



Márcia Filipa Mendes Rocha

WeDoCare: an IoT solution to help vulnerable social groups

Thesis submitted to the University of Coimbra
in compliance with the requirements for the degree of Master in Biomedical Engineering

July 2018



UNIVERSIDADE DE COIMBRA



Márcia Filipa Mendes Rocha

WeDocare: An IoT solution to help vulnerable social groups

Thesis submitted to the
University of Coimbra for the degree of
Master in Biomedical Engineering

Supervisor:
Prof. Dr. Jorge Sá Silva (University of Coimbra)

Coimbra, 2018

This work was developed in collaboration with:



Saúde em Português



Esta cópia da tese é fornecida na condição de que quem a consulta reconhece que os direitos de autor são pertença do autor da tese e que nenhuma citação ou informação obtida a partir dela pode ser publicada sem a referência apropriada.

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognize that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without proper acknowledgement.

Dedication

Dedicated to my parents.

Dedication

Resumo

O relatório anual da APAV mostra um aumento no número de vítimas desde o ano 2015 [1]. Este ano, a Índia foi considerado o país mais perigoso do mundo para mulheres seguido de outros países menos desenvolvidos [2]. Apesar de haver um aumento no número de movimentos que dão voz às mulheres, como o movimento 'me too' que teve início em 2006 para ajudar vítimas de abuso sexual, uma grande parte das mulheres que sofreram violência sexual ou doméstica ainda não reporta a sua situação às autoridades. Há um grande número de alarmes pessoais no mercado, a maior parte deles baseado em botões de pânico. No entanto, nenhum teve muito sucesso no público. No âmbito deste estágio, desenvolvemos uma aplicação que reconhece ataques através de reconhecimento de voz e de gestos e deixa o utilizador ativar um alarme manualmente através de um botão dentro da aplicação. Como resultado, uma mensagem de texto é enviada para a polícia com a localização da vítima.

Resumo

Abstract

The annual report of the Portuguese Association for Victim Support (APAV) shows an increase in the number of victims since the year 2015 [1]. This year, India was considered the most dangerous country in the world for women followed by other less developed countries [2]. Even though there has been a rise in the number of movements that empower women, such as the 'me too' movement started in 2006 to help victims of sexual violence, a big part of women who went through domestic or sexual violence is still not reporting their situations to law enforcement. There is a large number of personal alarm systems in the market, most of them based on panic buttons. Nevertheless, none of them has got widespread acceptance. In the context of this thesis, we developed an application that recognizes an attack through speech and gesture recognition or lets the user trigger it manually by clicking a button inside the application. As a result, a text message is sent to the police with the victim's location.

Abstract

Glossary

APAV Associação Portuguesa de Apoio à Vítima.

API Application Programming Interface.

ART Android Runtime.

BLE Bluetooth Low Energy.

HitL Human-in-the-Loop.

IoT Internet of Things.

MVP Model View Presenter.

ORM Object Relational Mapping.

OS Operative System.

PSP Public Security Police.

VCS Version Control System.

WER Word Error Rate.

WHO World Health Organization.

XML Extensible Markup Language.

Glossary

List of Figures

2.1	Relative distribution of devices per Android system version [21].	7
2.2	GH4000 Handheld GNSS/GSM Tracker [30]	10
3.1	Screenshot from WeDoCare’s Kanban board on Trello.	14
3.2	Scheduling for the first semester in a Gantt chart.	16
3.3	Scheduling for the second semester in a Gantt chart.	17
3.4	Answers to the survey	20
4.1	WeDoCare 1.0 screenshots	26
4.2	First WeDoCare logo.	34
4.3	Final WeDoCare logo.	35
4.4	Animation in WeDoCare	35
4.5	WeDoCare mockups	36
4.6	WeDoCare interface	37
4.7	GreenDAO workflow [49].	38
4.8	SharedPreferences workflow	39
4.9	WeDoCare battery statistics.	45
4.10	Gesture recognition results.	49
4.11	Screenshots of WeDoCare website	50
C.1	Proposed WeDoCare logos	111

List of Figures

List of Tables

2.1	WeDoCare vs. Similar applications.	11
4.1	Requirement priority types.	27
4.2	Database entity.	39
4.3	SharedPreferences Values.	40
4.4	Results of the first battery test.	43
4.5	Results of the keyword recognition system	46
4.6	Results of the speech recognition system: another approach.	47

List of Tables

Contents

Glossary	xi
List of Figures	xiii
List of Tables	xv
1 Introduction	1
1.1 Context	1
1.2 Motivation and purpose of the study	2
1.3 The team	3
1.4 Document structure	4
2 State of the art	5
2.1 Concepts and paradigms	5
2.1.1 Internet of Things	5
2.1.2 Smartphones and context-aware computing	6
2.1.3 Human-in-the-Loop	6
2.2 Android Development	7
2.3 Similar Applications	8
2.3.1 Wearsafe	8
2.3.2 SafeTrek	9
2.3.3 Nimb	9
2.3.4 Guardian Circle	9
2.3.5 Watch over me	9
2.3.6 bSafe	10
2.3.7 Leaf	10
2.3.8 GH4000 Handheld GNSS/GSM Tracker	10
2.3.9 WeDoCare vs. Similar applications	11
3 Approach	13

Contents

3.1	Methodology	13
3.2	Planning	15
3.2.1	First semester	15
3.2.2	Second semester	16
3.3	Partnerships	18
3.3.1	Ergue-te	18
3.3.2	Saúde em Português	21
3.3.3	ISCAC - Coimbra Business School	22
3.3.4	Police	22
4	WeDoCare	23
4.1	Context	23
4.2	WeDoCare 1.0	26
4.3	Project requirements	27
4.3.1	Functional requirements	27
4.3.2	Non-functional requirements	30
4.4	Architecture	31
4.5	Development and Implementation	32
4.5.1	Mobile application	32
4.5.1.1	Technologies/Third party libraries	32
4.5.1.2	Keyword Recognition System	33
4.5.1.3	Logo	34
4.5.1.4	User Interface/User Experience	35
4.5.1.5	Storage	38
4.5.1.6	Version Control	41
4.5.1.7	Distribution	41
4.6	Tests and results	41
4.6.1	Battery life	41
4.6.2	Keyword recognition	45
4.6.3	Gesture detection	48
4.6.4	Website	49
5	Saúde em Português: case study	51
5.1	Risk analysis	51
5.2	Success criteria	53
5.3	Methodology	54
5.4	Legal concerns	54
5.5	Results	55

6 Conclusion	57
6.1 Final Results and future work	57
6.2 Personal consideration	58
Bibliography	61
Appendices	67
A User guide	69
B Anu and Naveen XPRIZE application	79
C Logos	111
D Privacy policy	113

Contents

1

Introduction

1.1 Context

We often hear stories of violence against women on the news. The annual report of the Portuguese Association for Victim Support (APAV) shows an increase in the number of victims since the year 2015. In 2017, the association reported 40928 calls from which 3918 were related to spousal violence. 5036 of victims are female, which translates into a statistic of 14 women being attacked per day [1].

This year, India was considered the most dangerous country in the world for women followed by other less developed countries. According to the the National Family Health Survey of 2015/2016, in India, 30% of the 79729 inquired women have suffered any type of violence since the age of 15, 33% of married women have suffered spousal violence, which includes sexual, physical and emotional abuse. However, only 14% of the victims reported their cases to authorities. In tenth place on the same list are the United States of America [2] [3]. In fact, a study from the World Health Organization (WHO) recognized domestic and sexual violence as a worldwide problem and that women are exposed to a greater risk of violence with romantic partners than with other people. [4]

Even though there has been a rise in the number of movements that empower women, such as the 'me too' movement started in 2006 to help victims of sexual violence [5], a big part of women who went through domestic or sexual violence is still not reporting their situations to law enforcement. The annual report of APAV says that only 46 % of the victims pressed charges against their attackers [1]. In less developed countries, this number is higher. In India, only 14% of women sought help [3].

The numbers that characterize spousal and sexual violence are alarming and it only gets worse knowing that the majority of the victims do not take action against the assailters. The reasons behind this do not vary much. In spousal violence situa-

tions, the aggressor assumes a domineering role in the relationship and has a sense of ownership towards the victim. An intimate partner usually stalks the victim and threatens to humiliate them, often with sharing sexual or violent content online, creating a paralysing dread in the victim that stops them from seeking help [6]. Frequently the victim depends financially on the aggressor and is afraid of losing their provider [7]. In other cases, it is simply because of the shame in assuming themselves as victims.

1.2 Motivation and purpose of the study

There is a large number of personal alarm systems in the market, most of them based on panic buttons. Nevertheless, none of them has got widespread acceptance. We feel that technology has not yet progressed enough towards the safety of sexual and domestic abuse victims, at least for the ones that live in low-wealth conditions.

In the past, the Socialite-LCT group developed WeDoCare as a solution to help refugees. WeDoCare 1.0 was an android native application developed with the purpose of detecting violent attacks through a scream recognition algorithm. The application would send an automated alert with the attack's location to other users nearby with the technology BLE Beacons. At the same time, WeDoCare would also post the same information on the user's Facebook page in order to alert the victim's friends about the situation. This location would be stored in a remote database and would later be shown to other users in a heat map. This way, other users could be informed of potential danger zones in a city. Similarly, the application also let users add helpful locales, such as hospitals and police stations, to that map.

In the beginning of the academic year we entered a social competition that made us think how WeDoCare could be of use to other social minorities. XPRIZE is, as it is defined on its website, "an innovation engine" [8]. It launches big prize competitions to challenge the development of solutions for social problems. We entered Anu & Naveen Women's safety XPRIZE [9] competition, first launched in October 2016 to promote the development of a technology based solution for women's safety that should be low-cost and trigger accurate location alerts for emergency situations. In September 2017, we submitted our application to the contest. The application can be consulted on Appendix A.

Based on the requirements of the Anu and Naveen Jain Women's Safety XPRIZE contest, we proposed both an innovative and fresh solution based on mobile phones, optionally complemented by an unobtrusive, auxiliary device to be attached to ladies' clothes. This solution would help in the detection of attacks against women and in the triggering of help requests - the whole of which would be performed within less than 9 seconds. This small device would have an accelerometer, a barometer and a button, so that these elements can be used for detection. This is particularly important in the case of women, as sometimes they leave their mobile phones in their handbag. This device has another important advantage: it can be hidden from perpetrators, as it would be placed covertly and can detect sudden and unusual movements. Both the mobile phone application and this additional device could generate the alert.

Even though we did not proceed to the next stages of the competition, we partnered with local associations that work with sexual violence victims to develop a new version of WeDoCare, even if it meant going a bit differently than planned in September. The final product is a Human-in-the-Loop (HitL) Android application that recognizes an attack through speech and gesture recognition or lets the user trigger it manually by clicking a button inside the application. As a result, a text message is sent to the police with the victim's location. The system is reliable in detection, alert, communication, dissemination, and actuation and ensures the user privacy at all times, since it does not store any type of personal data in a remote database under any circumstance.

1.3 The team

The research group involved in the current master thesis internship is the Communications and Telematics (CT) group. The CISUC-CT group has a vast experience in the communications area and is currently active in research projects in the areas of the Internet of Things, mobile phone programming, wireless sensor networks, network and systems management, and network security. Professor Jorge Sá Silva is the supervisor of this work and Márcia Rocha is the master thesis intern

Our key partners are Ergue-te [10], Saúde em Português [11] and the Public Security Police (PSP). Ergue-te is a social intervention association that aims to help prostitutes leave their work and find a new project in their lives. These are women who

suffer a high level of violence, not only from their clients but from their bosses and romantic partners as well, which makes them the target audience for WeDoCare. Saúde em Português is a Non Governmental Organization that promotes social and community integration and human rights. We specifically worked with one of its departments that provides assistance and protection to victims of trafficking. These partnerships are described later in this document.

1.4 Document structure

This dissertation is structured in six chapters and each one is, in turn, subdivided into several sections.

The first chapter serves as an introduction for the work presented in the following chapters by informing about the context and motivations for this project. On the second chapter we present the study of state of the art technologies and applications and how WeDoCare compares to them. Some relevant concepts are also explained. The third chapter explains the general approach to solve the problem first presented in the introduction chapter, including methodology, work planning and partnerships. The project itself is described in the following chapters.

On chapter number four we can read about the development of the system, its requirements, technologies and architecture. The tests made to the application are also described here. Chapter five reports the use of WeDoCare in a real scenario. Finally, chapter six is dedicated to final considerations about this work.

2

State of the art

2.1 Concepts and paradigms

2.1.1 Internet of Things

The Internet of Things (IoT) is a communication scenario that envisions a network of objects all interconnected and sensing information from the environment. The term was firstly used by Kevin Ashton to describe a scenario in which objects gather information by themselves. [12]

The objects that the paradigm comprises are desktop and laptop computers, smartphones, sensors, actuators and all the everyday *things* that support wireless communication and allow for smart connectivity. The IoT paradigm takes advantage of the huge amounts of data generated by the mentioned devices by using and processing them to develop a wide range of applications in different areas that can be grouped into four main domains: transportation/logistics domain, healthcare domain, smart environment domain, personal/social domain. [13].

Due to the advances in the miniaturization and portability of technology, it will soon be possible to embed smart connectivity into every trivial device, from a fridge to a lightbulb, allowing for the limit that separates technology from its users to disappear. It will no longer be needed that a human inserts data manually into a computer since the objects will be able to sense that information themselves. The Ericsson company estimated that there will be around 18 billion IoT connected devices by 2022. [14] On the other hand, Gartner shared, in 2013, that there will be 26 billion IoT devices by 2020 [15]. Even though these figures vary greatly, they help have a more clear understanding of the dissemination of the Internet of Things scenario.

Since the smartphone usually accompanies the user everywhere they go, we can make

the most of this device since even the cheapest mobile phones have sensors. The Android platform supports three generic types of sensors that provide data: motion sensors, environmental sensors and position sensors [16]. Not included in these groups are camera, fingerprint sensor, microphone and touch screen [17]. These sensors are already used in millions of Android applications which are, sometimes, connected to other pieces of hardware (a smartwatch or a wristband, for example). In section 2.3 we describe some applications similar to WeDoCare that make use of the sensors present in the mobile phone.

2.1.2 Smartphones and context-aware computing

Mobile phones penetrate many aspects of our day-to-day lives. This is much owed to the progress made in software and hardware development that allowed to transform a device initially created to make phone calls into a smartphone, a mobile phone that can perform many functions of a computer. A smartphone typically has a touchscreen and incorporates many sensors as mentioned in section 2.1.1. There are many applications available for download at the moment that were developed with the purpose of entertaining users, connecting people all over the world in a social network or even assisting users on daily tasks. The smartphone works therefore, as a personal digital assistant.

In order to better assist humans, there has been a recent trend in developing context-aware applications which are systems that provide results based on the execution environment [18]. The environment is perceived through the processing of data collected by sensors. In this project we collect data from the microphone, gyroscope and accelerometer that is later processed in order to detect if the user is being attacked.

2.1.3 Human-in-the-Loop

The HitL paradigm is present in systems that take Humans, their actions and intents into consideration. HitL systems can be classified into three categories, according to Stankovic et al.: (i) systems where humans directly control the system, (ii) systems that monitor humans and take action based on that monitoring and (iii) hybrid, a combination of (i) and (iii) [19]. In any category, the human influences the final output of the system. These systems have become more popular recently and have

applications in automobility, energy management and healthcare [19].

Humans can play two distinct roles in HitL solutions, working as sensors and provide the system with information it cannot infer itself or as actuators, as a response to the system's output.

2.2 Android Development

Android is currently the world's most popular mobile operative system (OS) with 85.9 % of all smartphones sold in 2017 having Android as its OS [20]. It is built on top of the Linux kernel and was designed and is currently being maintained by Google Inc. Google is now preparing the launch of Android's ninth version (Android 9.0 or Android P). However, the most used version is never the most recent since users do not update their phones immediately. This leads to a very fragmented ecosystem, with a high number of old versions of the platform still active. At the present moment, the most used versions are Android Marshmallow (6.0), Android Nougat (7.0, 7.1) and Android Lollipop (5.0, 5.1) [21].

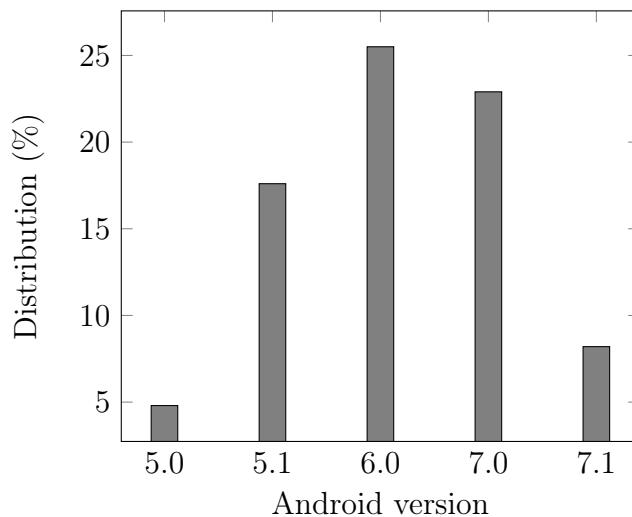


Figure 2.1: Relative distribution of devices per Android system version [21].

With these values in mind, it was decided that WeDoCare would support for versions 5.0 and above.

Even though the OS was first developed to be implemented in smartphones and tablets, there are new versions of Android that allow for the development of applications for other devices. Wear OS was developed, as the name implies, to run on

wearable devices, such as the smartwatch. When connected to the mobile phone, the user can see notifications and messages just by taking a look at the smartwatch. Android TV was introduced in 2014 and it is designed to run on devices with large, high-definition screens - televisions. Both versions of OS were built to let the user control the device remotely through voice commands. There is also Android Things, a version of the operative system built to run in IoT devices.

The latest versions of the OS (since Android 5.0) use the Android Runtime technology (ART) to compile Java and Kotlin code. It allows for better app performance than its predecessor, the Dalvik Virtual Machine, since it compiles the application at install time and not before its execution.

Since Google only controls the software, a high number of companies have built hardware that runs the Android OS. Apple only has eight models available for sale at this moment [22]. Due to a wide choice of mobile phones, it is easier to find a cheaper Android smartphone than an iPhone, which price ranges from €419 for iPhone SE to €1179 for iPhone X.

The Android platform was chosen for this project because it is the most popular, as stated above and because our target group most likely possess an Android smartphone rather than an iOS smartphone due to cost differences.

2.3 Similar Applications

In this section we will describe applications similar to WeDoCare. Some projects below are the semi finalists of the Anu & Naveen Jain Women's Safety XPRIZE [9], a competition that challenges teams to develop a project to help women in India feel safer. In some cases, there is the possibility of integrating additional hardware. Even though this can improve the reliability of the solution, it implies extra costs for the user and, therefore, is not a solution that is within reach of everyone. WeDoCare entered the same competition but was not selected to continue after the first phase of the contest.

2.3.1 Wearsafe

Wearsafe [23] comes as a personal or enterprise solution. Its core is a free mobile application with a button that sends an emergency alert to a group chat previously defined by the user that will coordinate the emergency response. The alert can be

activated through a button inside the application homescreen or by a wearable device which can be both a smartwatch or a Wearsafe Tag, useful for when the smartphone is not within the user's reach. The pairing of such devices with the mobile phone implies a subscription cost. The application features also include audio streaming, location updates and the possibility for friends and family to call emergency services right from the application.

2.3.2 SafeTrek

SafeTrek [24] is a paid mobile application that sends emergency alerts directly to the police. When the user feels scared, they can press a button inside the application homescreen. When safe, the user can simply release the button and enter a pin to confirm their safety. If in danger, the user simply releases the button without entering the pin and their location will be shared with the police. The minimum pricing is \$29.99 per year.

2.3.3 Nimb

Nimb [25] is a personal safety app that optionally pairs with the Nimb Ring, which costs \$249 and is useful for the times when the user cannot reach the phone. The system allows users to send alert to friends, family, nearby users or emergency responders. The option to ask emergency responders for help can be accessed only through a subscription plan that costs at least \$155.88.

2.3.4 Guardian Circle

The Guardian Circle [26] is a free mobile application that works almost as a social network for personal safety. Users can ask their guardians (can be whoever they want, from family to neighbors) for help inside the application. Guardians can then communicate and coordinate an emergency response. When facing an emergency, users have to first select the alert type (emergency, urgent, request or only a test) and can optionally write about what is going on as there is not a quick 'help' button.

2.3.5 Watch over me

Watch Over Me [27] is a freemium application. The application sends emergency alerts to a safety network through push notifications for free. However, since this feature does not work in areas with low connectivity, users can for \$4.99 per year unlock the 'Total safety feature' that sends alerts via SMS. The company covers the

2. State of the art

the cost of those text messages. When the user feels insecure, they can set a timer inside the application so that it can watch over them for a specified amount of time and additionally share details. If the user does not tell the system that they are safe until the timer finishes, their friends will get an alert.

2.3.6 bSafe

bSafe[28] is a mobile application that works without the need of additional hardware. Inside the application, the user can create a safety network of friends with whom to share their location and send emergency alerts by tapping an emergency button. Additional features include a Fake Call and a timer that works the same way as the timer in Watch Over Me described in the previous subsection.

2.3.7 Leaf

Leaf [29] is a wristband with a GPS incorporated that costs \$37 and pairs with the smartphone. It lets the user share live location with guardians in through a mobile application. The wearable has a panic button that lets the user send emergency alerts and shared live location with guardians. It also helps users find safe places like police stations and hospitals. This solution won Anu & Naveen Jain Women's Safety XPRIZE.

2.3.8 GH4000 Handheld GNSS/GSM Tracker



Figure 2.2: GH4000 Handheld GNSS/GSM Tracker [30]

This personal tracker costs 71\$ serves not only for finding the user's location but also for sending alerts and making calls [30]. Ergue-te informed us that this device

is sometimes lent by the portuguese police to domestic violence victims who are still living with their aggressors.

2.3.9 WeDoCare vs. Similar applications

As we can see from the applications above, location sharing is a common feature implemented among them and is also implemented in WeDoCare. Since WeDoCare is an anonymous system, the location of our users will never be shared with other than the police. This 'sharing location with the authorities' feature is only implemented in three of the applications described and is only available when users adhere to a subscription plan. WeDoCare is a totally free application as not only users do not have to pay for extra functionalities as they do not need to buy additional hardware to pair with the application. A further strength of WeDoCare is the possibility of activating an alarm without any wearable device when it is not possible to reach the mobile phone. As already said, WeDoCare can detect an attack through a keyword recognition module.

WeDoCare can be more easily compared with the other mobile applications in the table below.

Application	Anonymity	Location sharing	Cost	Additional hardware	Intelligent attack detection
WeDoCare	Yes	Yes	Free	No	Yes
Wearsafe	No	No	Freemium	Yes	No
SafeTrek	No	Yes	Freemium	No	No
Nimb	No	Yes	Freemium	No	No
Watch Over Me	No	Yes	Freemium	No	No
bSafe	No	Yes	Free	Yes	No
Guardian Circle	No	Yes	Free	No	No
Leaf	No	Yes	Paid	Yes	No

Table 2.1: WeDoCare vs. Similar applications.

WeDoCare shares some features with other applications but it clearly stands out for the privacy it offers. Also, it is the only system capable of detecting violent attacks with a complete 'hands-free' way. Since it is free as well, WeDoCare is in advantage over other solutions when it comes to low-cost and reliable safety applications.

The tracker device described in section 2.3.8 may not go unnoticed by the attackers since it is a piece of additional hardware. Furthermore, there is the risk of the victim forgetting to take it with them. It is also not cheap and, therefore, not accessible to

2. State of the art

people who struggle financially.

3

Approach

Throughout the elaboration of this work, weekly meetings, usually on Mondays, were scheduled together with Professor Jorge Sá Silva which had the purpose of establishing objectives for the following week according to the progress made in the previous one. Everything that was studied and developed would be demonstrated to Professor Jorge Sá Silva who would then evaluate the completed tasks, its strengths and weaknesses, and decide the iterations for the next week accordingly. Weekly meetings were also scheduled with the whole Socialite-LCT group, frequently on Thursdays. In those meetings, everyone would share what they were working on at the time so that all the team members could constructively share their opinion and make suggestions to improve everyone's work.

During the academic year, some meetings were also scheduled with Ergue-te, Saúde em Português and the local police. The objective of these meetings is better explained in section 3.3.

As expected, some artifacts appeared and introduced delays in the completion of tasks. These artifacts were, mainly, defects in the code.

There was an office available at the Department of Informatics Engineering, but everyone had the chance to work remotely and asynchronously, even people working on the same project. In order to make it work, we made use of productivity tools and platforms such as Slack [31] and Skype [32] for communication and Gitlab [33] for project collaboration.

3.1 Methodology

Agile methodologies are based on incremental procedures for continuous delivery of software and have become the golden standard in software development. Instead of

3. Approach

defining a precise and strict plan in the beginning of the project, agile methodologies welcome change over time according to feedback from users or clients [34]. To implement agile software development we used the Kanban [35] framework.

The core of the Kanban framework is the visualization of the workflow in a Kanban board which is itself divided in cards for the allocation of tasks according to their status in the project. This board allows for transparency throughout the whole development since everyone who looks at it can see the state of the project at all times in a highly visual manner.

This framework is very light weight and flexible because it does not require someone in the team to perform pre-defined agile roles, like other agile frameworks do. Such flexibility makes Kanban fit for small teams. In our case, Professor Jorge Sá Silva assumed the role of the Product Owner. The development of the project was assumed by one person only. All the tasks were defined and assigned according to their priorities by Professor Jorge Sá Silva, who could also change their priority at any time, as long as it did not interfere with the ongoing tasks. Kanban has the purpose of minimizing the work in progress, thus, we set the tasks for the week in most realistic way possible. We used Trello [36], a platform for project management, to create our Kanban board and to keep track of our progress. The board is represented on figure 3.1.

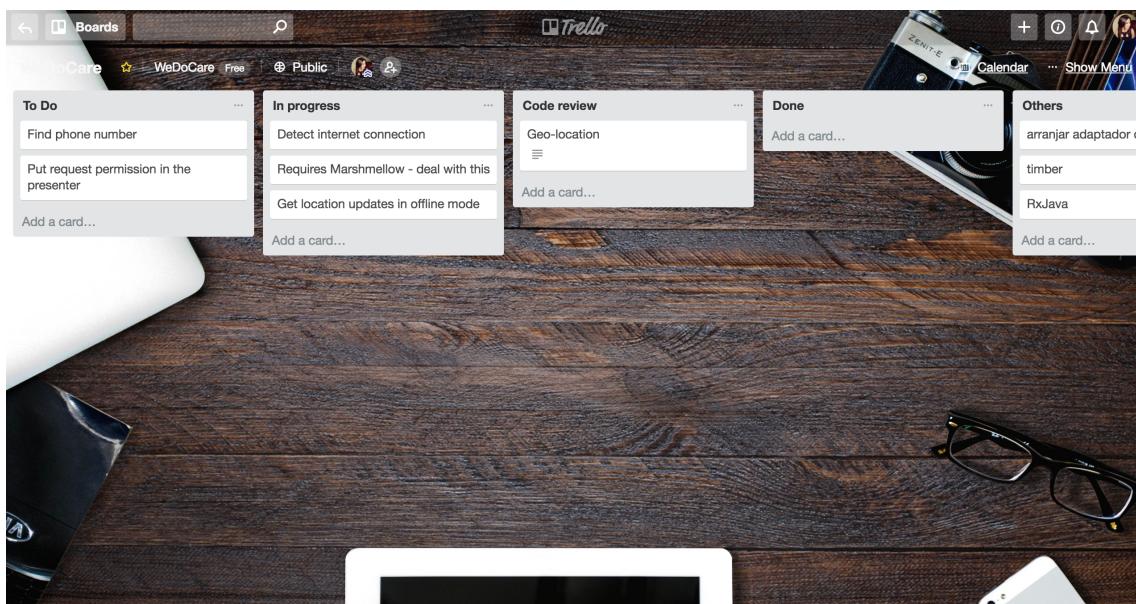


Figure 3.1: Screenshot from WeDoCare's Kanban board on Trello.

There are four cards in this board. In the first three cards, the tasks were organized

in order of highest to lowest priority, from top to bottom. Every time a task was no longer in progress, it was pushed for 'Code Review' and another, the one with highest priority in the "To Do" card, was pulled from the backlog.

To Do The tasks on this card were the ones given by Professor Jorge Sá Silva on Mondays. This card could occasionally include tasks from the previous week or some that were added to the backlog during the week, if something urgent had come up.

In Progress Here were the tasks that were being developed, as the name says.

Code review When a task was no longer in progress, it would be moved to this board for code revision.

Done After revision and bug fixes, the task was considered 'Done' was added to this card. The completed tasks were reviewed with Professor Jorge Sá Silva in our Monday meetings.

Throughout the year and as often as possible, the results would be delivered to our partners so that we could have their feedback on the various stages of the project.

The general planning for the internship is described next.

3.2 Planning

The schedules below were elaborated during the first week of each semester to provide general guidance and help managing the time for each milestone. The plans were not strictly followed since some tasks took longer to complete than initially thought.

3.2.1 First semester

The internship started in September 2017. The first semester was an adaptation period because the methodology adopted was like any other used in previous projects of this course. The technologies applied were also unknown. During these first months, the possibility of two partnerships with local associations arose and together we started to think about new features for a new application. The schedule for the first semestre is represented in figure 3.2.

Study of the State of the Art During these weeks, we studied applications similar to WeDoCare and the key concepts of this study.

3. Approach

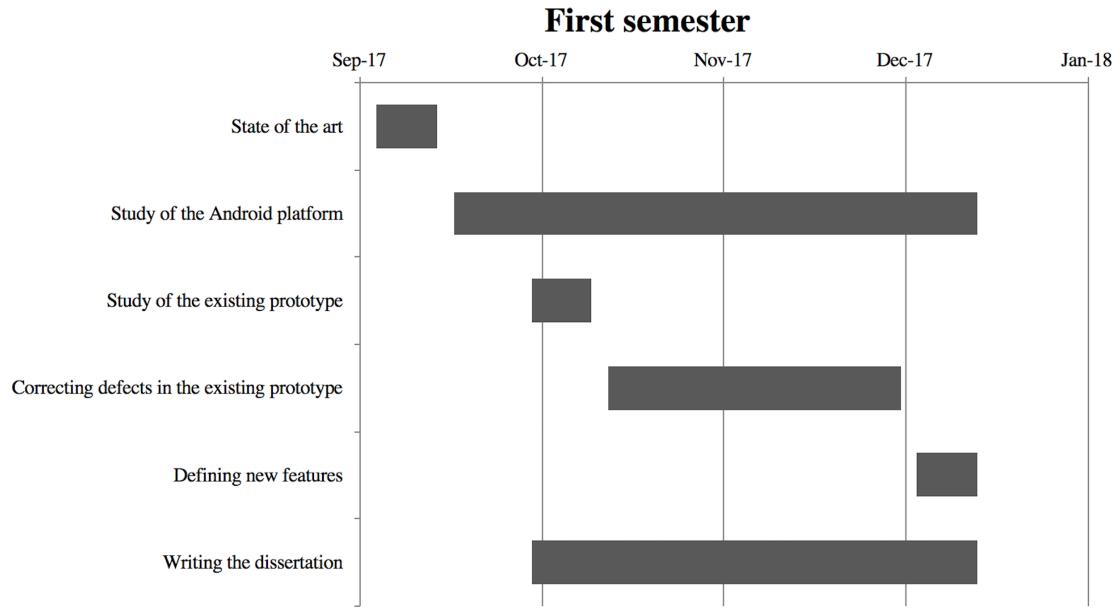


Figure 3.2: Scheduling for the first semester in a Gantt chart.

Study of the Android Platform This task was assigned for the whole semester and included the following subtasks: study of the Android SDK, common code patterns, common libraries and Material design guidelines.

Study of the existing prototype Here we had to familiarize with the existing prototype, WeDoCare 1.0 as studied the Android Platform. Subtasks included the study of technologies used and code structure.

Correction of defects in the existing prototype The application had some defects that were not expected and needed to be fixed.

Deciding new features to be implemented Since the existing prototype was not fit for the problem we wanted to solve, we teamed up with Ergue-te and Saúde em Português during the semester and thought about new features for a new application. During those weeks, we thought about new functionalities and defined the first pre-requirements for WeDoCare 2.0.

3.2.2 Second semester

The second semester was dedicated to the development of the application itself. Throughout these months we continue to meet with our partners so that they could be frequently updated on the project progress and we could have their feedback. The schedule for this semester is represented in figure 3.3.

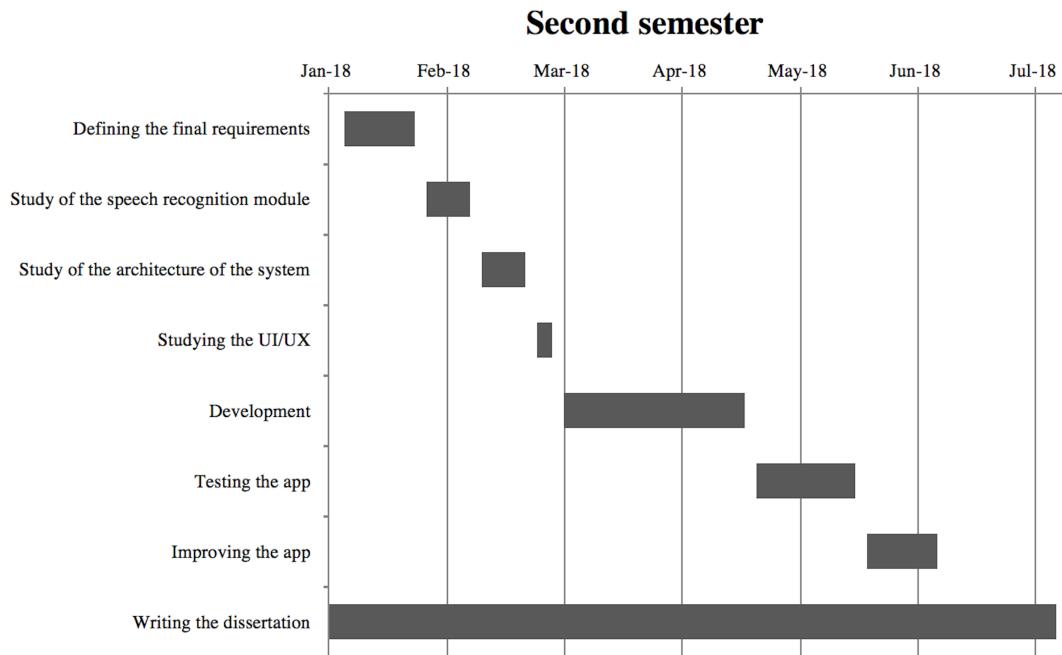


Figure 3.3: Scheduling for the second semester in a Gantt chart.

Defining the final requirements Subtasks here include the definition of functional and non-functional requirements.

Investigation of the speech detection technology In this task we studied and compared various speech recognition solutions available.

Defining the architecture of the system During these weeks we defined the system's main components, its technologies, and the code pattern that would be used.

Study of the user interface Before developing WeDoCare 2.0, we did some mock-ups to create the User Interface.

Development of the new prototype WeDoCare was built from scratch during this task.

Tests WeDoCare was distributed to a restricted group of volunteers. Functional and Battery tests were performed.

Validation with real users WeDoCare was deployed for real users, members of Ergue-te and Saúde em Português.

Improvement Improvement of some functionalities based on the feedback from the real users.

3.3 Partnerships

From the beginning we wanted to validate our project. To accomplish this, we contacted and partnered with Ergue-te, Saúde em Português and the local police. The partnerships and the role they played in the design and development of WeDoCare is better explained in the next sections.

We partnered with Ergue-te and Saúde em Português so that we could be closer with our target audience. We can consider these associations our clients, who had an active voice at every stage of the project. We established contact with Ergue-te first, who were crucial in the requirements definition. In the second semester we liaised with Saúde em Português.

The partnership with ISCAC - Coimbra Business School dates before the start of this internship. Professor Madalena Abreu, coordinator of the Marketing course, and Marta Sequeira, Marketing student investigated how we could organize a crowdfunding campaign for WeDoCare. A crowdfunding campaign is "the practice of obtaining needed funding (as for a new business) by soliciting contributions from a large number of people especially from the online community" [37]. Professor André Rodrigues has a Software Engineering background and followed the whole development of the project.

Over the semestre, we tried to schedule meetings with our partners at least once a month. We would present the evolution of WeDoCare and do a short demonstration of the functionalities implemented at the time, so that everyone could offer constructive criticism and we could improve the application.

3.3.1 Ergue-te

Ergue-te is a social intervention association that aims to help prostitutes leave their work and find a new project in their lives. These are women who suffer a high level of violence, not only from their clients but from their bosses and romantic partners as well, which makes them the target audience for WeDoCare. These women kept their identity anonymous at all times and it was never possible to establish direct contact with them. Consequently, all the meetings were scheduled with the Ergue-te team only.

In October, we established first contact with Ergue-te in order to introduce our project, which was still a solution for the refugee crisis at this point. After contextualizing the application and presenting its features and, the team showed interest in discussing WeDoCare with their associates. In this meeting, it was also possible to trace the victim's profile. These women often live in poor conditions and some of them even came to Portugal through a human trafficking network and have no way to leave the country. The profile of portuguese prostitutes vary. A minority of them have their own apartment to work and have families and friends who are not aware of their job and others are homeless, sometimes with a history of substance abuse and work on the streets. On the other side, all of them have one thing in common: they become very suspicious when it comes to sharing personal information.

In order to get the public's opinion about the product, inquiries with questions related to the system functionalities were handed to sixteen people. WeDoCare was presented as a solution that would recognize an attack and send an emergency alert to someone. The application was described only vaguely to the inquired because we thought it was the best way to know their opinion about features that could be added to the system. The results of this survey came with satisfactory answers. Even though this topic was not in the inquiries, the survey respondents confirmed Ergue-te they have suffered aggressions in the past. When asked if an application like WeDoCare could be useful in those situations, the majority responded positively. It is also important to point out that the answers indicated that the majority of them had an Android phone. When asked about what was important in a risk situation the most outstanding answer was "quick assistance". Other answers include: precise location, audio recording/streaming and police intervention.

The answers to the survey are represented in a chart in figure 3.4.

3. Approach

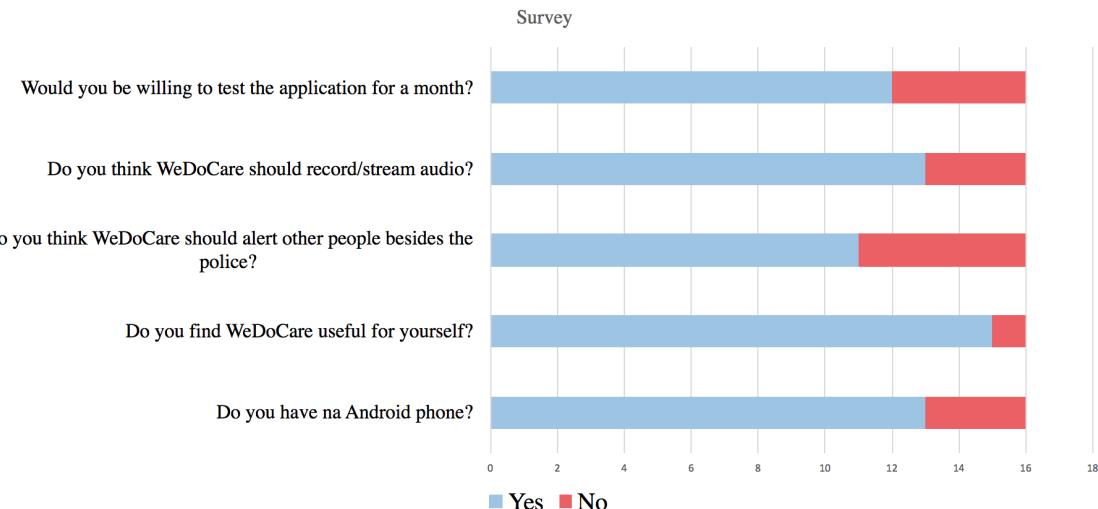


Figure 3.4: Answers to the survey

The results were later discussed in a second meeting. Since we are suggesting a mobile solution, and considering that during the attack the victim can not usually access her phone, we suggested detecting an attack using speech recognition and sending an alert through a notification, like in the first version of the application. However, in this case, violence can occur behind closed doors and sending a notification alert to the people nearby was not efficient enough. In addition, attracting attention to the attack could make the situation worse for the victim. We concluded, at the end, that the fastest way to assist the victim is to alert the authorities (police) directly.

Most of our potential users answered affirmatively the question "Would you be interested in alerting other people besides the police?". Ergue-te members informed us that it is common for the victims to call them for help in those situations. When that happens, Ergue-te members usually prefer to call the police instead of directly go to the location of the attack because they are aware of the danger it would pose to them. We were strongly advised not to implement this functionality at least in the first version of the application.

Some of the women inquired also showed interest in a feature that would record/stream audio. This functionality was also not implemented because not only we wanted to make the first version as simple as possible and focused on developing the necessary features for the victim to get help first, but because, as told by the association, the women would not dare press charges against the attackers unless the police caught them in the act and arrested them immediately and, in this case, it would be useless

to store the audio files.

When finally asked if they were willing to test the such application, some of them answered negatively. This was predictable because, like said before, these women are very suspicious when it comes to sharing information and this causes them to mistrust technology.

After this meeting, we proceeded with the elaboration of the application requirements, set out in section 4.3, which were later reviewed with Ergue-te.

3.3.2 Saúde em Português

Saúde em Português [11] is a Non Governmental Organization that promotes social and community integration and human rights. We specifically worked with one of its departments that provides assistance and protection to victims of trafficking.

Saúde em Português joined us in the second semester and, at this time, the application requirements had already been defined. We contacted this association because we wanted to try and include individuals with a different profile and generalize our target audience that goes from women to individuals who are likely to suffer sexual violence and exploitation. Furthermore, it is safer to assume that a bigger test group implies a bigger number of violence occurrences and that would enable us to draw more valid conclusions.

WeDoCare got a very positive reaction from the organization who showed willingness in collaborating with us immediately. We were told that they work with victims who are mainly men who come from Eastern European countries but can work portuguese victims of slavery as well. No inquiries were distributed to the victims. Instead, the organization took the responsibility of directly communicate with potential users and find if they would eventually be willing to use and test the application.

When we got this confirmation, we had to take in consideration that some of the new users did not understand Portuguese and that WeDoCare would have to be supported in English, Portuguese, Russian, Nepali and Romanian.

3. Approach

3.3.3 ISCAC - Coimbra Business School

Professor André Rodrigues, Professor Madalena Abreu and MSc Student Marta Sequeira were always present at meetings. Professor Madalena and Marta both are very skilled in understanding people's needs due to their Marketing background and were very helpful in providing a different insight on the reality we dealt with. The two of them were responsible for preparing a crowdfunding campaign project that is not yet online. This funding will be put to use in a later stage of the project when the validation is completed.

Professor André worked closely with us during the year and helped developing the application.

3.3.4 Police

Once it was decided that the alert should be sent directly to the authorities, it was clear that the police must be our key partner in this project and therefore we arranged a meeting with the public security police of Coimbra by the end of the first semester. In spite of being receptive to the project, the police expressed their concerns about false positive alarms, which would imply unnecessary mobilization of resources. In fact, in 2016, 75% of all the calls made to 112 did not correspond to emergencies [38], a number that was confirmed by the public security police. If this happened with WeDoCare users, the application would be discredited and the police would cease to collaborate.

The police did not actively participate in gatherings that happened over the internship. Instead, we focused on delivering them only the best final product possible.

The national direction of the PSP must authorize the PSP of Coimbra to participate in the tests. We have already the authorization from the national police and the formalization of this partnership is due to happen soon.

4

WeDoCare

4.1 Context

The first version of the application was developed during academic year of 2015/2016. The system was initially thought as a solution to help refugees, a vulnerable group likely to suffer violent attacks on grounds of discrimination. These are people who have fled from their home-country and often find themselves alone, in a new environment and culture and take shelter in places that, most of the time, lack security. Migrant women and children are more exposed to the danger of social violence because they can be easier targets for attackers, which makes them an even more vulnerable group. It must be taken into account that acts of violence are more often witnessed in less developed countries where more people face poverty conditions. It was for this reason that WeDoCare 1.0 was conceptualized and designed as an IoT and HiTL solution that makes use of the smartphone's sensors such as the microphone and GPS, thus avoiding the need to purchase additional hardware. This way, WeDoCare could be accessible to people who own even a cheap smartphone since the application uses two of the most common sensors a mobile device can have.

This reality was not as common in Portugal, namely in Coimbra, as it was in other European countries and cities which meant that it would be complicated to validate WeDoCare 1.0. Furthermore, since WeDoCare entered Anu & Naveen Jain Women's Safety XPRIZE competition in September we focused on adapting WeDoCare to other social minorities. As a result, we partnered with local associations and developed WeDoCare 2.0.

WeDoCare 2.0 is a android native application, whose main goal is to detect violent attacks in an automated way using speech recognition. During installation time, WeDoCare collects the serial ID of the SIM card and asks the user to grant all necessary permissions. Then, and every time the application starts, it requests for location updates every five minutes if the location access is turned on. The user can

4. WeDoCare

see if the location access is turned on/off in the main screen of the application.

The WeDoCare's main screen is composed by CardViews [39] and a TabLayout [40]. The CardViews contain an emergency button to trigger the alert manually, a button to activate the speech recognition and another which makes an address form appear. This form contains fields the user should fill with information about their current location because sometimes the coordinates WeDoCare gets might not be accurate enough. These fields are optional and can be modified anytime. The speech recognition CardView changes icon and color according to the speech recognition state so that the user can know whether it is turned on or off just by looking at it.

According to Material Design guidelines "tabs organize and allow navigation between groups of content that are related and at the same level of hierarchy" [41]. We have a "Home" tab, that contains what we called the 'main screen', described in the previous paragraph, a "Location" tab with an embedded map and a pin pointing to the user's current location and a "History", that contains a list of the messages sent to the police.

On top of the application there is an ActionBar [42] that holds the current activity [43] or application title and a navigation button which opens and closes a Navigation-Drawer [44]. A Navigation Drawer is useful to provide methods for other application functionalities. This navigation drawer lets the user access the application's privacy policy, frequently asked questions and entities responsible for WeDoCare.

The user can activate the alarm in two different ways: by saying the word "socorro" or by clicking the panic button. In both cases, a notification appears with the text "Don't forget to buy bread" and a button. The content of the notification is, apparently, meaningless so that attackers are not able to understand what it truly means. When the notification appears, the user has then seventeen seconds to click on the notification button and cancel the alarm. If the timer finishes without the user clicking the button, a SMS is sent to the police with the location of the attack. Before sending it, however WeDoCare checks if the SIM card ID is the same as that collected during installation. If the values are different, it may be because the mobile phone has been stolen or sold and is no longer in the possession of an Ergue-te or Saúde em Português member.

Before sharing the user's location, WeDoCare processes the location information

available, if any. There are five different outcomes of this data processing:

No location information available. If location access is turned off and the user has not inserted any location information, no messages will be sent to the police.

Only coordinates information are available. A message with coordinates information will be sent to the police.

Only physical address information is available. A message with address information will be sent to the police.

Both information is available. If both information is available, the physical address is converted to a pair of coordinates through a computational process called geocoding and the distance between the two pairs of coordinates is calculated. If the distance is smaller than 100 meters, then the physical address corresponds to the coordinates obtained and the police receives both information. Otherwise, the address probably does not correspond to the user's coordinates meaning the physical address was likely inserted by the user while before that moment and does not correspond to their current location. In this case, the police will only receive the coordinates.

Geocoding requires Internet connection. The system tries to convert the physical address to coordinates when the user first inserts the data. If, at that moment, there is no Internet connection available, the system stores the information and Geocoding is done when the system detects a network connection.

Even though good practices say that android critical permissions must be asked right before the execution of critical actions [45], we opted to ignore this guideline because we consider the violent situation to be so important that we do not want anything to get in the way of attack detections or the sending of the SMS. We will expose this problem with a practical example. Lets consider that the user has the mobile phone locked, with the application running in the background, and activates an alarm through speech recognition without having yet guaranteed the permission to send SMS. When the timer finishes, instead of sending the SMS to the police, that application would show a dialog to the user asking them to grant the permission to send the SMS and block until the user grants it or denies it.

Every time the application is started, the WeDoCare checks the language settings of the Android device and shows WeDoCare in the same language as the mobile

4. WeDoCare

phone. The default language is English.

The application contains its privacy policy that can be consulted on appendix D.

During the development phase and first tests the SMS was sent to the user's own number.

4.2 WeDoCare 1.0

WeDoCare 1.0 was an android native application developed with the purpose of detecting violent attacks through a scream recognition algorithm. The application would send an automated alert with the attack's location to other users nearby with the technology BLE Beacons. At the same time, WeDoCare would also post the same information on the user's Facebook page in order to alert the victim's friends about the situation. This location would be stored in a remote database and would later be shown to other users in a heat map. This way, other users could be informed of potential danger zones in a city. Similarly, the application also let users add helpful locales, such as hospitals and police stations, to that map.

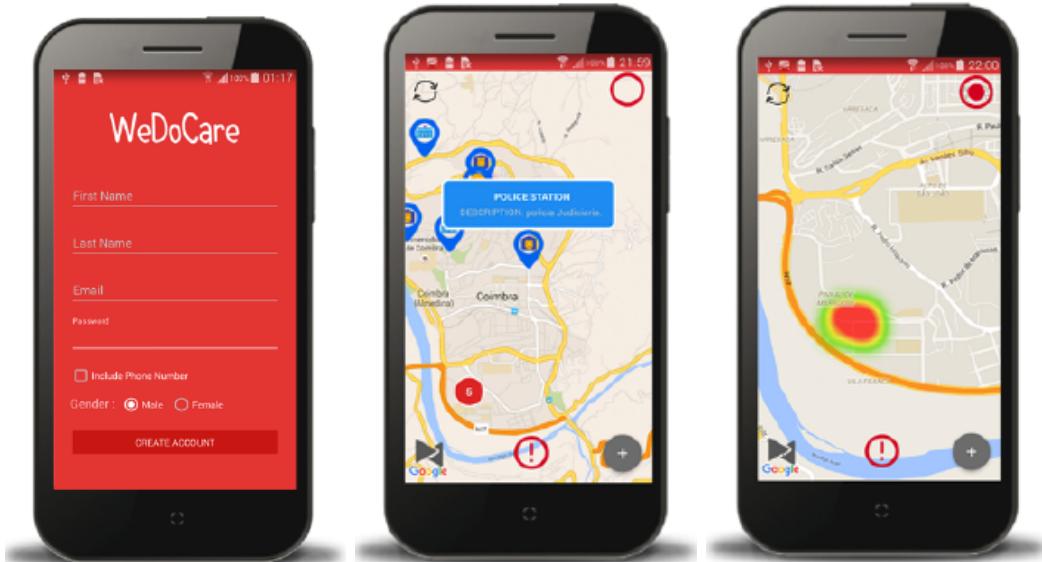


Figure 4.1: WeDoCare 1.0 screenshots

It is relevant to explain that Bluetooth Low Energy (BLE) is a wireless low-power solution technology, a feature firstly introduced with the Bluetooth Core Specification 4.0, which allows short range communication between devices and exchange of

small amounts of data between them [46]. A Beacon is a hardware that makes use of BLE and since this feature is already proliferated in the majority of modern mobile devices, these can be used to broadcast information in a wi-fi independent way. A beacon signal can be detected up to 70m by a compatible device [47].

There were some problems encountered with this version. First, the scream recognition algorithm was very inaccurate and would detect a high number of false positives because it was built and trained with a small dataset that did not include screams recorded in real situations. Second, there were some problems in connecting to the database and persisting data. And third, the beacon signal was never transmitted. The code for the application did not follow any architecture and was very hard to read and test. When we tried to add a simple button that would activate the alarm, we found that it was very hard to implement new features in the code because it was highly coupled.

For the reasons mentioned here, WeDoCare 2.0 was built from scratch.

4.3 Project requirements

4.3.1 Functional requirements

A functional requirement describes the functional behavior of the system. Each requirement will be explained as follows:

Priority: There are three different priority types

Must	Mandatory requirements. Without them, the application does not work.
Should	Requirements that must be implemented, but if not, the application still works.
Could	Not mandatory requirements and the ones with lower priority.

Table 4.1: Requirement priority types.

Description: Overall description of the requirement.

Stimulus/Response Sequences: Description of actions that need to be performed by the user in order to fulfill the requirement and expected results.

- Send an emergency alert manually

Priority: Must

Description: The user must be able to trigger an emergency alert through a button.

Stimulus/Response Sequences: The user clicks the emergency button that should be present on the main screen and very easily accessible. The system must send an automatic message to the police member with the application's identifier and the user's location (coordinates, address and link to open the pinned location on Google Maps application).

- **Send an emergency alert automatically**

Priority: Must

Description: The emergency alert must be activated automatically when it detects the words 'socorro' and 'help'.

Stimulus/Response Sequences: If the application is running in the background and the Speech Detection Algorithm is activated, the system must detect the keywords 'socorro' or 'help', meaning that the person is in danger. The system must send an automatic message to the police with the application's identifier and the user's location (coordinates, address and link to open the pinned location on Google Maps application).

- **Cancel an emergency alert**

Priority: Must

Description: The emergency alert must be canceled by the user in case of a false alarm.

Stimulus/Response Sequences: When the emergency alert is activated, the system displays a discrete notification to the user, that, apparently, is not related to the application. The user has then seventeen seconds to acknowledge this notification. If the notification is acknowledged before that time, the system must not send the text message to the police. Otherwise, both must be notified of the danger situation.

- **Store the users current location in the system**

Priority: Should

Description: The user should be able to indicate his or her current location anytime.

Stimulus/Response Sequences: The user should be allowed to fill in a form with details about a location's address (street, number, floor, frac-

tion). This information should be editable anytime.

- **Activate/deactivate the keyword detection algorithm**

Priority: Should

Description: The user should be able to turn the keyword detection algorithm on/off so that it is only running when he or she feels that a violent situation might happen and, therefore, reduce power consumption.

Stimulus/Response Sequences When the user wishes to activate the keyword detection algorithm, he or she should be able to turn it on by clicking a button that should be shown in the main screen. The system would from that moment start recording audio and searching for the word 'socorro' or 'help' in the background.

- **Inform the user about functionalities that might not work**

Priority: Should

Description: The user should be informed if something is interfering with the proper functioning of the application.

Stimulus/Response Sequences The system should show text alerts to user explaining that a feature might not work.

- **Consult the history of sent messages**

Priority: Could

Description: The user could be able to consult a list with information about the messages sent to the police.

Stimulus/Response Sequences: The user could consult an informative list with information about the time a message was sent to the police and the location sent. This list could also contain information about the messages that, due to some malfunction, were not sent.

- **Support for other languages**

Priority: Must

Description: The system must present the application in English (default), Portuguese, Nepali, Russian or Romanian.

Stimulus/Response Sequences When WeDoCare is launched it chooses the its language according to the language defined in the user's mobile phone.

4.3.2 Non-functional requirements

Opposed to functional requirements, which describe what the system needs *to do*, a non-functional requirement describes what the system needs *to be*. The following system non-functional requirements are important for designing the system's architecture.

- **Privacy**

In this specific case, the goal is to create a complete serverless application that operates without storing any type of information which could lately be accessible to someone. The information that needs to be stored persistently, should be stored locally: either on a local database or using the SharedPreferences interface.

- **Battery usage**

The application must be designed to be low-battery consuming so that it does not drain all the energy from the mobile phone and it fails in a danger situation.

Must: Last at least one day.

- **Reliability**

The system should always give the right result on the recognition of the keyword and send a 'true positive' alarm to the police.

Desired: 100 % of the times

Must: 97 % of the times

- **Maintainability**

The code should be written in a way that is easy to test and allows the extension of the application with the implementation of new features.

- **Availability**

The system must work without an Internet connection and have permission to get the users location as well as to send text messages, meaning the phone in which the application is installed must have a SIM card on it.

4.4 Architecture

Since there is no need for other technologies in order to implement the requirements mentioned above, the system is limited to only two elements - the victim's smartphone, which runs WeDoCare, and the police's smartphone. The communication between these devices is performed via SMS.

This application will not store information of any kind in a remote database or will share it under any circumstance. This approach was chosen due to privacy concerns, as explained in section 3.3. Instead, WeDoCare stores data persistently in a local database or using the SharedPreferences interface.

This particular application serves only for personal use and since every necessary information is collected during runtime, processed and then forgotten, it is not necessary to associate a human identity with it with the implementation of authentication methods. The application will only be installed on devices that belong to people authorized by the associations to participate in the tests. For this reason, WeDoCare will not be available on the Google Play Store for download. It is important, however, that the application is not accessed by people outside the testing group, which could happen if the mobile phone is sold or stolen. The simplest way to make sure that alerts from unauthorized people are not sent to the police is to verify that the SMS comes from the same SIM card ID as the one collected during the installation.

The code follows the Model View Presenter (MVP) architecture [48]. The MVP pattern establishes the separation of business logic from the interface code which results in more readable, extendible and maintainable code. In more detail, the Model provides the data we want to see in the View. The Presenter acts as a "man in the middle" between these two components and is responsible for formatting the data and pass it to the View. The View holds the code for the user interface and presents results to the user. The View can only communicate directly with the Presenter or other View methods. This separation of code makes it easier to create decoupled classes.

4.5 Development and Implementation

4.5.1 Mobile application

4.5.1.1 Technologies/Third party libraries

greenDAO greenDAO [49] is an Android Object Relational Mapping (ORM) used to create SQLite databases and that lets developers focus more on the database content than on developing SQLite requirements, which can be time consuming. This framework maps java objects to database tables, which allows for storing, updating, deleting and querying for database entries with a easy to integrate object oriented framework. Other advantages of this framework include encryption of data, low memory consumption and small library size.

Dagger Dagger [50] is a framework for dependency injection, a technique in software development whereby an object depends on other object. This framework generates code for proper dependency injection that developers would have to write themselves. Dagger makes use of a set of annotations to build a graph of objects linked by their dependencies.

EventBus EventBus [51] is a annotation based library that enables communication between decoupled classes using the publish/subscriber pattern. It delivers results in the main thread and background threads with a high and fast performance.

Butter Knife Butter Knife [52] is a library for binding views and methods that uses annotations to generate boilerplate code, saving developers the time of writing repetitive lines.

PermissionsDispatcher In Android development, it is mandatory to ask the user for permissions before performing critical actions. Writing code for such permissions and dealing with the permission results can be extensive and time consuming. PermissionsDispatcher [53] is an annotation based Application Programming Interface (API) to handle runtime permissions with minimum lines of code.

Google Play Services With Google Play Services [54], the application can use Google features, such as Maps and Location, and receive automatic Google

updates and bug fixes if it's deployed on the Google Play Store.

Material Dialogs Material Dialogs [55] is an API to create dialog messages according to the Material Design Principles. It is important to show Dialogs to users when an error occurs or when critical information needs the acknowledgment or input, but creating pleasant Dialogs using only the class android.app.Dialog can require a lot of methods and be very time consuming. This API has more straight forward methods to implement various types of Dialogs (Input Dialogs, Progress Dialogs, Basic Dialogs, etc).

Ripple Background Animations are important because motion provides a more meaningful app journey. However, animations are very complex to create. Ripple Background [56] is customizable animation designed to be integrated with other elements, like an ImageView. WeDoCare starts the Ripple Background animation when the user clicks the panic button.

4.5.1.2 Keyword Recognition System

Speech recognition is the processing and translation of spoken language by computers. It takes a big dataset and a deep understanding of audio processing techniques to develop and train an accurate speech-to-text algorithm. Instead of creating this algorithm from the very start, we focused on the study of existing solutions available on the market. For the purpose of this study we focused on two free speech recognition systems developed for programmers who want to add speech recognition to their applications rather than do speech recognition research: the CMU Sphinx and the Google API.

The CMU Sphinx is an open-source system created by the Carnegie Mellon University. It can be integrated with the Android SDK and works online and offline as long as there is an acoustic model for the language being recognized [57]. The Google API works online. A study that compared the word error rate (WER) for the two systems indicated that the Google system has a WER of 9%, in contrast with the CMU system which has a WER of 37% [58], meaning the first is far more superior. The study, however, makes a comparison between English sentences only. With the intention of performing a similar comparison with Portuguese sentences, we tried to find a Portuguese acoustic model to use with the CMU Sphinx system. Since this was not possible, we proceeded with studying the Google Api.

Google Cloud Speech-to-text [59] is capable of translating audio to text in real-time with a high accuracy, even in noisy environments. Even though such qualities are desirable for WeDoCare, this version of the system is not free and is intended for online use only which makes it not fit to integrate our application.

Finally we chose the Android Speech API. It is free and works online and offline as long as the packages for the Google offline speech recognition are installed on the mobile device. The main disadvantages are that this API does not support real-time recognition and does not perform so well in noisy environments as the Google Cloud Speech-to-Text API. The performance of the system is discussed later in this chapter, in section 4.6.2 .

When the user turns the speech recognition on, internally, WeDoCare starts a Service, an application component to perform long tasks [60] that implements the RecognitionListener interface [61]. The service can get results in two different methods: onPartialResults() and onResults(). The first methods is called when partial results are available and the second is called only when the full recognition results are available. The system keeps receiving and parsing results until it detects silence.

4.5.1.3 Logo



Figure 4.2: First WeDoCare logo.

WeDoCare's first logo is on figure 4.2. It clearly represents a woman figure, which gives the idea of exclusion of male users. A gender neutral logo was a request from

Saúde em Português. The final logo is represented on figure 4.3.



Figure 4.3: Final WeDoCare logo.

The final logo was developed with Adobe Illustrator [62]. We also tried to move far from the original logo, this is, a logo with a human figure. All the attempts are on appendix C.

4.5.1.4 User Interface/User Experience

The User Interface is every component on the application screen that interacts with the user. The User Experience is how these components interact with the user. It is very important for the application to have a visual language that can engage users while they navigate in the application and give them an understanding of what is happening in the application. This can be achieved with the use of animations and transitions. A practical example in WeDoCare is when the user clicks the panic button, represented in figure 4.4.



Figure 4.4: Animation in WeDoCare

Letting the user trigger an emergency alarm manually is one of the most important WeDoCare features and a simple button did not match the seriousness of the situ-

4. WeDoCare

ation. This red ripple animation is intended to let the user know that the alarm is activated. The red background behind the SOS icon is associated with a sense of danger and the animation lasts until the end of the countdown for sending the SMS. We drew some mockups using the JUSTINMIND tool [63] before drawing the interface in the Android Studio. We wanted the application to be as simple as possible and to match the colors in the logo. The mockups on which we based to build the final WeDoCare prototype are on figure 4.5.

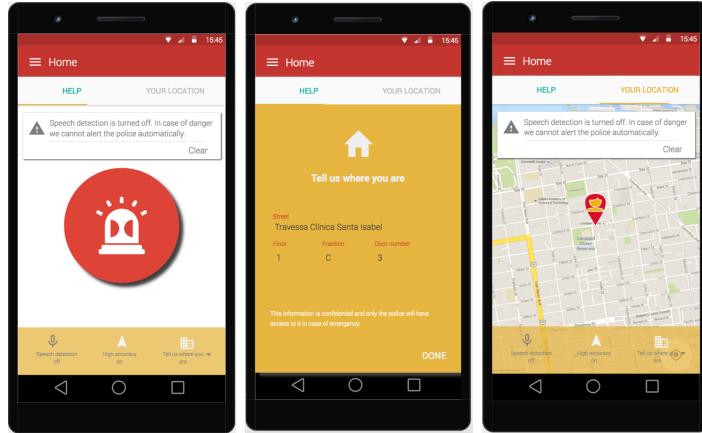
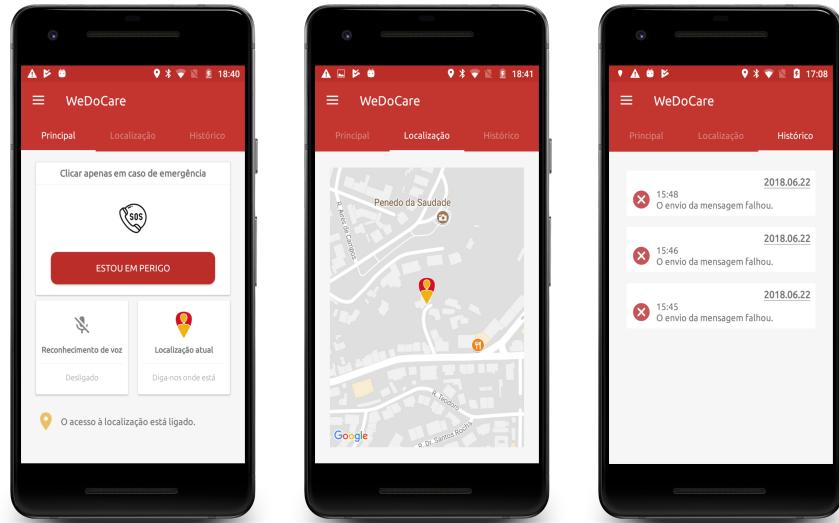


Figure 4.5: WeDoCare mockups

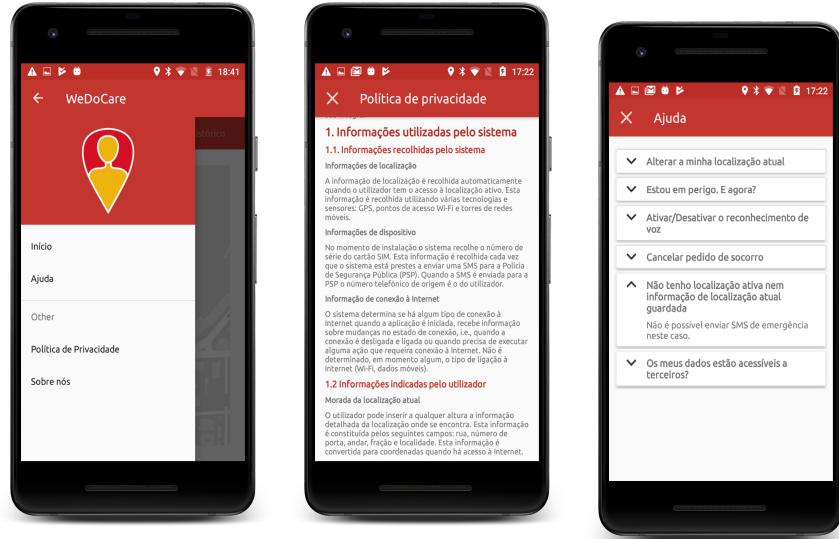
Due to the feedback we continuously received from the Socialite-LCT group and our partners, some changes were applied to the interface as it was being implemented, which resulted in a different layout from what is represented on the figure above. The final result is represented on figure 4.6



(a) Main screen.

(b) Map screen.

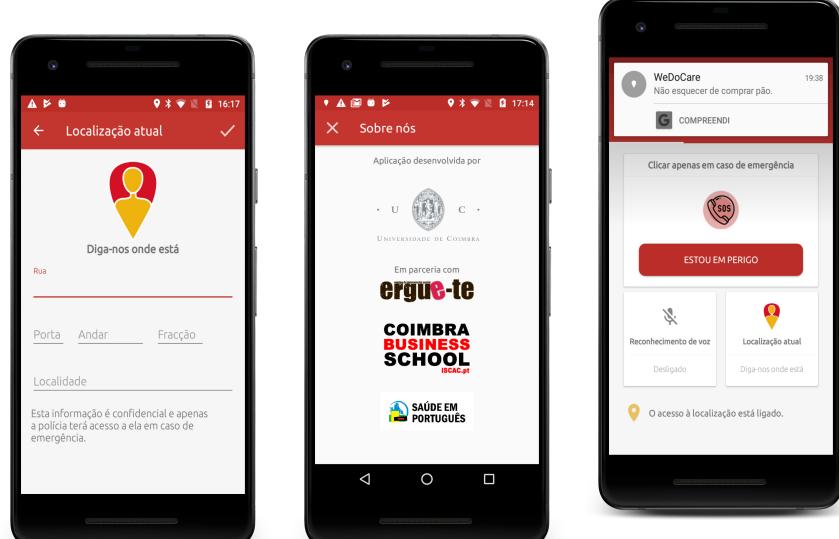
(c) History screen.



(d) Navigation drawer

(e) Privacy policy screen.

(f) Help screen



(g) Address screen.

(h) About screen.

(i) Main screen with notification and animation.

Figure 4.6: WeDoCare interface

4.5.1.5 Storage

To persist data we use an embedded SQLite database and the SharedPreferences interface [64]. The classes to access the database and SharedPreferences are in the Model part of the code.

SQLite is a lightweight relational database [65] integrated with the Android OS [66]. We use the database to store multiple objects of the same type. On the other hand, the SharedPreferences interface provides methods to store data in key-value pairs. We opt to use this interface when the data is not complex and can be organized in a simple key-value structure. In both strategies, no Internet connection is required.

To create our SQLite database, we used greenDAO, an Android ORM, which works as an intermediary between our entity class and the database as represented in 4.7.

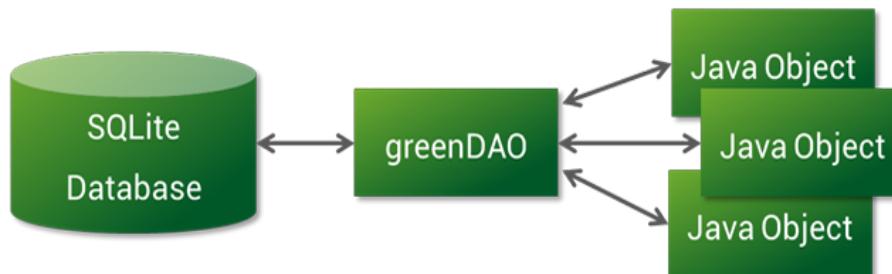


Figure 4.7: GreenDAO workflow [49].

Only information regarding the messages sent to the police is saved in the database to be later shown in the history seen. It is important that the user can see if the SMS was indeed sent to the police or if, due to some technical problem, the sending of the SMS failed. The entity type that represents this information is represented on table 4.2. sms_event is the name of the entity type in the database. The first column contains the attributes of the sms_event entity type and the second represents the variable types.

Table 4.2: Database entity.

sms_event	
id (auto increment)	Long
time	String
date	String
sent_result	boolean

We created a class for these entity types first and then focused on creating the classes that instantiate the database and have methods for writing and reading from the database.

SharedPreferences write information into a XML file that is located in the application folder in the mobile device. A SharedPreferences object contains all the preferences in the application. The figure 4.10 shows the SharedPreferences workflow.

**Figure 4.8:** SharedPreferences workflow

We wrote a class that contains methods to create a SharedPreferences object and to add and remove preferences from it. The preferences are represented on table 4.3 and hold, mostly values for the user current address.

Table 4.3: SharedPreferences Values.

Key	Type	Default Value
PREF_KEY_STREET	String	null
PREF_KEY_FLOOR	String	null
PREF_KEY_DOOR_NUMBER	String	null
PREF_KEY_FRACTION	String	null
PREF_KEY_LATITUDE	String	null
PREF_KEY_LONGITUDE	String	null
PREF_KEY_CITY_LOCAL	String	null
PREF_KEY_INSTALLATION	boolean	false
PREF_KEY_PHONE_NUMBER	String	null
PREF_KEY_SMS_DESTINATION	String	null

The key column has the values for the key in the SharedPreferences Object, the Type column has the type of the preference and the Default Value column holds the default value that is returned when we try to read a preference without other value. Each key holds the following information:

PREF_KEY_STREET Information about the user's current street location.

PREF_KEY_FLOOR Information about the floor of building where the user is.

PREF_KEY_DOOR_NUMBER Information about the number of the building where the user is.

PREF_KEY_FRACTION Information about the fraction of the building where the user is.

PREF_KEY_LATITUDE Information about the latitude of the user's current physical address location.

PREF_KEY_CITY_LOCAL Information about the user's current city.

PREF_KEY_LONGITUDE Information about the longitude of the user's current physical address location.

PREF_KEY_INSTALLATION To check the installation state of the application. After being installed, the application returns true.

PREF_KEY_PHONE_NUMBER Information about the SIM card ID.

PREF_KEY_SMS_DESTINATION Information about the SMS destination. Only used during tests.

4.5.1.6 Version Control

It is a common practice in software development to use a version control system (VCS) to help keep track of all changes made in the project over time and, if a change causes conflict in the project, the VCS lets the developer return to an earlier stage in the project, this is, an older version of the project, where this change has not yet been committed. It also lets developers work simultaneously on different features and then merge their changes without disrupting the project. VCS is fit for both teams and individuals. Specifically, we used Git [67] for version control.

Git can also be used with remote repositories. For this project, the code is stored in a GitLab [33] repository.

4.5.1.7 Distribution

The application was distributed via Google Play Store. Before passing WeDoCare to our first users tested it internally between the Socialite-LCT group so that the team could report bugs. Google Play Store has a test channel that lets us distribute the application up to 100 users.

The application was later upgraded to a beta version and distributed in a real environment so that we could get feedback on the product quality.

4.6 Tests and results

We ran several application tests. First, we distributed the application to the Socialite-LCT team, Ergue-te and Saúde em Português for two weeks so that they could provide general evaluation of the application and report errors. After, reliability tests were performed. We defined testing protocols together with Professor Jorge Sá Silva and Professor André Rodrigues that would let us conclude about the application performance.

4.6.1 Battery life

Long battery life is, perhaps, the most important aspect of user experience. No one wants to install an application that drains all the phone's battery because a dead

4. WeDoCare

mobile phone is, obviously, useless. If WeDoCare was one of those applications, not only our users would likely uninstall it but it could fail them in an emergency as well, leading them to believe that WeDoCare is not a viable solution.

Instead of developing the application for *minimum battery consumption first*, we chose to develop it for *reliability first*. Embedding location awareness in an application can be very battery-consuming and, in general, there is a direct proportionality ratio between the precision of the location data and the battery consumption. We use the Fused Location Provider API, a Google Play Services API, to make our application context aware. The *setAccuracy()* method accepts four different values as argument:

PRIORITY_HIGH_ACCURACY For the most accurate location possible.

Uses whatever resources available (GPS, Wi-Fi, cell towers) to compute location.

PRIORITY_BALANCED_POWER_ACCURACY Avoids using GPS to compute location in order to save battery, preferring Wi-Fi and cell tower information.

PRIORITY_LOW_POWER Provides minimum accuracy location data and minimum battery consumption. Uses cell towers to find the phone's location.

PRIORITY_NO_POWER Receives location information from other location-aware applications.

WeDoCare first requested location updates every twenty seconds using the **PRIORITY_HIGH_ACCURACY** value.

Constantly trying to convert physical address to coordinates would be battery consuming. Instead, WeDoCare listens for changes in the connectivity state and, if the conversion has not already happened, tries to compute the coordinates when an Internet connection is available. There are of course other components like the Speech Recognition service and the number of times the user opens the application which are also accountable for battery consumption.

First, we wanted to have a general idea of the battery consumption. For this purpose, we elaborated the following test protocol:

A Creation of control values

1. Charge the phone completely. Register the time of full charge.
2. Register the battery level 12h later.
3. Repeat for 5 days.

B Measure WeDoCare battery consumption

1. Charge the phone completely. Register the time of full charge.
2. Open WeDoCare.
3. Turn on location access and speech recognition.
4. Use the phone normally but with WeDoCare always running on background.
5. Register the battery level 12h later.
6. Repeat for 5 days.

A group of eight volunteers participated in these tests. Due to human error, most of the records do not correspond to a twelve hour period. Therefore, the best way to draw conclusions based on the values registered is by calculating the weighted mean for each set of data. The weighted mean formula is

$$\bar{x} = \frac{\sum_{i=1}^n x_i w_i}{\sum_{i=1}^n w_i}$$

where x is the value and w the weight.

The results of this test can be seen on table 4.4

Table 4.4: Results of the first battery test.

Mobile phone	Phase A	Phase B
Vodafone Smart Ultra 6	68%	29%
Samsung Note 3 Neo	10%	0%
Vodafone Smart Ultra 6	59%	37%
ZTE Blade	75%	51%
Xiomi Redmi Note 3	62%	40%
Samsung J5000 FN	63%	41%
Samsung J3 2017	17%	11%
LG G3	57%	0%

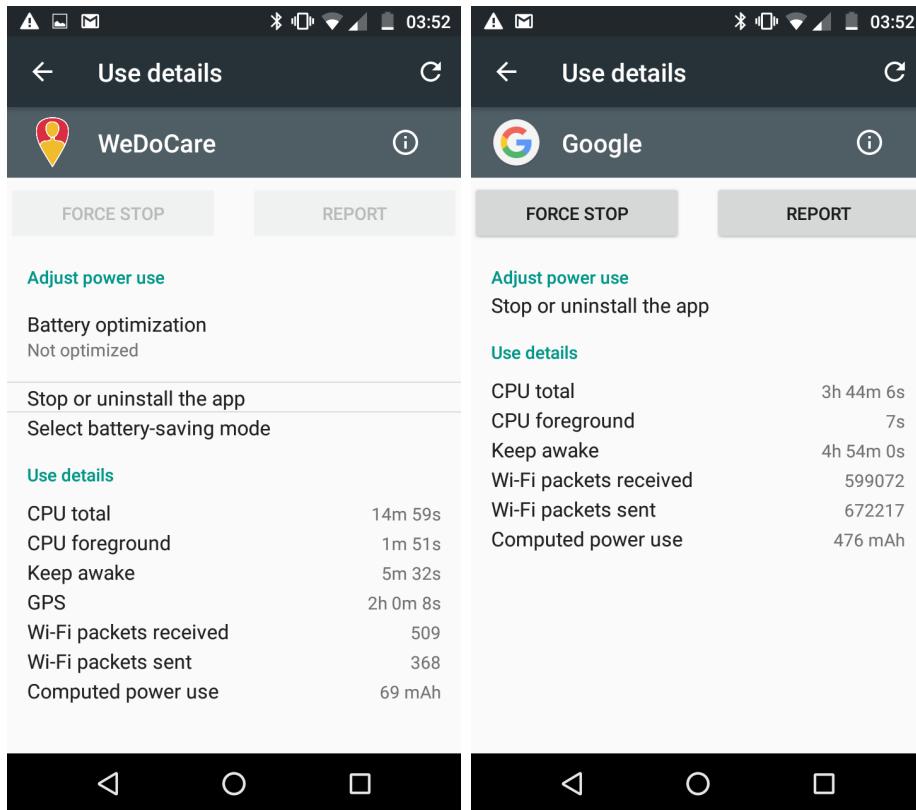
Phase A indicates the weighted mean for normal use of the phone without WeDoCare and Phase B indicates the weighted mean for normal use of the phone with WeDoCare. Every person uses the phone differently and that influences more the

4. WeDoCare

battery life than its capacity. Since these values are part of an empirical analysis and are so independent from one another, it does not make sense to find a value that represents them, like a mean.

The only conclusion that can be drawn is that WeDoCare allows, in most of the cases, for at least one day of use when its most battery-consuming functionality, this is, location updates, is continuously active. Only two out of eight mobile phones ran completely out of battery when WeDoCare was running. Since the Samsung Note 3 Neo device shows a high battery consumption even without WeDoCare, it was expected that the application would drain its battery completely. We cannot justify what happened with LG G3 phone but it shows that sometimes, the way WeDoCare requests location updates might be excessive for some users or devices. For this reason, we decided to space the location updates for every five minutes. The accuracy mode was remained for high accuracy because a precise location is crucial in case of emergency.

After these adjustments we installed the application on a Motorola Moto G3 and used the application under the same conditions. Instead of measuring the battery levels for twelve hours, we considered the statistics shown on the phone settings represented on figure 4.9. The battery of this mobile phone has a capacity of 2470 mAh which lasts for approximately 24h on regular use. The values in the figure represent the consumption of each application since the last full battery charge.



(a) WeDoCare battery statistics. (b) Google battery statistics.

Figure 4.9: WeDoCare battery statistics.

The battery consumption related to the speech recognition service is accounted in the Google battery statistics. During this time we took the care of not opening Google applications but it is not possible to be sure that WeDoCare is the only contributor for the Computer Power Use shown in figure. Nevertheless, summing both Computed Power Use values, it means that WeDoCare consumes more or less 5% of the total battery of the smartphone.

4.6.2 Keyword recognition

The speech recognition system must work 97% of the times. The disadvantage of using the Android Speech Recognition is that we do not have access to the code and it is not possible to improve the algorithm behind it. Nevertheless, we tested the performance of this recognition system in five different scenarios, all of them as close to reality as possible. Since some of our users are not portuguese speakers we studied the recognition for both 'Socorro' and 'Help' words. Twenty volunteers participated in these tests. For each case, the participants had to repeat the words 'Help' and 'Socorro' five times in a loud tone, almost screaming, with and without background

4. WeDoCare

noise. When the system detects the word, it launches a push notification.

The scenarios were the following:

1. Phone near the person;
2. Person is 5 meters away from the phone;
3. Phone is inside the trouser's pocket;
4. Phone is inside the person's purse/backpack;
5. Reading the sentence "Enviei pedidos the socorro aos meus amigos" / "I asked my friends for help".

A score between 0 and 5, representing the number of times the system detected the keyword, was assigned to each case. In the end we computed the means for every different scenario. The results can be seen on table

4.5.

Table 4.5: Results of the keyword recognition system

	Portuguese		English	
	Without background noise	With background noise	Without background noise	With background noise
Near	3,8	3,5	4,4	3,4
5 meter distance	1,7	1,1	0,1	0,3
Pocket	2,5	2,2	0,6	0,7
Purse	1,8	2,0	1,0	0,8
Sentence	3,4	2,9	3,4	3,1

The system never detected false positives. The words are more frequently recognized when spoken with good diction. None of the participants were native english speakers which often resulted in poor pronunciation of the word 'help', leading to worse results for the English scenarios in general. The performance of the speech recognition system did not decrease significantly with the presence of background noise. However, as already said, the system gets the results on the `onResults()` method and since the service does not deliver results until it detects that audio is no longer being received, the results did not come immediately after the participant saying the word. For the same reason, this also happened when the participant said the word in the middle of the sentence. In "Enviei pedidos the socorro aos meus amigos", the result of the recognition only came after the participant saying "amigos" and not immediately after "socorro".

As a result, in order to remove this delay WeDoCare now receives the recognition results on the `onPartialResults()` method. Considering the same sentence, this method delivers results as follows:

- i Enviei
- ii Enviei pedidos
- iii Enviei pedidos de
- iv Enviei pedidos de socorro
- v Enviei pedidos de socorro aos
- vi Enviei pedidos de socorro aos meus
- vii Enviei pedidos de socorro aos meus amigos.

If we constantly parse the partial results, the keyword will be found on iv, and thus, sooner. Receiving the results in this method allows for near-real-time processing.

Another approach to analyse the data was to convert the results into binary labels. If the system detects the keyword at least one out of five tries, than the result is a true positive and receives the label '1'. Otherwise, it receives the label '0'. This approach is closer to a real situation, since the user is not likely to scream for help only once in that case. It was calculated the percentage value for the number of true positives for each case. The results can be seen on table 4.6.

Table 4.6: Results of the speech recognition system: another approach.

	Portuguese		English	
	Without background noise (%)	With background noise (%)	Without background noise (%)	With background noise (%)
Near	89,5	89,5	94,7	94,7
5 meter distance	73,7	63,2	5,3	21,1
Pocket	73,7	68,4	23,6	42,1
Purse	68,4	63,2	42,1	26,3
Sentence	100,0	84,2	89,5	94,7

Even for this approach, performance of the speech recognition service is far from what is desired which makes this feature inefficient for remote automated attack detection. There must be, therefore, another functionality in the application to trigger the alarm without, at least, the necessity of unlocking the phone.

To compensate for this flaw, we integrated gesture detection in WeDoCare, explained in more detail in the next section.

4.6.3 Gesture detection

An Android phone is provided with various types of sensors, including sensors to measure motion such as accelerometers, gravity sensors, gyroscopes and rotational vector sensors. WeDoCare can use these sensors to look for a pattern in movement and trigger an alarm from it.

Android Development Kit has classes to create gesture-based events, but it requires writing a lot of boilerplate code. To avoid this, we found Sensey [68], an Android library for Gesture Detection. This library provides a set of methods to detect pre-defined gestures, which include Wrist Twist gesture, Shake gesture, Touch types and, among others, the one we chose for WeDoCare: the chop gesture.

Our first approach was to implement the shake gesture which resulted in a high number of false positives. The chop gesture is a more precise and vigorous gesture. Since it is not a common movement to do with the mobile phone, it is less likely to trigger false positives.

The library reads data from accelerometer. The time defined for the chop gesture was 100 milliseconds and the threshold for the accelerometer data was 10m s^{-2} . These are the only parameters required by the library and were obtained following a trial-error approach. The gesture detection was tested in three different devices. The procedure was to simply perform the gesture with the mobile phone and checking if the push notification appears. The results are on figure 4.10.

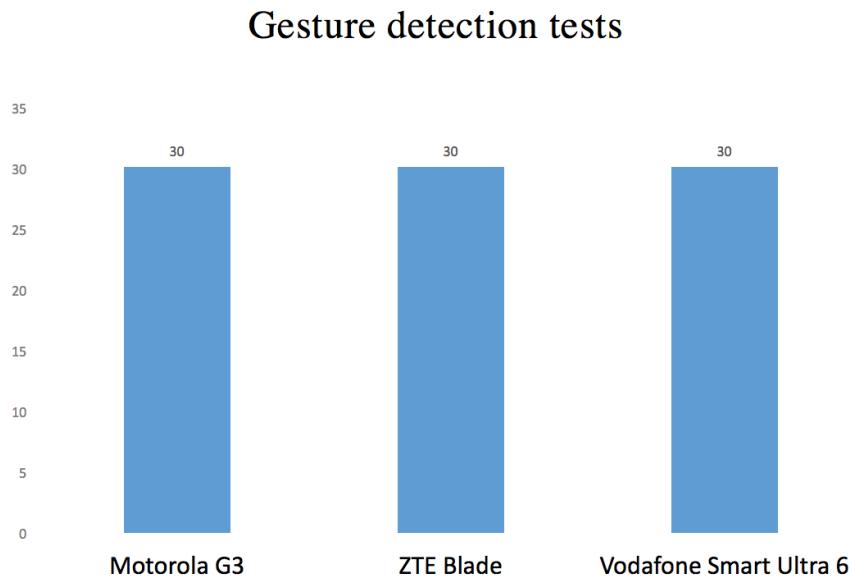


Figure 4.10: Gesture recognition results.

For each mobile device we performed the gesture thirty times. Based on the results shown, it means that the system detects the gesture and triggers the alarm 100% of the times and is reliable.

4.6.4 Website

There was already a website online for WeDoCare but the information it contained was not up-to-date with its most recent version. We have opted to keep the webpage's main structure and layout and change only the information content. To do this, we used the most common tools for web development - HTML, CSS and JavaScript. We also made use of the already integrated libraries which made the development process easier. The used integrated libraries were Bootstrap [69], WOW.js [70], Animate.css [71], Font Awesome [72] and jQuery [73].

The website is supported in both English and Portuguese languages.

4. WeDoCare

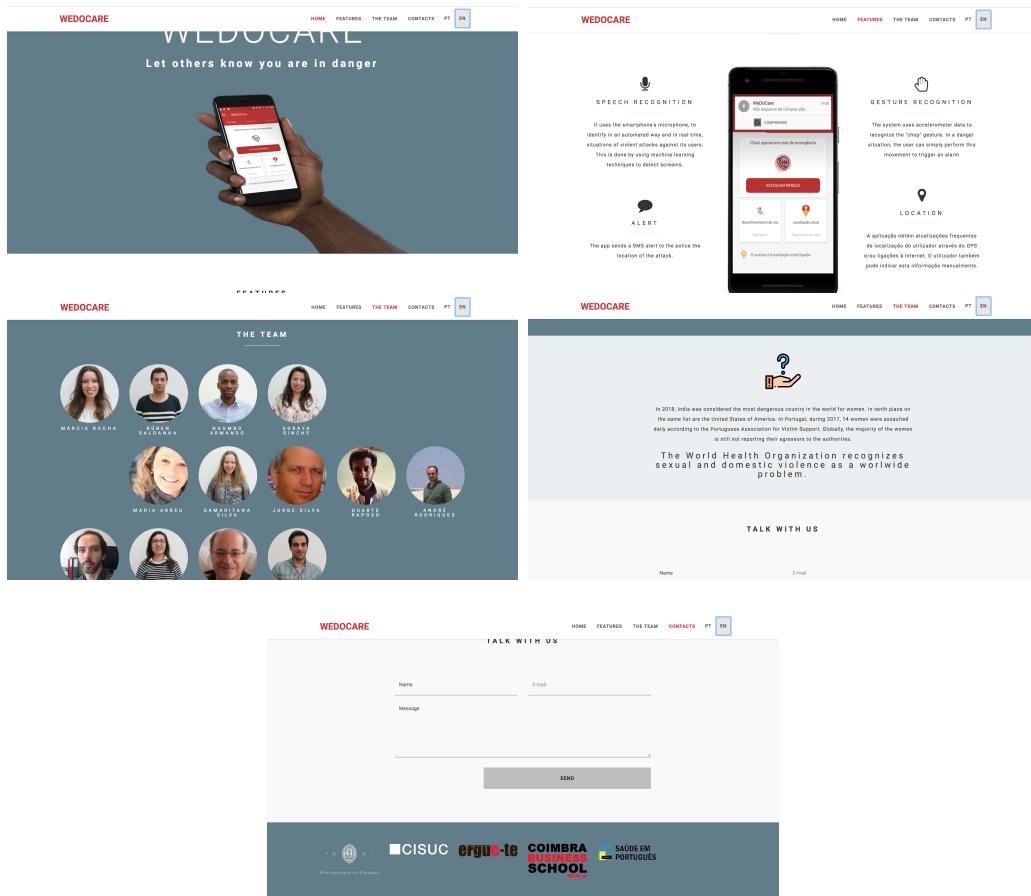


Figure 4.11: Screenshots of WeDoCare website

5

Saúde em Português: case study

The final step of this internship was to test the application in a real environment. We were supposed to count with users from Ergue-te and Saúde em Português for this stage but due the delays in scheduling meetings with the police it was not possible to include users from both associations in this study. Since the partnership with the police was not yet established at this time, the police could not receive the SMS with the victim's location and the only solution was to send them to the associations. Saúde em Português agreed to collaborate with us under this condition and Ergue-te will actively participate when the Police collaborates with us actively as well.

Before starting the tests, we scheduled a meeting with both associations to inform them about the gesture detection feature.

5.1 Risk analysis

Some concerns related to our beta testers and how they could jeopardize the testing of the system in a real scenario arose along the meetings with Ergue-te and Saúde em Português. These concerns represent the risks of our project and are associated with situations that are beyond our control and are hard to prevent. These risks are:

- **Some members from the association might refuse to adhere to the test program**

Part of the people we want to include in this phase are prostitutes. These women are very cautious with their privacy and with what they share with others, and can be afraid of relying on technology because they know it implies sharing of personal information at some point. Even if they are assured that their information is not stored or accessible to anyone, their disconnection from digital tools does not let them completely put their trust on the system.

This is a limiting factor that may shorten our testing population.

- Even with the application installed, it is highly probable that user closes it unintentionally and without noticing they closed it at some point

This is a very expectable situation. Even though our potential testing population has a smartphone, some of them do not take full advantage of their functionalities simply because they are not completely comfortable with the device. Closing the application will make all the system services to stop and, in case of emergency, the user will not be able to trigger an alarm automatically. This situation might discredit the application in the eyes of the victim who may stop using the system.

- Low number of occurrences which could lead to the police neglecting the system

The system will be implemented in a violent environment. If during the test period a low number of attacks occurs the police might forget about the phone that was given to them for emergency situations. If, by chance, the mobile phone runs out of battery power, the victim will not be assisted and this situation might also discredit the application in the eyes of the victim. Besides, it is also difficult to analyse the applicability of the system if the number of occurrences is very low, which might also discredit the system in the eyes of the police.

- The user has no credit on the mobile phone

The SMS sent by the system are charged according to the user's operator. If the phone is without credit, it is impossible to inform the police that the victim needs assistance. In this case, the system works properly but it is not possible to meet its final purpose, which is to aid the victims.

- The user does not activate access to location services and does not indicate the address of her or his current location

In this scenario, it is not possible to alert send a SMS to the police as there is no information about the location of the attack. Like in the scenario above, the system also loses its purpose in this situation. As already said, the testers will be assured that their location is not stored by the system and in they can follow instructions on how to stop google from keep the history of the user's

locations in the User's Guide, given in appendix C. However, their lack of trust in technology might still lead them not to indicate this information still.

- **The user sells the mobile phone or it is stolen**

The potential testers of our application often find themselves in situations of poverty in which is common to sell their mobile phones. On the other hand, if the phone is robbed, which can also happen because our testers expose themselves to danger almost everyday, our test group will shorten and it is harder to get meaningful results from this phase.

It is hard to calculate the probabilities of the above scenarios happening and it is only possible to say that they are likely to occur.

5.2 Success criteria

The success criteria are critical situations that need to happen in order to consider this case study a success. These are:

- **The panic button triggers the alert every time it is pressed**

The panic button is the most reliable way to trigger an emergency alert and get help from the police, but is also the less convenient way to trigger the alarm because it requires the user to unlock the phone. However, if other alternatives fail, this button must work 100% of the times.

- **Gesture detection works every time the user does the Chop movement**

Gesture recognition is the most reliable way for the user to trigger an alert without unlocking the phone. In a panic situation, the user will probably perform the chop gesture more than once. It is very important that the recognition works almost 100% of the times.

- **The keyword recognition works, at least, 70% of the times**

Since it is not possible to improve the recognition system, the performance of the keyword recognition in this stage must at least equal the performance of the keyword recognition test described previously.

- **Low energy consumption**

WeDoCare must not drain the phone's battery completely so that it becomes unavailable in case of emergency.

5.3 Methodology

We distributed the application through Google Play Store. To do this, we needed the Google accounts of our users, so that only them could download the application. Instead of giving us their true e-mails, Saúde em Português created new ones for them to associate with their Google Play account and install the application.

Since the partnership with PSP was not finished by the time of deployment, the messages were sent to a member of Saúde em Português, who would then contact the police. It was only possible to distribute the application to three users and one of them moved to Alentejo. The messages from this particular user would be sent directly to a member of Saúde em Português who would then contact a member of Saúde em Português from that area.

The association was responsible for informing users about how the application works since we could never contact the users. We elaborated an User Guide, given in appendix B, that exposes all the functionalities of WeDoCare for both association and users to consult if clarification is needed.

During this time, a meeting was scheduled together with Saúde em Português to monitor the progress of the tests. The results are discussed later in this chapter.

5.4 Legal concerns

We met with the Legal Office from the Faculty of Science and Technology of the University of Coimbra, namely the director of DITS Eng. Jorge Figueira, so that they could help us understand our legal and civil responsibility towards our partners and testers.

5.5 Results

The application was distributed successfully to the testing group.

During a period of three weeks, no attacks occurred but the application is still on the field. However, Saúde em Português reported that its members feel safer already just by knowing that they can easily ask for help if necessary. We also got the information that the users feel comfortable using WeDoCare, proving that its UI/UX meets its purpose.

No errors or malfunctions were reported during this time.

6

Conclusion

6.1 Final Results and future work

The purpose of this work was to develop a reliable mobile application with social purpose while exploring HitL and IoT concepts and evaluate its utility in real context. Throughout the year, we partnered with local associations and the local police to decide how WeDoCare could be of use to social minorities, which was the main goal of this internship. It was a very ambitious challenge from the start because of the social responsibility these partnerships required and because we committed to deliver them the final version of the application for testing during this internship.

The delays in formalizing the partnership with the police were beyond our influences and made it impossible to test the application with Ergue-te members during this year, as it was initially planned. As a result, we do not have as much feedback as we were hoping to.

Our key feature is reliability. We were able to develop an application that activates accurate emergency location alerts using keyword and gesture recognition and a button. Two out of these three methods work 100 % but the keyword recognition method proved to be insufficient for attack detection. The additional hardware that was first proposed as part of the solution for the Anu & Naveen contest would help increase the reliability of WeDoCare whenever the user cannot reach the mobile phone. At the moment, there is a member of the Socialite-LCT group working on this module. We also found that WeDoCare goes to sleep when it is inactive for long periods of time, which means that the system stops responding. Since this was only discovered by the end of the tests, we did not have the time to study and overcome this defect.

In future work, aspects like developing for low battery consumption, threads and processes, reactive programming and unit testing must be prioritized as they are

6. Conclusion

important for the application performance.

Nevertheless, we consider WeDoCare 2.0 a success because, in the end, we met all the proposed objectives for this work. We developed a system that, despite of its limitations, is fully functional and is being validated with real users.

We also had the opportunity to gain Android development skills and best practices code that is easily scalable, maintainable and testable, which makes it easier to integrate new features and improvements in the future.

6.2 Personal consideration

I joined the project because of my passion for software development and because it's important for me to work on a project with values that I stand for. This experience was, beyond challenging, rewarding.

I started the project with zero knowledge of Android development and the amount of information there is on this topic that can be overwhelming for an unexperienced programmer. Since I was the only responsible for developing the Android application, there was everything to learn in so little time that it was hard to know where to start. Knowing what I know at the moment and assuming the limitations of the application, I recognize the final product exceeds my initial expectations. I had the opportunity to learn and deepen Android platform development skills, different design patterns and various libraries that now allow me to pursue a career as an Android Developer. By updating the app's landing page I could also learn the basics of Web Development and that, together with designing the application's UI/UX, triggered my interest for good design.

One of my biggest concerns when developing WeDoCare was to provide a good UI/UX. Since there were no designers on the team, I had to extensively study the best design practices in order to do so. Animations play a very important role in this part because motion provides meaning. After reading some tutorials I tried to write code for my own animation but failed and because I had a tight deadline I ended up using a third library to implement it. This was my greatest difficulty. Even so, studying and working on the application design was the most fun challenge for me because it was what made me feel most out of my comfort zone while also

working on my creative side.

It is extremely gratifying to know that this work can have a big impact on society. This project proves that there is no need for always trying to reinvent the wheel when it comes to find technological solutions because, sometimes, all it takes is a good understanding of the problem we are dealing with.

6. Conclusion

Bibliography

- [1] “Estatisticas APAV (Relatorio Anual 2017),” 2018.
- [2] “A India é o pais mais perigoso para ser mulher.” <http://visao.sapo.pt/actualidade/mundo/2018-06-27-A-India-e-o-pais-mais-perigoso-para-se-ser-mulher>. last checked: 01.06.2018.
- [3] “National Family Health Survey (NFHS-4),” 2015-2016.
- [4] M. E. L. H. C. H. W. Claudia Garcia-Moreno, Henrica AFM Jansen, “Prevalence of intimate partner violence: findings from the WHO multi-country study on women’s health and domestic violence,” *Lancet*, vol. 368, 2006.
- [5] “me too..” <https://metoomvmt.org/>. last checked: 3.07.2018.
- [6] D. Woodlock, “The Abuse of Technology in Domestic Violence and Stalking,” *Violence against women*, vol. 1, 2016.
- [7] K. C. B. P. J. K. M. S. G. S. P. Matthew J. Breiding, PhD, “Economic Insecurity and Intimate Partner and Sexual Violence Victimization,” *American Journal of Preventive Medicine*, 2017.
- [8] “Who we are.” <https://www.xprize.org/about/what-is-an-xprize>. last checked: 03.07.2018.
- [9] “Anu and Naveen Jain Women’s Safety XPRIZE.” <https://safety.xprize.org/teams1>. last checked: 8.02.2018.
- [10] “ergue-te.” <http://erguete.pt>. last checked: 10.6.2018.
- [11] “Saude em Portugues.” <http://www.saudeemportugues.com>. last checked: 10.6.2018.
- [12] “That ‘Internet of Things’ thing.” <http://www.rfidjournal.com/articles/view?4986>. last checked: 3.02.2018.
- [13] G. M. Luigi Atzori, Antonio Iera, “The Internet of Things: A survey,” *Computer Networks*, 2010.
- [14] “Internet of Things forecast.” <http://www.ericsson.com/en/mobile-report/internet-of-things-forecast>. last checked: 8.02.2018.
- [15] P. K. P. Middleton and J. Tully, “Forecast: The internet of things, worldwide,

Bibliography

- 2013,” *Gartner, Tech. Rep.*, November 2013.
- [16] “Sensors Overview.” https://developer.android.com/guide/topics/sensors/sensors_overview.html. last checked: 7.02.2018.
- [17] “Sensors.” <https://source.android.com/devices/sensors/>. last checked: 7.02.2018.
- [18] A. C. Francesco Piccialli, “The Internet of Things Supporting Context-Aware Computing: A Cultural Heritage Case Study,” *Mobile Networks and Applications*, April 2017.
- [19] C.-J. M. L. S. L. S. Munir, J. A. Stankovic, “Cyber Physical System Challenges for Human-in-the-Loop Control,” *8th Int. Workshop Feedback Computing, San Jose, CA, USA*, 2013.
- [20] “Global market share held by smartphone operating systems from 2009 to 2017.” <https://www.statista.com/statistics/263453/global-market-share-held-by-smartphone-operating-systems/>. last checked: 15.05.2018.
- [21] “Dashboards: Platform versions.”
- [22] <https://www.apple.com/iphone/>. last checked: 7.6.2018.
- [23] “wearsafe labs.” <https://www.wearsafe.com/>. last checked: 7.6.2018.
- [24] “SafeTrek.” <https://www.safetrekapp.com/>. last checked: 7.6.2018.
- [25] “NIMB.” <https://nimb.com/app/>. last checked: 5.5.2018.
- [26] “Guardian Circle.” <http://guardiancircle.com/>. last checked: 6.6.2018.
- [27] “Watch Over Me.” <http://watchovermeapp.com/>. last checked: 6.6.2018.
- [28] “bSafe.” <https://getbsafe.com/features/>. last checked: 6.6.2018.
- [29] “LEAF.” <https://www.leafwearables.com/>. last checked: 12.6.2018.
- [30] “GH4000 Handheld GNSS/GSM Tracker.” https://teltonika.lt/product/gh4000-handheld-gnss-gsm-tracker/#product_features. last checked: 30.06.2018.
- [31] “Slack.” <https://slack.com/>. last checked: 6.6.2018.
- [32] “Skype.” <https://www.skype.com/pt/>. last checked: 6.6.2018.
- [33] “Gitlab.” <https://about.gitlab.com>. last checked: 7.6.2018.
- [34] “Principles behind the Agile Manifesto.” <http://agilemanifesto.org/principles.html>. last checked: 9.6.2018.
- [35] “Kanban. What is kanban.” <https://www.atlassian.com/agile/kanban>. last checked: 10.6.2018.
- [36] “Trello.” <https://trello.com>. last checked: 9.6.2018.
- [37] “Definition of crowdfunding.” <https://www.merriam-webster.com/dictionary/crowdfunding>. last checked: 10.6.2018.

- [38] “Ha 25 mil chamadas diarias para o 112, mas 75% nao sao emergencias, diz a PSP.” <https://observador.pt/2016/02/11/ha-25-mil-chamadas-diarias-112-75-nao-sao-emergencias-diz-psp/>. last checked: 11.6.2018.
- [39] “Cardview.” <https://developer.android.com/reference/android/support/v7/widget/CardView>. last checked: 25.06.2018.
- [40] “TabLayout.” <https://developer.android.com/reference/android/support/design/widget/TabLayout>. last checked: 25.06.2018.
- [41] “Tabs: Usage.” <https://material.io/design/components/tabs.html#>. last checked: 25.06.2018.
- [42] “ActionBar.” <https://developer.android.com/reference/android/app/ActionBar>. last checked: 25.06.2018.
- [43] “Activity.” <https://developer.android.com/reference/android/app/Activity>. last checked: 25.06.2018.
- [44] “Criacao de uma gaveta de navegacao.” <https://developer.android.com/training/implementing-navigation/nav-drawer>. last checked: 25.06.2018.
- [45] “Permissions overview: request prompts for dangerous permissions.” <https://developer.android.com/guide/topics/permissions/overview>. last checked: 25.06.2018.
- [46] J. P. Carles Gomez, Joaquim Oller, “Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology,” *Sensors*, August 2012.
- [47] N. S. Sunny Gleason, “Building Smarter Beacons: Bidirectional Beacon Communication.” <https://www.pubnub.com/blog/2015-02-03-building-smarter-beacons-bidirectional-beacon-communication/>, February 2015. last checked: 27.11.2017.
- [48] “Model-View-Presenter.” <https://en.wikipedia.org/wiki/Model%E2%80%93view%E2%80%93presenter>. last checked: 20.06.2018.
- [49] “greenDAO: Android ORM for your SQLite database.” <http://greenrobot.org/greendao/>. last checked: 20.06.2018.
- [50] “Dagger.” <https://google.github.io/dagger/>. last checked: 21.06.2018.
- [51] “EventBus.” <http://greenrobot.org/eventbus/>. last checked: 21.06.2018.
- [52] “Butter Knife.” <http://jakewharton.github.io/butterknife/>. last checked: 21.06.2018.
- [53] “PermissionsDispatcher.” <https://github.com/permissions-dispatcher/PermissionsDispatcher>. last checked: 21.06.2018.
- [54] “Overview of Google Play Services.” <https://developers.google.com/>

- [android/guides/overview](https://developer.android.com/guide/components/services). last checked: 21.06.2018.
- [55] “Material Dialogs.” <https://github.com/afollestad/material-dialogs>. last checked: 21.06.2018.
- [56] “Android Ripple Background.” <https://github.com/skyfishjy/android-ripple-background>. last checked: 21.06.2018.
- [57] “PocketSphinx on Android.” <https://cmusphinx.github.io/wiki/tutorialandroid/>. last checked: 22.06.2018.
- [58] G. B. Veton Kepuska, “Comparing Speech Recognition Systems (Microsoft API, Google API And CMU Sphinx),” *International Journal of Engineering Research and Application*, March 2017.
- [59] “Cloud speech-to-text.” <https://cloud.google.com/speech-to-text/>. last checked: 22.06.2018.
- [60] “Servicos.” <https://developer.android.com/guide/components/services>. last checked: 26.06.2018.
- [61] “RecognitionListener.” <https://developer.android.com/reference/android/speech/RecognitionListener>. last checked: 26.06.2018.
- [62] “The state of the art of illustration.” <https://www.adobe.com/products/illustrator.html?promoid=PGRQQLFS&mv=other>. last checked: 6.07.2018.
- [63] “JUSTINMIND: All-in-one Prototyping Tool for web and mobile apps.” <https://www.justinmind.com/>. last checked: 24.06.2018.
- [64] “SharedPreferences.” <https://developer.android.com/reference/android/content/SharedPreferences>. last checked: 22.06.2018.
- [65] “About SQLite.” <https://www.sqlite.org/about.html>. last checked: 20.06.2018.
- [66] “SQLite Android Bindings.” <https://sqlite.org/android/doc/trunk/www/index.wiki>. last checked: 20.06.2018.
- [67] “git –local-branching-on-the-cheap.” <https://git-scm.com/>. last checked: 26.06.2018.
- [68] “Sensey.” <https://github.com/nisrulz/sensey>. last checked: 28.06.2018.
- [69] “Bootstrap.” <https://getbootstrap.com/>. last checked: 6.07.2018.
- [70] “WOW.js.” <https://mynameismatthieu.com/WOW/>. last checked: 06.07.2018.
- [71] “Animate.css.” <https://daneden.github.io/animate.css/>. last checked: 06.07.2018.
- [72] “Font Awesome: Icons. Easy. Done.” <https://fontawesome.com/>. last checked: 06.07.2018.
- [73] “jQuery: write less, do more..” <https://jquery.com/>. last checked: 06.07.2018.

Bibliography

Appendices

A

User guide

WeDoCare



Manual de usuario

Capítulo 1

WeDoCare

1.1 A aplicação

O WeDoCare é uma aplicação desenvolvida pela Universidade de Coimbra em parceria com o Instituto Superior de Contabilidade e Administração de Coimbra, a associação ERGUE-TE e a associação Saúde em Português que visa a mobilização de ajuda rápida em situações de violência doméstica e sexual.

A aplicação utiliza o reconhecimento de voz e serviços de localização para detetar uma destas situações de emergência e envia um alerta para a Polícia de Segurança Pública sobre a ocorrência através de uma SMS.

O requisito necessário para o funcionamento da aplicação é a existência de um cartão SIM com saldo no telemóvel. O envio da SMS pode ser cobrado de acordo com os preços definidos pelo tarifário do utilizador. A aplicação está desenvolvida para que o seu funcionamento seja garantido quando não é possível ter acesso à Internet, no entanto, é necessário proceder a algumas configurações que serão explicadas no capítulo seguinte.

A aplicação é suportada nas seguintes línguas: Português, Inglês, Russo, Nepalês e Romeno.

1.2 Proteção de dados e identidade

As informações do utilizador, nomeadamente a informação de localização e número de telemóvel, não estarão acessíveis a terceiros incluindo a Universidade de Coimbra e suas instituições parceiras. No entanto, no caso de envio de sms para a PSP, a mensagem terá o conteúdo da última localização do utilizador e o seu contacto telefónico.

Capítulo 2

Instalação

2.1 Permissões

O utilizador terá, em primeiro lugar, de garantir as permissões necessárias para que a aplicação funcione corretamente. Estas permissões são para acesso à localização, gravação de audio, gestão de chamadas e envio de SMS.

Para tal, basta o utilizador selecionar **Permitir** nas caixas de diálogo que aparecem sucessivamente. Um exemplo está na figura que se segue.

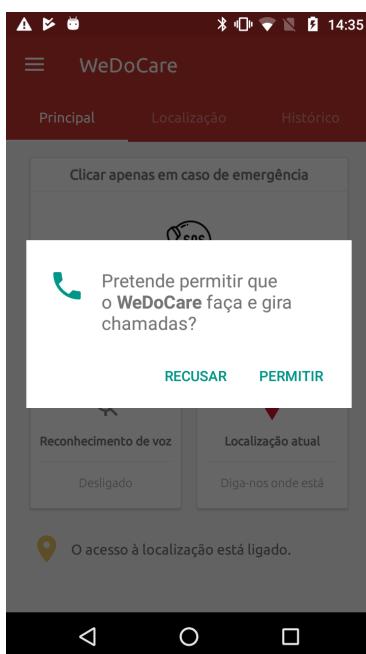


Figura 2.1: Pedido de permissão.

Caso o utilizador não garanta as permissões neste momento, deve fazê-lo em

- Nas **Definições** do telefone, ir a **Aplicações**

- Selecionar **WeDoCare**.
- Selecionar **Permissões** e dar acesso a todas as permissões que aparecem no ecrã.

Se as permissões não forem dadas as funcionalidades da aplicação ficarão comprometidas.

2.2 Reconhecimento de voz em modo offline

Para ativar o reconhecimento de voz em modo offline, seguir os seguintes passos:

- Nas **Definições** do telemóvel, ir para **Idioma e Entrada**.
- Clicar em **Voz**
- Em **Idiomas** procurar **Português (Brasil)** e premir sem soltar para selecionar como idioma principal. Clicar em **Guardar**
- Em **Reconhecimento de voz offline** verificar se o idioma **Português (Brasil)** se encontra instalado. **Caso não se encontre instalado**, no separador **Tudo** procurar **Português (Brasil)** e clicar no idioma para instalar.

O mesmo procedimento se aplica para outros idiomas. É importante que o idioma principal seja o que o utilizador considera que seja o que vai utilizar em caso de emergência.

Capítulo 3

Funcionalidades do WeDoCare

3.1 Acesso à localização

Para além da autorização para o acesso à localização do dispositivo, a localização do telemóvel deve estar ativada. Para ativar:

- Nas **Definições** do telemóvel, ir para **Localização**.
- Selecionar o modo **ativado**

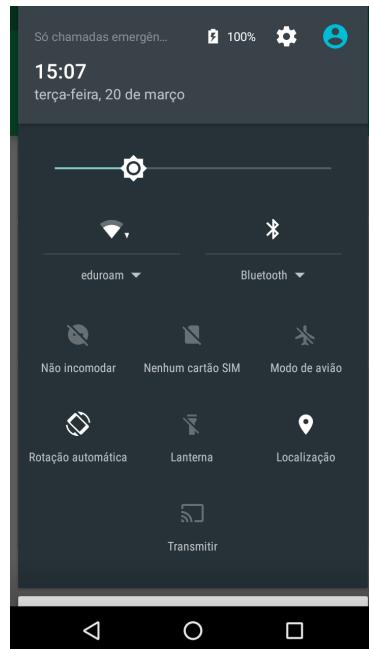


Figura 3.1: Localização ativa.

Se a localização estiver ativa, o ícone da localização aparece como na figura 3.1

3.2 Reconhecimento de voz

O reconhecimento de voz deve ser ativado/desativado manualmente. Aconselha-se a que esta funcionalidade esteja ativa apenas quando necessário por motivos de poupança de bateria. No ecrã principal do **WeDoCare**, clicar em **Reconhecimento de voz** para ativar/desativar o reconhecimento de voz.

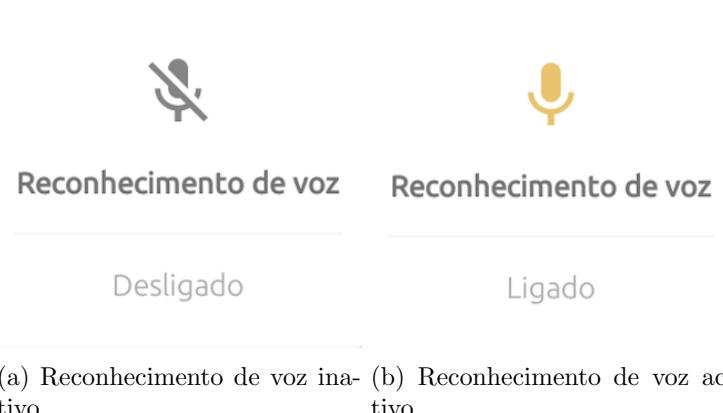


Figura 3.2: Botão de reconhecimento de voz.

3.3 Localização atual

A informação com localização exata do utilizador deve ser introduzida e modificada sempre que necessário. Para indicar esta informação:

- No ecrã principal do **WeDoCare**, clicar em Localização atual.
- Um formulário aparece. Os campos, apesar de facultativos, devem ser preenchidos com informação correta.
- Clicar em para guardar informação.

3.4 Pedido de ajuda

O pedido de ajuda pode ser feito de duas maneiras: dizendo a palavra socorro ou clicando no botão de emergência do ecrã principal. Em ambos os casos um SMS é enviado para polícia de segurança pública com informação de localização.

Nota importante: Se não houver informação de localização (morada registada ou acesso à localização do telefone), o sms não será enviado.

3.4.1 'Socorro'

O reconhecimento de voz **tem de estar ativo** neste caso. Se o **WeDoCare** detetar a palavra socorro, receberá uma notificação com o conteúdo 'Não esquecer de comprar pão!'. A partir deste momento, tem **17 segundos** para clicar em **Compreendi** e **cancelar o pedido de socorro**. Se este tempo for ultrapassado é enviada uma mensagem de socorro para a Polícia de Segurança Pública com informação de localização.

3.4.2 Botão de emergência

É possível desencadear um pedido de ajuda manual, através do botão de emergência que se encontra no ecrã Principal do **WeDoCare**. Neste caso receberá uma notificação com o conteúdo 'Não esquecer de comprar pão!'. A partir deste momento, tem **17 segundos** para clicar em **Compreendi** e **cancelar o pedido de socorro**. Se este tempo for ultrapassado, será enviada uma mensagem de socorro para a Polícia de Segurança Pública com informação de localização.

3.4.3 'Chop'

O pedido de ajuda pode ser ativado através do gesto 'chop' que é um gesto que se assemelha ao do corte com uma faca. Mesmo com o telemóvel bloqueado esta funcionalidade está ativa. Neste caso receberá uma notificação com o conteúdo 'Não esquecer de comprar pão!'. A partir deste momento, tem **17 segundos** para clicar em **Compreendi** e **cancelar o pedido de socorro**. Se este tempo for ultrapassado, será enviada uma mensagem de socorro para a Polícia de Segurança Pública com informação de localização.



Figura 3.3: Ecrã principal do WeDoCare durante o pedido de ajuda.

3.5 Outras

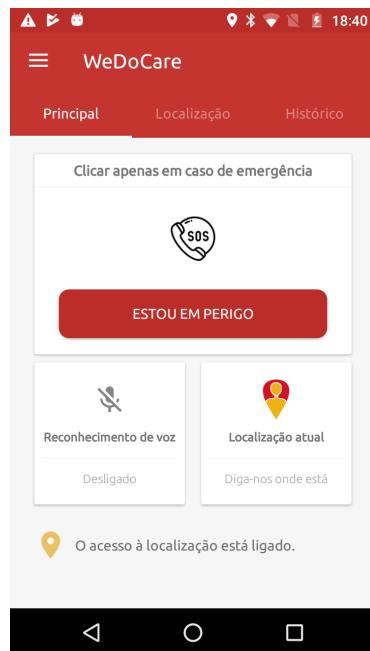


Figura 3.4: WeDoCare.

Outras funcionalidades da aplicação:

- : Navegação para o ecrã de ajuda, política de privacidade e ”Sobre nós”.
- **Localização:** Localização atual do utilizador mostrada no mapa.
- **Histórico:** Data, hora e resultado do envio das últimas SMS para a polícia de segurança pública.

3.5.1 Notificações

As notificações do WeDoCare têm uma vibração e som associado para que o utilizador consiga perceber que um pedido de socorro foi ativado. Para permitir o funcionamento desta funcionalidade e para ter a certeza que as notificações aparecem mesmo que o telemóvel esteja bloqueado:

Em **Definições**, aceder a **Som e Notificações**. Na secção 'Notificação', verificar se a opção **Mostrar todas as notificações com o dispositivo bloqueado** está selecionada. Em **Notificações de aplicações**, clicar em **WeDoCare** e verificar se as opções **Tratar como prioridade** e **Permitir espreitar** estão ativas.

Nota muito importante: Em algumas marcas de telemóveis, como por exemplo, Huawei e Xiaomi, o botão de ação das notificações está omitido por defeito. Para ver o botão 'Compreendi' é necessário **deslizar com dois dedos sobre a notificação**.



Figura 3.5: Notificação com botão 'Compreendi' oculto no dispositivo Huawei P9 Lite

Na figura 3.5 é possível reparar que se encontra uma seta azul na notificação. Ao invés de deslizar com dois dedos sobre a notificação, também é possível clicar neste pequeno ícone e o botão 'Compreendi' aparecerá.

3.5.2 Impedir que a Google guarde o seu histórico de localizações

A funcionalidade de guardar o seu histórico de localizações não está diretamente relacionada com ao WeDoCare mas sim com a Google. Para aumentar a sua privacidade pode desativar esta funcionalidade em **Definições**, ir a **Localização** e deslizar até **Histórico de Localizações da Google**. Verificar se a opção **Utilizar o histórico de localizações** está desativada.

3.5.3 Otimização de bateria

A partir da versão 6.0, o Android entra num modo 'Sleep' quando o telemóvel não é usado durante muito tempo para poupança de bateria. Isto implica que algumas funcionalidades do WeDoCare possam ser desativadas. Para evitar isto ir a **Definições** e clicar em **Aplicações**. Depois, clicar no ícone e selecionar **Otimização de bateria**. Se o WeDoCare não aparecer na lista de aplicações **Não otimizada** clicar na seta ▼ e depois em **Todas as aplicações**. Deslizar no ecrã até encontrar o WeDoCare. Clicar em **WeDoCare** e depois selecionar **Não otimizar** e clicar em **Concluído**.

B

Anu and Naveen XPRIZE
application

2017



WeDoCare

General Description

ANU AND NAVEEN JAIN WOMEN'S SAFETY XPRIZE
LCTSENSE - UNIVERSITY OF COIMBRA - PORTUGAL

Contents

Table index	2
Figure index	3
Acronyms	4
Abstract	5
1. UC/LCTSens Group Description.....	6
2. Introduction	7
3. WeDoCare features.....	10
3.1. General description	10
3.2. WeDoCare user-interface	12
3.3. Ladies' clothes node	18
3.3.1. Introduction.....	18
3.3.2. Requirements	19
3.3.3. Architecture.....	20
3.3.4. Implementation details	21
4. Requirements.....	25
4.1. Requirements of the contest.....	25
4.2. Compliance with the requirements and comparison with competitors	26
5. Conclusion	28
References.....	29

Table index

Table 1 - Main system attributes (required)	25
Table 2 - Main system features (required)	26

Figure index

Figure 1 - WeDoCare system	7
Figure 2 - WeDoCare cycle schematics.....	10
Figure 3- WeDoCare app outlook.....	11
Figure 4 - WeDoCare's login screen	13
Figure 5 - WeDoCare's registration screen.....	14
Figure 6 - Various screenshots of the WeDoCare's map screen.....	15
Figure 7 - WeDoCare's navigation drawer screen	16
Figure 8 - WeDoCare's settings screen.....	16
Figure 9 - WeDoCare's danger zone screen	17
Figure 10 - WeDoCare helpful locale screen	17
Figure 11 - Hermes simplified architecture.....	19
Figure 12 - Fenix (on the left) and Pegasus (on the right)	19
Figure 13 - Ladies' clothes node architecture	21
Figure 14 - A node from mbientlab.com	21
Figure 15 - Two cases used in car alarm controls.....	22
Figure 16 - SensorTag dimensions (from TI site)	23
Figure 17- SensorTag architecture (from TI site).....	23

Acronyms

AI	Artificial Intelligence
ANN	Artificial Neural Networks
API	Application Programming Interface
IoT	Internet of Things
JSON	JavaScript Object Notation
MFCC	Mel Frequency Cepstral Coefficients
MVC	Model-View-Controller
POI	Point of Interest
REST	Representational State Transfer
RTOS	Real Time Operating Systems
SVM	Support Vector Machine
UI	User Interface
XML	eXtensible Markup Language

Abstract

There is a large number of personal alarm systems in the market, most of them based on panic buttons. Nevertheless, none of them has got widespread acceptance. The reasons are easy to explain:

- most systems require extra and/or expensive hardware;
- some are difficult to activate in the event of an attack; and
- most of them generate a high percentage of false positive messages, which makes them useless.

In the context of the "Anu and Naveen Jain Women's Safety XPRIZE" our research group developed a system, named WeDoCare, which overcomes the mentioned drawbacks. WeDoCare:

- detects attacks in real-time;
- is ubiquitous;
- provides an automatic triggering solution;
- is both easy and intuitive to use;
- does not mandatorily require extra hardware, which makes it usable by all people regardless of their social and economic situation;
- and, most importantly, it is RELIABLE.

Reliability is a key feature of any system targeting attack detection. The WeDoCare project constitutes a significant advance beyond the state-of-the-art by developing a performance-controlled system for use in personal attack detection. The overall goal of WeDoCare is an automatic, low-cost, easy-to-use solution that meets the objective targets of Women protection.

WeDoCare is a fresh approach that uses innovative methods to offer reliability in all phases and components of the system operation, namely prevention, detection, alert, communication, dissemination, and actuation.

1. UC/LCTSense Group Description

The University of Coimbra (UC), Portugal, comprises eight Faculties, more than 2000 teachers and 22000 students. Founded in the year 1290, the University of Coimbra is the oldest in Portugal and one of the oldest in the World. The Department of Informatics Engineering (DEI) of the University of Coimbra (www.dei.uc.pt) is one of the 14 departments of the Faculty of Sciences and Technology (FCTUC). Its research unit is the Centre for Informatics and Systems of the University of Coimbra (CISUC, <http://www.cisuc.uc.pt/>). The research group involved in the current proposal is the Communications and Telematics (CT) group. The CISUC-CT group has a vast experience in the communications area and is currently active in research projects in the areas of the Internet of Things, mobile phone programming, wireless sensor networks, network and systems management, and network security. In the last few years the group has published more than 150 papers in international journals and conferences, and has been involved in several R&D projects at national and European levels. Additionally, the senior members of LCT have been involved in program committees and organisation of both national and international conferences, as well as reviewing activities for international journals, conferences and European projects (for detailed information please see: <https://www.cisuc.uc.pt/groups/show/lct>).

The WeDoCare project also includes the participation of researchers from the Faculty of Psychology of the University of Coimbra.

2. Introduction

Both physical and psychological abuses are worldwide phenomena, irrespective of the degree of development of countries or even socio-economic status of victims and perpetrators. In many cases, the perpetrators of abuse are the so-called “respectable” individuals, including family members, teachers and celebrities. Moreover, in most situations abuses occur in environments normally considered safe, such as schools, offices, and even the victims' homes. Apart from sexual abuse, another common form of abuse concerns domestic violence, under the form of emotional, physical or sexual-domestic harassment, which is painfully experienced in many countries by more than 60% of women, during their lifetime.

In the current scenario of high vulnerability, this proposal aims at supporting proactive action so as to help preventing all forms of sexual, physical or emotional abuse, which may occur either in the street or even at home, as is the case of domestic violence.

Based on the requirements of the Anu and Naveen Jain Women's Safety XPRIZE contest, described in the next section, we propose both an innovative and fresh solution based on mobile phones, optionally complemented by an unobtrusive, auxiliary device to be attached to ladies' clothes. This solution will help in the detection of attacks against women and in the triggering of help requests - the whole of which will be performed within less than 9 seconds.

We base our solution on one key feature: reliability. Taking advantage of cutting-edge technologies, WeDoCare proposes to help potential victims by addressing reliability in a variety of ways (Figure 1):

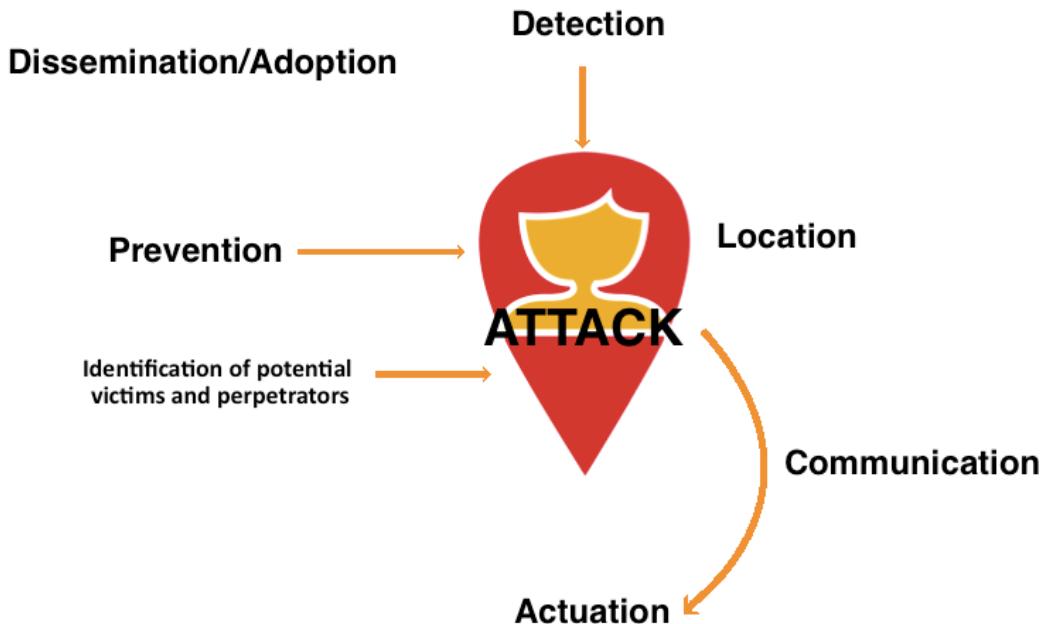


Figure 1 - WeDoCare system

Reliability of detection

WeDoCare provides reliable detection. The most important reason for the failure of current alarm systems is the large number of false positive messages that they generate. Our system is unique in the way that it uses smartphone-based technologies and innovative artificial intelligence methods that combine the use of microphone, GPS, and accelerometer data, with historic analysis, in order to automatically detect attack events, based on the victim's behaviour, such as screams, agitated movements, and other features, which are linked to emergency situations in different scenarios.

All of these methods are transparent to the user.

Although the purpose of the WeDoCare project is to provide a free solution based on a mobile phone application, the optional, auxiliary device to be attached to ladies' clothes can significantly improve the detection reliability. Indeed, women tend to leave their mobile phones in their purses while walking or leave them on a piece of furniture while talking to other people.

Reliability of the communication process

The proposed architecture relies also on an innovative beacon system that allows mobile phones to communicate with other nearby mobile phones in range, without the need of cellular or data network communications. This enables communicating with surrounding people even when there is no Internet or cellular connection available, increasing the effectiveness of our approach.

Reliability of actuation

WeDoCare makes nearby emergency help available when an attack/threat takes place. It is not only important to alert police authorities but it is also invaluable to warn people in surrounding areas, so that they can help avoiding or stopping the attack.

Reliability of location

A key aspect when an attack occurs is the identification of the victim's location. Using smartphone technology, the victim can be located in indoor or outdoor environments. When the victim is attacked in outdoor environments, WeDoCare uses GPS to achieve high precision location. On the other hand, when the attack occurs inside a building or at home, where the GPS technology is not available, location is determined using proximity-based technologies: Wi-Fi and Cell-ID, based on our previous work [Tran2014].

Reliability of dissemination and adoption of WeDoCare

Our mechanism will run mainly on a person's own mobile phone, therefore not requiring extra hardware or data connections to work, which is a clear advantage, as the vast majority of the

population already use this sort of device. Quite often, when travelling or wandering around a city or region, the only likely device people carry with them is their mobile phone. This fact points out to implementing the proposed mechanisms on these specific and widely spread devices.

Reliability of prevention

WeDoCare provides danger zones identification, by assisting people in identifying areas where attacks are likely to occur, so they can choose alternative paths around signalled spots or avoid those areas altogether, resulting in a lower probability of attacks.

Reliability of identification of potential victims and perpetrators

The explosion of social networking activities and of Internet of Things (IoT) technologies can be combined to offer vast added-value services for detection of potential victims and perpetrators. This is of key importance since a high percentage of sexual abuses occur in domestic or family environments.

By analysing users' digital footprints in social networks and applying artificial intelligence techniques, we are working on innovative deep learning algorithms that assess user personality with the aim of identifying both potential abusers and victims.

Our team has also a group of psychologists from the University of Coimbra that are working on the concept of leveraging indirect sensing and using the digital footprints (social sensing) to identify critical personalities.

This is something that has seemingly never been attempted before.

Last but not least, WeDoCare strictly respects user privacy, as user's information is only shared with explicit consent.

It is important to be noted that during the initial months of this contest, we have been focusing our work on the mobile phone application. Although we have also been working on the auxiliary node, based on our previous work [Rodrigues2012], [Rodrigues2013], the node is not ready and we do not have evaluation results yet. However, the node will be prepared for tests during Round 2 of the Anu and Naveen Jain Women's Safety XPRIZE contest.

3. WeDoCare features

3.1. General description

Our goal is to provide technology-based solutions within most people's reach (Fig. 2). The use of sensor-enabled smartphones is a promising solution to large-scale data collection [Yang2015]. In fact, the powerful computing and communication capacities, massive market proliferation, and inherent mobility, make Mobile Phone Sensing Systems a much more flexible and cost-effective sensing solution than traditional static sensor devices.

Therefore, we decided to use smartphone-based technologies. With recent developments in machine learning, new applications that use smartphones' sensors to improve the quality of life or to infer human activities are coming to light. Furthermore, all mobile phone devices have a microphone. Despite being rarely regarded as a sensor, this component allows gathering a substantial amount of information. In fact, we can develop many applications using sound to obtain information about the environment (loud environments can be stressful or joyful, depending on the context) and the user's behaviour. While voice can transmit moods and emotions, the microphone can detect screams or gunshots. Much research in the field of scream recognition or gunshot recognition can be found in the literature, but a simple and useful application to help protecting people from violence has never been developed, to the best of the proposers' knowledge.

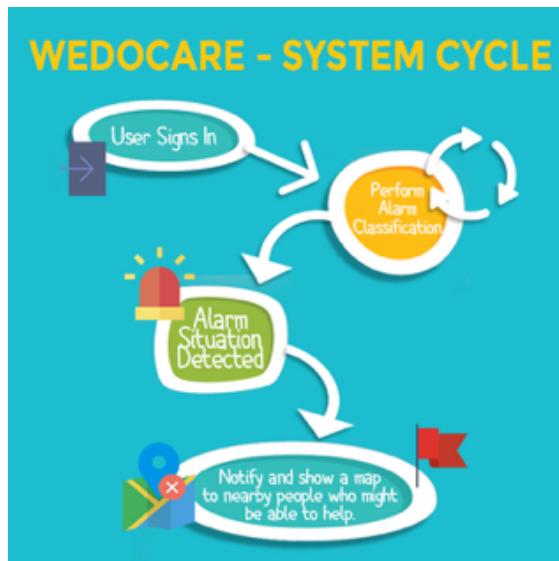


Figure 2 - WeDoCare cycle schematics.

Our idea is unique as it uses smartphones to recognize screams/shouts and accelerometer patterns for the detection of emergency situations, and by triggering collaborative help. Our mechanism is implemented on a person's own mobile phone, which brings significant advantages because these devices are used by the majority of the population. Although our app can be complemented by a small, unobtrusive node to be concealed in women's clothes to

improve the reliability on the detection, WeDoCare also works as an app per-si, so it is not mandatory to purchase or carry additional devices.

The WeDoCare innovative beacon system enables communication with nearby or surrounding people without being limited to an Internet connection. This is an essential requirement for this type of applications, also identified in previous meetings we had with the United Nations for Human Rights. For instance, refugees and migrants often don't have access to a mobile network, or to mobile data communications (Internet), and this beacon system is supported on wireless network meshes, which increases the effectiveness of our application. Because the user does not have to pay for a mobile data plan, the beacon system also provides an alternative solution that is free to exploit.

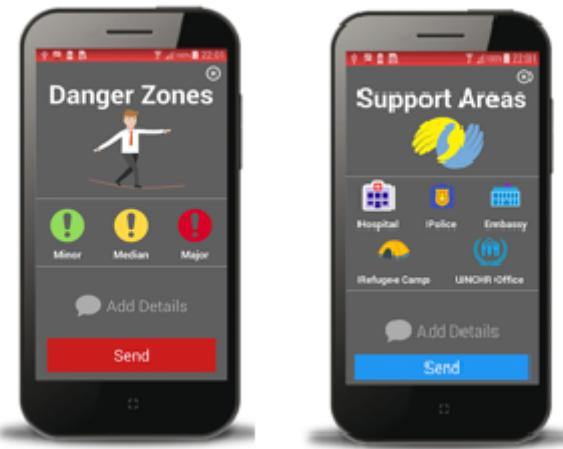


Figure 3- WeDoCare app outlook

We base WeDoCare's specification on the requirements set forth by the Anu and Naveen Jain Women's Safety XPRIZE regulations, discussed in the previous section, and by one distinct feature we think is essential in this kind of systems: Reliability. So, we base our specification in describing all the technical details of the components of WeDoCare and how we increased their reliability.

The other attributes that are required by the specification are, however, not forgotten. Thus, we have:

- a robust trigger (and so, reliable), based on a panic button, scream detection (by an inference algorithm), and accelerometer detection (sudden moves by an inference algorithm);
- reliable connectivity (we can alert other people even without Internet or cellular connection);
- location awareness (our alerts are location-aware: we always include in our alerts information about where the person under threat is located);
- low cost (the cost of our solution is under 40 dollars per user. Indeed it is free if one does not use the auxiliary device);
- inconspicuous (no one will suspect a mobile phone nor the auxiliary device we will build and/or integrate).

Additional WeDoCare features are:

- Data security is maintained at all times and cannot be accessed by third parties. User location is only disclosed under threat or attack situations, as this is vital for reaching out to the victim.
- We provide privacy and privacy controls. We allow the review of all user data ever collected by the application and allow the user to selectively enable or disable features that require that data collection, and to edit alert thresholds.
- We have and will continue to apply user-centered design as we continue to develop WeDoCare.
- We thrive to allow that all features can be accessed and used by the maximum possible number of users.

3.2. WeDoCare user-interface

WeDoCare has a very simple interface so that the user can be easily guided. The application contains a navigation drawer, allowing the user navigate throughout the app. On the map menu, the user is able to see various pins pointing to helpful locales or danger zones.

Danger zones are represented with a red marker and they have a certain transparency rate depending on the associated risk level. Danger zones with high risk level are more opaque, while danger zones with low risk level are more transparent. This allows the user to easily identify different types of danger zones. The user can choose to use heatmaps for intensity representation and visual comfort. On the other hand, we have blue markers which represent helpful locales such as hospitals or police stations. Each map pin has a description associated with it. Any user can add a danger zone or a helpful locale, but this is restricted to three additions a day to prevent spamming or false additions to the map. If a user is abusing the system, she is automatically added to a blacklist and prevented from adding pins during a certain amount of time.

When the user enters or passes through a danger zone, the application generates a notification warning, thus alerting the user to the potential danger. It then suggests the user to take a different route. With this feature, users can stay safe and avoid areas where crimes are more common.

Additionally, the app has a panic button which can also be used as a button to cancel false alarms.

The user can, at any time, activate the beacon system to begin listening for users in danger.

For the design of this application, we used Material Design. Created and designed by Google, Material Design is a design language that combines the classical principles of successful projects with innovation and technology. The goal of Google is to develop a design system that allows unifying the user experience on all of its products on any platform.

The main purpose of Material Design is to create a visual language that synthesizes classic principles of good design with the innovation in technology. Material Design allows developers

to implement a single underlying system that provides a unified experience across platforms and device sizes.

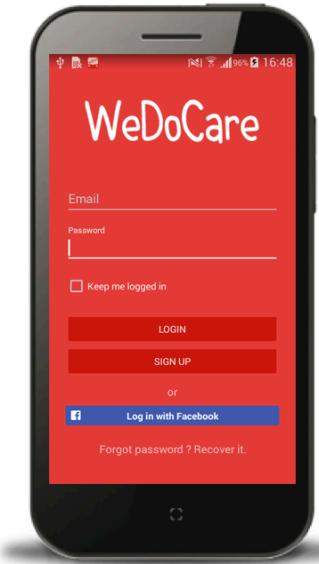


Figure 4 - WeDoCare's login screen

The login screen includes text fields where the users can insert their e-mail and password. Touching a text field places the cursor and displays the keyboard. The type of text field determines what kind of characters are allowed inside the field. Common input types include: text, passwords, number or mixed format (emails). Password input is disguised by default. When the user engages with the text input field, the floating inline labels move to float above the field.

The login screen has three buttons. Two of them are used to login (through Facebook or our login system). The third button takes the user to the registration screen. These buttons, based on the Material Design guidelines, trigger an ink reaction and lifts on press. Raised buttons, such as the ones we use, add dimension to mostly flat layouts. They emphasize functions on busy or wide spaces. Raised buttons behave like a piece of material resting on another sheet – they lift and fill with color on press.

This screen also has a checkbox where the user can toggle the “keep me logged in” feature. This feature allows the user not to have to go through the login process the next time she uses the application.

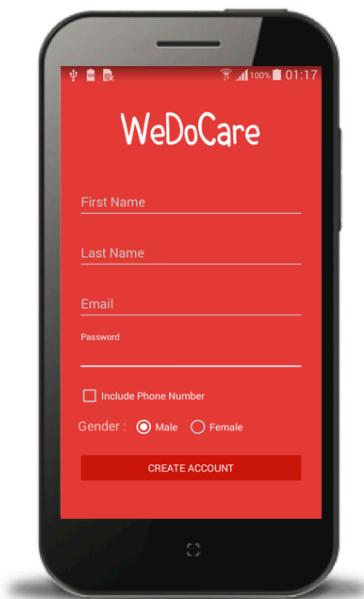


Figure 5 - WeDoCare's registration screen

The registration screen has various text fields, a checkbox and two radio buttons for the input of information required for registration. Radio buttons allow the selection of a single option from a set. The use of radio buttons allows the user to see all available options side-by-side. The text fields are used to insert: first name, last name, e-mail and password. The checkbox is used to optionally provide the user's phone number if he/she chooses to do so, and finally the two radio buttons are used for gender selection.

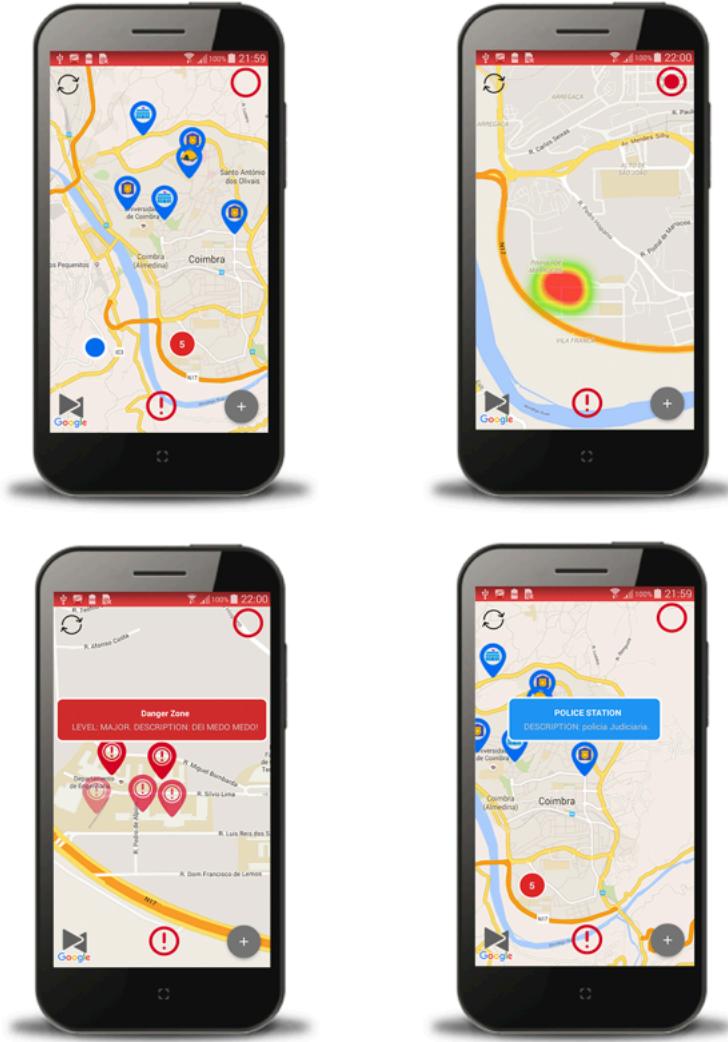


Figure 6 - Various screenshots of the WeDoCare's map screen.

The map screen is where the POIs and the user's current position are shown. A blue sphere represents the current location of the user. A red flag represents an ongoing user attack in the vicinity. POI's are represented by all other pins drawn on the map, namely red markers which represent danger zones and blue markers which represent helpful locales. The map contains four buttons. (described from the top left to bottom right):

- Refresh button: refreshes the Points of Interest on the map.
- Toggle Danger Zones: Shows or hides danger zone heat maps.
- Activate Communications: Activates the hardware required to communicate with other devices through the beacon system.
- Emergency button: Notifies all people around the user about an attack.
- Add POI: Is used to add a point of interest to the map. This button is a Floating Action Button used for a promoted action. Shaped like a circled icon floating above the User

Interface (UI), it has an ink wash upon focus and lifts upon selection. When pressed, it expands onto the screen and contains more related actions. These actions take the user to other menus where the user can add a danger zone or helpful locale.

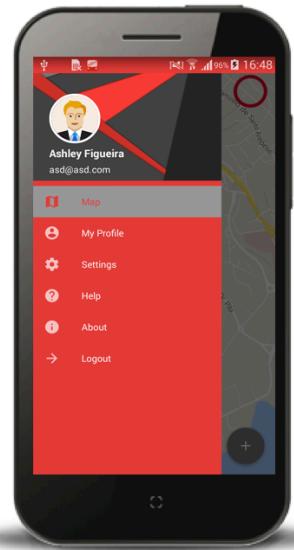


Figure 7 - WeDoCare's navigation drawer screen

The navigation drawer slides in from the left and contains the navigation destinations for the app. That is, the navigation drawer is used to allow the user to navigate through different screens. These screens are: the map, profile, applications settings, help, and about screens. The nav drawer spans the height of the screen, with everything behind it visible but darkened by a scrim. The navigation drawer also includes a log out button.



Figure 8 - WeDoCare's settings screen

The settings screen is where the user can change the background behavior of the application. These include a section for location and a section for the beacon system. The location settings allow the user to have control over the frequency at which the user's position is requested. This has great impact on battery consumption, as we will see in next section. The beacon section is where the user can change the time-to-live of beacon alarms.

The help screen has information about the use of the application, and the about screen has general information on the development of this application.



Figure 9 - WeDoCare's danger zone screen

The Danger Zone screen is where the user can add a danger zone. This has three radio buttons where the user can choose the danger zones' risk level. This is represented as: minor, medium and major. The user can add more information to the danger zone.



Figure 10 - WeDoCare helpful locale screen

The Helpful locale screen is where the user can add a helpful locale. There are various types of helpful locales available right now on the application, such as hospitals and police stations.

There is also a cancel button in the app that can be used to cancel the transmission of a false alert message. Whenever an attack is detected, the user has 8 seconds to deactivate the alarm.

3.3. Ladies' clothes node

3.3.1. Introduction

To increase the reliability of WeDoCare we propose an additional, unobtrusive, small device to be attached to women's clothes. This small device has an accelerometer, a barometer and a button, so that these elements can be used for detection. This is particularly important in the case of women, as sometimes they leave their mobile phones in their handbag.

This device has another important advantage: it can be hidden from perpetrators, as it is placed covertly and can detect sudden and unusual movements.

Both the mobile phone application and this additional device can generate the alert. The auxiliary device is connected to the phone through Bluetooth Low Energy (BLE) so the mobile phone can transmit the alert. As is the case of the mobile application, when an attack is detected the user has 8 seconds to cancel the transmission of the alert message.

We implemented a first version prototype using some off-the-shelf components (mostly Arduino based with discrete modules) but, since the rounds of this contest have tight deadlines, it was important to give priority to getting data sets for the training procedures of our Artificial Intelligence (AI) algorithms.

As a second phase we are developing a custom node to get a more compact device and to reduce energy consumption. This is nothing new to our team, as in the past we have collaborated in the development of devices such as the Hermes modular platform [Rodrigues2012], comprising two nodes that can be used individually or in conjunction according to the application scenarios [Rodrigues2013]. Hermes' architecture is detailed in Figure 11 and each node is presented in Figure 12.

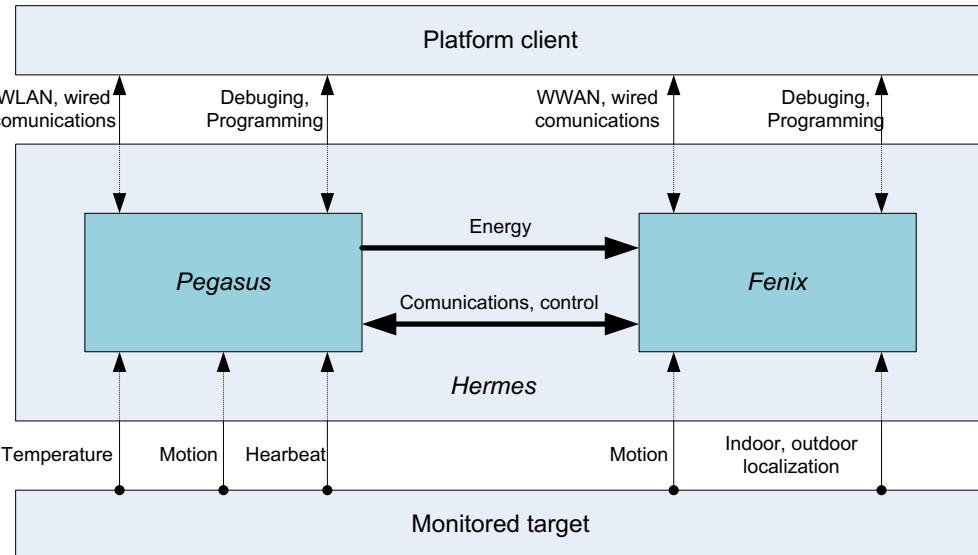


Figure 11 - Hermes simplified architecture

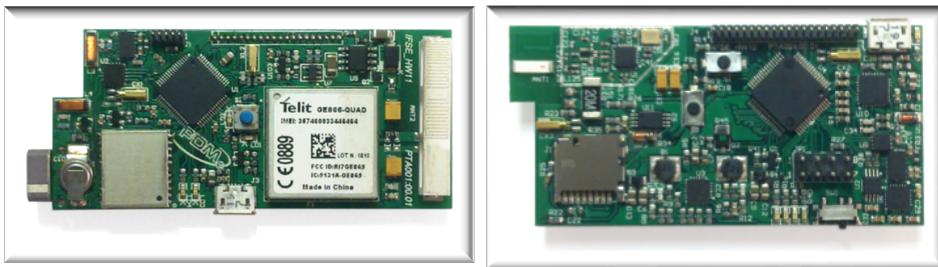


Figure 12 - Fenix (on the left) and Pegasus (on the right)

This section is further organized in the following way: in the next sub-section we detail the device requirements and, based on these, a draft architecture was developed and is presented. Finally the section concludes by presenting some implementation issues.

3.3.2. Requirements

Based on the contest requirements (table 1), we defined a specific set of requirements to our auxiliary device:

Device's requirements:

- Detect attacks when the victim is conscious and, consequently, she can contribute on sending the alert message (even if her arms are pinned).
- Even in the case the victim is not conscious the system must detect the attack and send the alert message.
- Response time - identification and alert message sent, should be less than 8 seconds.

- Contribute to improve the location of the attack.
- The cost should be less than 40\$.
- The auxiliary device must communicate with the mobile phone using a widely supported technology like BLE.
- Easy mechanism to send an alarm and cancel a false alarm.
- The communication with the mobile phone should be robust.
- Not be detectable by the attacker.
 - It can be put in the pocket or attached to the clothes using velcro.
 - Size must be less than one coin of 2€ (diameter of 26mm)
- Be comfortable.
- Minimal maintenance required.

3.3.3. Architecture

The node architecture is presented in Figure 13. It comprises:

- a small panic button
- an accelerometer
- a barometer
- a microcontroller unit
- a BLE radio
- two LEDs for debugging purposes
- a power supply unit
- a small plastic case that holds the electronics

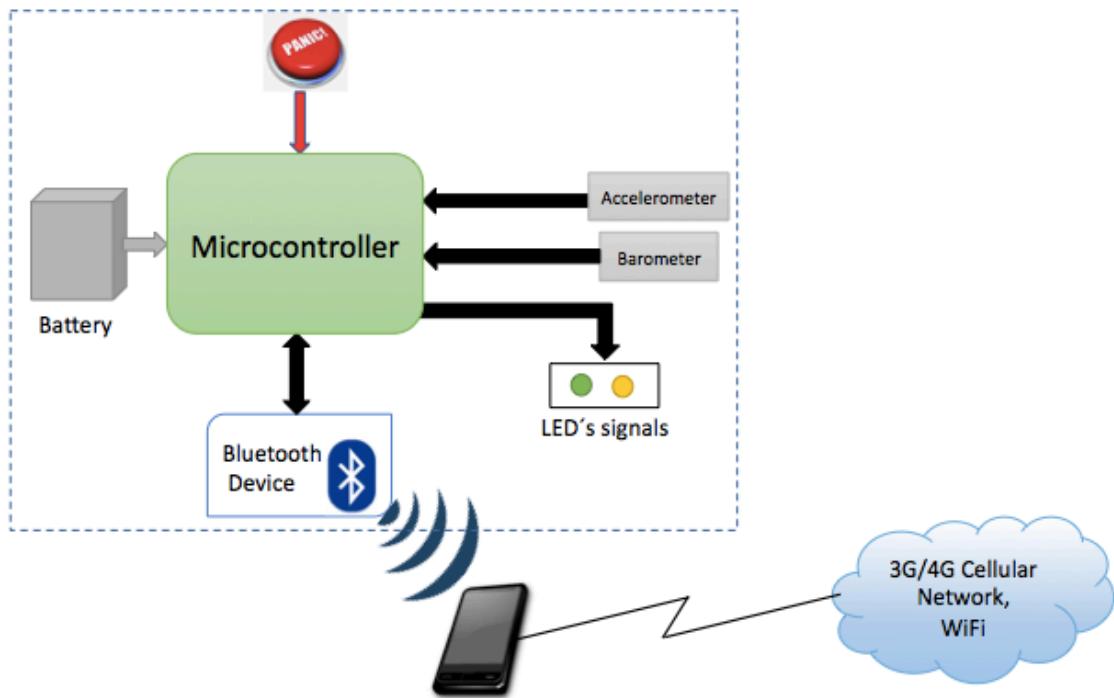


Figure 13 - Ladies' clothes node architecture

3.3.4. Implementation details

We are working on a second version prototype that implements all the functions in a compact PCB that will be installed inside a plastic case. The final appearance should not differ much from a device like the one presented in Figure 14 that has 25mm diameter. Our implementation will be quite diverse, as will be detailed in the next paragraphs, but this image helps to clarify what we are implementing.

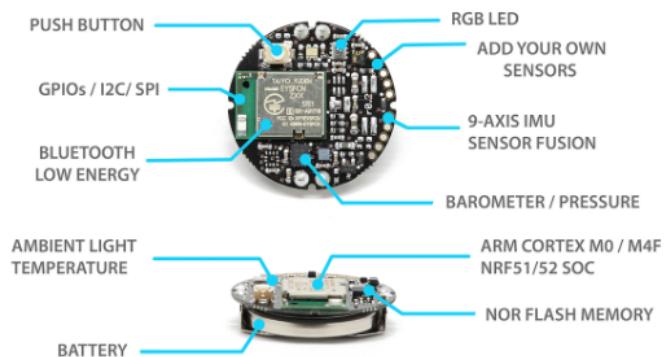


Figure 14 - A node from mbientlab.com

This node will be protected by a plastic case like the ones presented in Figure 15. Those are used for housing alarm controls (for houses, cars, etc.), and they are very cheap (around 2€).

We think using a case like those could contribute to lowering the device price and to making it inconspicuous by hiding its real functionality.

Additionally, this enables us to save time and money by avoiding developing a new case.



Figure 15 - Two cases used in car alarm controls

The device preferred location is inside a pants pocket. In cases where this is not possible it should be attached to the ladies' briefs using velcro.

The panic button enables the victim to generate an alarm by pressing it. The system acknowledges this by playing a predefined sound on the user smartphone. Additionally, this button, when pressed during more than 5 seconds, automatically cancels a previous alert (as mentioned before, the user has 8 seconds to cancel an alert).

The accelerometer enables the victim to generate an alert (even in case it cannot use their hands) because the accelerometer can detect specific gestures such as knocking on the floor twice. We want to go further and use the accelerometer to detect when the victim is being undressed even in case she is unconscious.

The main reason to support a barometer is to help in 3D localisation (Round 2 functionality). In fact several works [Banerjee2015] demonstrated the advantage of using a barometer to detect floor location inside a building. We want to provide an energy efficient device that can last for months (half a year would be the target) with a coin cell.

From our previous experience in developing WSN-based solutions, we know this requires very low power hardware and an energy efficient operating system. After surveying the market for available development kits that we could use to implement a second generation prototype, we decided to use the TI SensorTag (<http://www.ti.com/tool/tidc-cc2650stk-sensortag>) based on the following reasons:

- it supports all the hardware we require;
- it provides a good software ecosystem;
- the boards design is open (access to BOM, PCB design, schematics);
- low cost (29\$).

Figure 16 presents the SensorTag dimensions. Device hardware architecture is presented in Figure 17.



Figure 16 - SensorTag dimensions (from TI site)

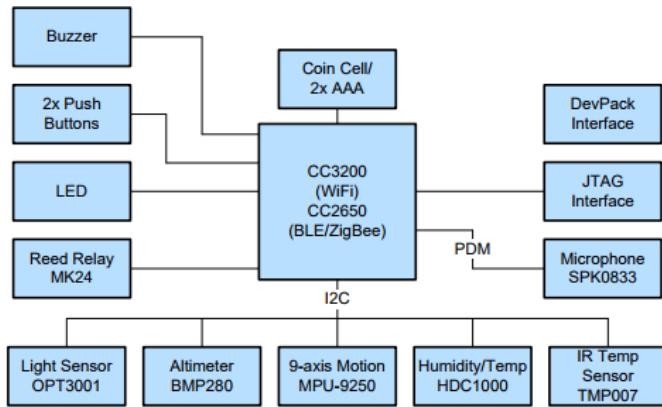


Figure 17- SensorTag architecture (from TI site)

TI provides several options for the SensorTag communication technologies (WiFi, BLE, ZigBee, narrow band). In this context, we decided to use the CC2650 SoC that includes a Cortex M3 based MCU and supports a BLE stack.

Energy consumption is crucial. According to the manufacturer, this SoC has the following characteristics:

- Active-Mode RX: 5.9 mA
- Active-Mode TX at 0 dBm: 6.1 mA
- Active-Mode TX at +5 dBm: 9.1 mA
- Active-Mode MCU: 61 μ A/MHz
- Active-Mode MCU: 48.5 CoreMark/mA
- Active-Mode Sensor Controller: 8.2 μ A/MHz
- Standby: 1 μ A (RTC Running and RAM/CPU Retention)
- Shutdown: 100 nA (Wake Up on External Events)

We want to take advantage of the low power modes (standby and shutdown) by enabling the node to sleep most of the time, being awakened either by the movement sensor (in this case, a programmable motion processing unit that can generate an interrupt when some predefined

movement happens) or by the alert button. Adding to this, a sporadic health status message has to be sent to the smartphone.

The SensorTag can be programmed using the TI development ecosystem that includes an IDE, drivers and a Real Time Operating System (RTOS). It is also a primary platform for the Contiki operating system (a highly energy-efficient operating system used in several IoT solutions).

We are developing the node firmware using the TI tools and, at the same time, designing a new node (similar to Figure 14) based on the SensorTag design information provided in the SensorTag design kit (this includes BOM, schematics, and PCB design files).

We are working on a node with miniaturized dimensions, 25 mm diameter x 10 mm height, so that its use is not uncomfortable, given its small size and weight. Its production cost will be less than 35\$.

4. Requirements

4.1. Requirements of the contest

According to the rules of the contest, the Anu and Naveen Jain Women's Safety XPRIZE will award the most accurate and most usable technology solution that can:

- Trigger location-accurate alerts in emergency situations even in low-connectivity scenarios.
- Transmit alerts to a network of responders, and rapidly provide a response to the user within 90 seconds that help is on its way.
- Exhibit a novel approach to building or combining existing and/or emerging technologies to better connect users and responders under \$40 of the device cost.

The Women's Safety XPRIZE will require the solutions to work in a variety of situations in which women may be at risk. The final Round 2 testing will require teams to demonstrate the effectiveness of their solution in several situations. A variety of situations will be proposed by the Judging Panel, from which each team must choose three examples of such scenarios:

- Scenario 1: User is located on the fourth floor of a corporate office environment with access to high connectivity to Wi-Fi and mobile networks; user's arms are physically restrained.
- Scenario 2: User is in a moving vehicle with access to intermittent Wi-Fi and mobile network connectivity, to operate a mobile phone.
- Scenario 3: User is in a room with no Wi-Fi connectivity and low mobile network strength, and has access to a smartphone.

It is to be noted that above examples of scenarios are just for understanding and they may or may not be present in the final list of proposed scenarios by the Judging Panel.

Table 1 - Main system attributes (required)

Feature	Detail
Robust Trigger	The solution requires minimal user input to trigger an alert across all the three scenarios chosen by the team. Users must be able to cancel alert triggers quickly and easily with a single action.
Reliable Connectivity	The solution must be able to send and receive an alert ping even when the primary medium of connectivity fails and the solution should be able to send signals over a period of time.
Location Awareness	Must provide an accurate multi-dimensional location to allow responders to pinpoint user location in all user scenarios specified in Competition Overview.
Low Cost	The device cost must be less than \$40.
Inconspicuous	The solution should not be easily identified or disabled by a non-user in an emergency

	condition.
--	------------

Table 2 - Main system features (required)

Security	Technology must be designed for optimal data security.
Privacy	User interface which allows (a) full review of all user data collected by the technology, (b) customization of details of data and location sharing, (c) review and edit alert threshold.
User-Centered Design	Teams have considered inputs from potential users.
Accessibility	All features can be accessed and understood by the maximum possible number of users.

4.2. Compliance with the requirements and comparison with competitors

Concerning the state-of-the-art, several applications have been developed to solve similar issues, although they present several limitations. Safelet [Safelet], for instance, is a bracelet that lets a user warn others that she/he is in danger. This particular piece of hardware contains a button that, once triggered, issues an alarm to the user's friends and family. The user's smartphone also begins recording. This is useful because it gives the ability to check later what really happened regarding a particular emergency situation. However, this solution has a significant limitation, which is the extra hardware the user needs to purchase. The bracelet has non-negligible cost, and certainly not affordable to a high number of low-income, vulnerable users, such as the ones we want to help with WeDoCare. Furthermore, emergency contacts may be unable to help, because they might be outside the victim's vicinity.

Another similar solution is Athena [Athena]. It is based on a round button that clips onto a person's belt and is dedicated to preventing physical assaults, by emitting loud alarms whenever the button is clicked. It also sends out text messages with the users' location to their designated emergency contacts. This solution is similar to the previous one, with the advantage that it can be used anywhere, that is, it can be hidden from perpetrators, unlike Safelet, which is placed on the users' wrist and can be easily removed. However, it also requires a user to buy extra hardware, which is a significant obstacle to our target users.

The Anu and Naveen Jain Women's Safety contest has 85 competitors from several countries. Almost all competitor solutions are based on buttons, rings, bracelets, apps for mobile phones that rely on shaking the phone, and spectacles. Normally they send a message to the person's contacts or police stations. Some of the solutions are also based on subscription services, and only some support privacy mechanisms.

Comparatively, our solution:

- is free (or less than 35\$ if it is complemented by the auxiliary node to be attached to the user's clothes).

- Although WeDoCare has also a panic button, it relies on an automatic system that detects violent attacks against the user, which overcomes scenarios where arms are physically restrained. Often when under attack, women are taken by surprise, which does not allow them to carry out common actions (pressing a button or picking up the mobile phone to call someone). On the other hand, screaming and/or moving desperately is something that is both instinctive and instantaneous.

- It is used in real-time.

- It is difficult to detect. In the case of the mobile phone app, the aggressor does not know that the application is installed in the mobile phone. In the case of the clothes' node, it is so small that it is difficult to detect.

WeDoCare is also innovative:

- It is innovative in terms of supported detection methods.

- It is innovative in terms of the complementary communication system used when no Internet or GSM connections are available.

- It uses an innovative social solution based on sending alarms to surrounding citizens, giving them a chance to help and collaborate by helping others staying safe.

- The application also warns the user whenever she/he is passing within a zone where attacks occur more often, so that these sites can be avoided.

- In the future, it will use an innovative approach based on social sensors to identify potential victims and attackers.

And, most important, our solution is reliable:

- It is reliable in detecting the threat.

- It is more reliable in contacting and requesting help - WeDoCare also sends the alert messages when no cellular or Internet connection is available.

5. Conclusion

In this document we presented WeDoCare, a system that uses smartphone's sensors, in particular the microphone and the accelerometer, to detect, in an automated way and in real-time, situations of violent attacks against users.

WeDoCare is highly committed to promoting a technology transfer to the society, in terms of product design and development of the research findings. From its inception, the project aims at bringing its research results to the society. The involved partners are fully committed to ensuring the maximisation of the project results' exploitation, due to their wide networks of contacts and collaborating entities.

References

- [Athena] Athena. <http://mashable.com/2015/11/03/athena-indiegogo/#RB1hfqUY9Eq0>
- [Ballou2008] Glen M. Ballou, Editor, "Handbook for Sound Engineers", Fourth Edition, , Chapter 2, Elsevier 2008.
- [Banerjee2015] D. Banerjee, S. K. Agarwal, and P. Sharma, "Improving Floor Localization Accuracy in 3D Spaces Using Barometer," in Proceedings of the 2015 ACM International Symposium on Wearable Computers, 2015, pp. 171–178.
- [Rodrigues2012] A. Rodrigues et al., "Hermes: A versatile platform for wireless embedded systems," in 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012, pp. 1–9.
- [Rodrigues2013] A. Rodrigues, J. S. Silva, and F. Boavida, "iSenior—A Support System for Elderly Citizens," IEEE Trans. Emerg. Top. Comput., vol. 1, no. 2, pp. 207–217, Dec. 2013.
- [Safelet] Safelet. <http://www.safelet.com/>
- [Tran2014] T. Dien Tran, J. Oliviera, J. Sá Silva, V. Pereira, N. Sousa, D. Raposo, F. Cardoso, "A Scalable Localization System for Critical Controlled Wireless Sensor Networks", The 6th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT 2014), October 2014, St. Petersburg (Russia), ISBN 978-1-4799-5290-8.

B. Anu and Naveen XPRIZE application

C

Logos



Figure C.1: Proposed WeDoCare logos

C. Logos

D

Privacy policy

Política de privacidade

Esta secção informa os utilizadores acerca da política de privacidade da aplicação WeDoCare (“o sistema”) e ajuda-os a compreender os dados que o sistema recolhe, o porquê de os recolher e como os utiliza. É importante que este documento seja lido com atenção na sua integra.

1. Informações utilizadas pelo sistema

1.1 Informações recolhidas pelo sistema

- Informações de localização
A informação de localização é recolhida automaticamente quando o utilizador tem o acesso à localização ativo. Esta informação é recolhida utilizando várias tecnologias e sensores: GPS, pontos de acesso Wi-Fi e torres de redes móveis.
- Informações de dispositivo
No momento de instalação o sistema recolhe o número de série do cartão SIM. Esta informação é recolhida cada vez que o sistema está prestes a enviar uma SMS para a Polícia de Segurança Pública (PSP). Quando a SMS é enviada para a PSP o número telefónico de origem é o do utilizador.
- Informação de conexão à Internet
O sistema determina se há algum tipo de conexão à internet quando a aplicação é iniciada, recebe informação sobre mudanças no estado de conexão, i.e., quando a conexão é desligada e ligada ou quando precisa de executar alguma ação que requeira conexão à Internet. Não é determinado, em momento algum, o tipo de ligação à Internet (Wi-Fi, dados móveis, conexão Ethernet, WiMAX).

1.2 Informações indicadas pelo utilizador

- Morada da localização atual
O utilizador pode inserir a qualquer altura a informação detalhada da localização onde se encontra. Esta informação é constituída pelos seguintes campos: rua, número de porta, andar, fração e localidade. Esta informação é convertida para coordenadas quando há acesso à Internet.
- Reconhecimento de voz
Quando o reconhecimento de voz está ativo, o sistema recebe informação de som de forma contínua e processa esta informação para analisar se nela está a palavra-chave ‘socorro’.

1.3 Armazenamento local

O sistema armazena localmente as informações de envio de SMS, mais precisamente a data e hora de envio e se este foi sucedido. Estas informações são

guardadas numa base de dados da aplicação para construir um histórico de envio de sms. A informação de morada da localização atual também é guardada (se existir) localmente. Não é guardado um histórico de localizações de utilizador porque sempre que existe uma nova informação, a informação antiga é eliminada do sistema.

O número de série do cartão SIM é guardado localmente e permanentemente pelo sistema e não é possível de ser alterado.

2. Como o sistema utiliza as informações que recolhe

As ações consideradas críticas (acesso à localização, envio de SMS, leitura do número de série do cartão SIM, recolha de som) são recolhidas com consentimento prévio do utilizador.

As informações recolhidas pelo sistema servem apenas para garantir todas as funcionalidades do mesmo. Estas informações, com exceção das indicadas no ponto 1.3, são recolhidas no modo ‘obter e esquecer’, ou seja, são obtidas, processadas para a tomada de decisões e depois ‘esquecidas’, não sendo guardadas em memória localmente ou em alguma base de dados remota.

O número de série do cartão SIM é apenas recolhido uma vez e serve para garantir que o sistema é apenas utilizado por pessoas autorizadas. No caso de passagem do telemóvel para pessoas não autorizadas por venda ou furto do dispositivo, situações em que é habitual a troca do cartão SIM, a funcionalidade de envio de SMS para a PSP está bloqueada. Esta ação tem como objetivo prevenir a mobilização inadequada de recursos de emergência.

As informações explícitas no ponto 3, apesar de guardadas num modo permanente, não estão acessíveis a terceiros (incluindo-se aqui a Universidade de Coimbra, responsável pelo desenvolvimento do sistema, e suas instituições parceiras).

Em caso de emergência, as informações de localização (se existir) e número de telemóvel do utilizador são partilhadas com a PSP para que esta saiba a localização da situação e consiga prestar auxílio à vítima.

Concluindo este tópico, as informações a que o sistema tem acesso são apenas as necessárias para detetar uma agressão ao utilizador, conhecer a localização deste ataque e alertar as autoridades competentes do mesmo e não se destinam a outra ação que não esteja mencionada neste documento.

3. Partilha de informação por motivos legais

No caso de um processo legal que resulte do envio de SMS para a PSP cabe ao utilizador lidar com a disponibilização de informação armazenada pelo sistema, caso seja necessário por lei.