsdoc.org/, last accessed 6th June 2018, 2018.

[Jue06] A Juels. \mbox{RFID} security and privacy: a research survey. *IEEE Journal on Selected Areas in Communications (J-SAC)*, 24(2):381–394, 2006.

[KFK+14] Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, and Edgar Weippl. QR code security: A survey of attacks and challenges for usable security. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8533 LNCS:79–90, 2014.

[Ley12] John Leyden. That square qr barcode on the poster? check it's not a sticker. Available at https://www.theregister.co.uk/2012/12/10/qr_code_sticker_scam/, last accessed 30th January 2018, 2012.

[Lud16] David Ludlow. How to extend wi-fi range, increase speed and fix problems. Available at http://www.expertreviews.co.uk/networks/1401371/how-to-extend-wi-fi-range-increase-speed-and-fix-problems/page/0/1, last accessed 4th February 2018, 2016.

[Mal06] Robert Malone. Can rfid invade your privacy? Available at https://www.forbes.com/2006/12/05/privacy-rfid-tags-biz-logistics-cx_rm_1207rfid.html, last accessed 26th January 2018, 2006.

[Mar18] Flavia Martelli. Bluetooth low energy: Wireless sensor networks. Slides Alma Mater Studiorum - Universitá Di Bologna, 2018.

[Mas18a] Global leader in mobile ticketing: Innovator in fare collection. Available at http://www.masabi.com/global-leader-in-mobile-ticketing/, last accessed 4th February 2018, 2018.

[Mas18b] Justride mobility platform: No more waiting in line - justride. Available at http://www.masabi.com/justride-mobile-ticketing/, last accessed 4th February 2018, 2018.

[Mas18c] Masabi awards. Available at http://www.masabi.com/awards/, last accessed 4th February 2018, 2018.

[McD09] Mindi McDowell. Understanding denial-of-service attacks. Available at https://www.us-cert.gov/ncas/tips/ST04-015, last accessed 30th January 2018, 2009.

[Met18a] Metro em números. Available at http://www.metrodoporto.pt/pages/307, last accessed 7th February 2018, 2018.

[Met18b] Metro: História. Available at http://www.metrodoporto.pt/pages/321, last accessed 7th February 2018, 2018.

[Met18c] Novas linhas de metro no porto e em gaia. Available at http://www.metrodoporto.pt/frontoffice/pages/379?news_id=243, last accessed 7th February 2018, 2018.

[moc18] Mocha - the fun, simple, flexible javascript test framework. Available at https://mochajs.org/, last accessed 7th June 2018, 2018.

[MyS18a] Db-engines ranking of relational dbms. Available at https://db-engines.com/en/ranking/relational+dbms, last accessed 6th June 2018, 2018.

[mys18b] Mysql: Npm package. Available at https://www.npmjs.com/package/mysql, last accessed 6th June 2018, 2018.

[NFR16] Wolfgang Narzt, Lukas Furtmüller, and Matthias Rosenthaler. Is bluetooth low energy an alternative to near field communication ? *Journal of Mobile Multimedia*, 1(July), 2016.

[NJT18a] Nj transit: About us. Available at http://www.njtransit.com/tm/tm_servlet.srv?hdnPageAction=CorpInfoTo, last accessed 7th February 2018, 2018.

[NJT18b] Nj transit: Mytix. Available at http://www.njtransit.com/var/var_servlet.srv?hdnPageAction=MobileTicketingTo, last accessed 7th February 2018, 2018.

[Oys18] Tfl oyster app. Available at https://tfl.gov.uk/fares-and-payments/ways-to-pay/tfl-oyster-app#on-this-page-1, last accessed 4th February 2018, 2018.

[Pag13] Pierluigi Paganini. Near field communication (nfc) technology, vulnerabilities and principal attack schema. Available at http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attac last accessed 26th January 2018, 2013.

[Par15] Juno Partanen. History of RFID tags. (February):1–8, 2015.

[piv18] Pivottable.js. Available at https://pivottable.js.org/examples/, last accessed 6th June 2018, 2018.

[plo18] Pivottable.js. Available at https://plot.ly/nodejs/, last accessed 6th June 2018, 2018.

[PM17] João Pedro and Norim Marques. Mobile ticketing using Bluetooth low energy technology. 2017.

[Rya13] Mike Ryan. Bluetooth: With Low Energy Comes Low Security. *Proceedings of the 7th USENIX Conference on Offensive Technologies*, page 4, 2013.

[sba18] Sb admin 2: A bootstrap admin theme, dashboard, or web app ui featuring powerful jquery plugins for extended functionality. Available at https://startbootstrap.com/template-overviews/sb-admin-2/, last accessed 6th June 2018, 2018.

[Sha18a] Shanghai: Public transportation. Available at https://www.tripadvisor.com/Travel-g308272-s303/Shanghai:China:Public.Transportation.html, last accessed 7th February 2018, 2018.

[Sha18b] Shanghai transportation. Available at https://www.travelchinaguide.com/cityguides/shanghai/getting-there.htm, last accessed 7th February 2018, 2018.

[Sma16] List of smart cards. Available at https://en.wikipedia.org/wiki/List_of_smart_cards, last accessed 9th February 2018, 2016.

[Smi14] Suzanne Smiley. Understanding near-field and far-field antennas. Available at https://blog.atlasrfidstore.com/near-field-vs-far-field-rfid-antennas, last accessed 26th January 2018, 2014.

[Smi16] Suzanne Smiley. Active rfid vs. passive rfid: What's the difference?s. Available at https://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid, last accessed 9th February 2018, 2016.

[Soa12] Soandos. How much battery power does near field communication require from a phone? Available at https://superuser.com/questions/452710/how-much-battery-power-does-near-field-communication-require-from-a-ph last accessed 26th January 2018, 2012.

[Soo08] Tan Jin Soon. QR code. *Synthesis Journal 2008*, pages 59–78, 2008.

[SPT18] Shanghai public transportation card. Available at https://www.travelchinaguide.com/cityguides/shanghai/transportation/, last accessed 7th February 2018, 2018.

[STC18a] Stcp: Linhas. Available at http://www.stcp.pt/pt/viajar/linhas/, last accessed 7th February 2018, 2018.

[STC18b] Stcp: Origem. Available at http://www.stcp.pt/pt/institucional/stcp/origem/, last accessed 7th February 2018, 2018.

[Thr13] James Thrasher. Rfid vs. nfc: What's the difference? Available at https://blog.atlasrfidstore.com/rfid-vs-nfc, last accessed 26th January 2018, 2013.

[TIP15] Transportes intermodais do porto. Available at https://www.portaldocidadao.pt/web/transportes-intermodais-do-porto/transportes-intermodais-do-porto, last accessed 26th June 2018, 2015.

[UAS] Prathap Reddy Uday Agarwal, Kunal Patel and Santosh S. AN92584 - Designing for Low Power and Estimating Battery Life for BLE Applications | Cypress Semiconductor. (001).

[UUI18] Uuid: Universally unique identifier. Available at https://en.wikipedia.org/wiki/Universally_unique_identifier, last accessed 6th June 2018, 2018.

[Van17] Mathy Vanhoef. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. *CCS '17 (ACM Conference on Computer and Communications Security)*, pages 1313–1328, 2017.

[Vio03] Bob Violino. Benetton to tag 15 million items. Available at http://www.rfidjournal.com/articles/view?344, last accessed 26th January 2018, 2003.

[Wan06] Roy Want. An introduction to RFID technology. *IEEE Pervasive Computing*, 5(1):25–33, 2006.

[Woo16] Sam Wood. A guide to understanding ticketing for london public transport. Available at https://www.meininger-hotels.com/blog/en/a-guide-to-understanding-ticketing-for-london-public-transport/, last accessed 4th February 2018, 2016.

[xls18] xlsx: Npm package. Available at https://www.npmjs.com/package/xlsx, last accessed 6th June 2018, 2018.

[Zha18] Maggie Zhang. World's largest subway system goes cashless as shanghai metro adopts qr code. Available at http://www.scmp.com/business/companies/article/2129550/shanghai-metro-adopts-qr-mobile-payments-it-goes-cashless, last accessed 7th February 2018, 2018.