

Faculdade de Engenharia da Universidade do Porto



**Sistema de identificação e localização baseado em
dispositivos de comunicações sem fios**

Ricardo Manuel Moreira Marques Osório

Dissertação realizada no âmbito do
Mestrado Integrado em Engenharia Electrotécnica e de Computadores
Major Telecomunicações

Orientador: Prof. Dr. José Ruela
Co-orientador: Eng. Carlos Pinho

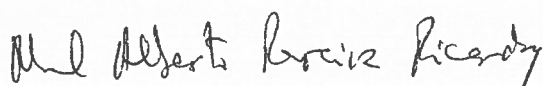
Julho 2011

A Dissertação intitulada

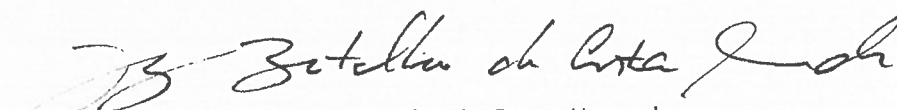
“Sistema de Identificação e Localização Baseado em Dispositivos de
Comunicações Sem Fios”

foi aprovada em provas realizadas em 18-07-2011

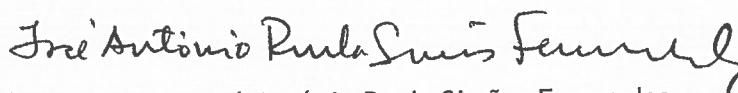
o júri



Presidente Professor Doutor Manuel Alberto Pereira Ricardo
Professor Associado do Departamento de Engenharia Electrotécnica e de
Computadores da Faculdade de Engenharia da Universidade do Porto



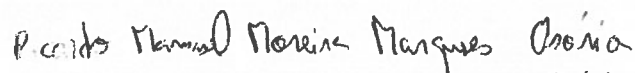
Professor Doutor Jorge Botelho da Costa Mamede
Professor Adjunto do Departamento de Engenharia Electrotécnica do Instituto
Superior de Engenharia do Porto



Professor Doutor José António Ruela Simões Fernandes
Professor Associado do Departamento de Engenharia Electrotécnica e de
Computadores da Faculdade de Engenharia da Universidade do Porto

Mestre Carlos Nuno Oliveira Pinho
Investigador do INESC-Porto

O autor declara que a presente dissertação (ou relatório de projeto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extractos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são corretamente citados.



Autor - Ricardo Manuel Moreira Marques Osório

Faculdade de Engenharia da Universidade do Porto

Resumo

A evolução tecnológica contínua a que assistimos na última década tem permitido melhorar as funcionalidades e assim aumentar os benefícios oferecidos pelos sistemas de informação e comunicação com que interagimos no dia-a-dia. Actualmente, a utilização de sistemas que permitam aceder em tempo real à identificação e localização de pessoas ou materiais tornou-se numa mais-valia para várias empresas. Essa mais-valia enquadra-se numa lógica de operacionalização, rapidez de resposta e fidelização de clientes, em particular na indústria, bem como numa lógica de controlo de pessoas e activos, ao nível de prestadores de serviços, tendo como principais consequências o aumento da produtividade e a redução de custos operacionais. Com a contínua redução de preço, crescente miniaturização e o aumento do poder computacional dos dispositivos de comunicações sem fios (*wireless*), assiste-se a uma disseminação deste tipo de sistemas e à sua introdução nas mais diversas áreas de aplicação (e.g., saúde, industrial, empresarial, etc.) como aparecimento no mercado de várias soluções de localização e identificação.

O presente documento caracteriza e analisa a situação actual relativamente a este tipo de sistemas e aponta uma solução para o problema em estudo oferecendo diferenciação em relação às soluções actualmente disponíveis no mercado.

A solução implementada distingue-se das soluções no mercado na medida em que implementa um conjunto de funcionalidades inovadoras, tais como permitir que num só sistema coexista a capacidade de localização a nível interior e exterior. As tecnologias utilizadas (*WiFi*, 3G e GPS), favorecem a configuração e instalação do sistema, a segurança da rede, a utilização de *hardware* com outro tipo de funcionalidades (e.g. *smartphones* Android que permitem a troca de notificações entre utilizadores do sistema) bem como a utilização de *software* adaptado às necessidades deste projecto.

Abstract

The continuous technological evolution we have witnessed in the last decade has allowed improving the features and thus the benefits offered by information and communications systems we interact with every day. Currently, the use of systems that allow access to real-time tracking and identification of people or materials has become a valuable asset for many companies. This added value fits into a logic of operationalization, responsiveness and customer loyalty, particularly in industry, as well in a logic of control of people and assets for service providers, having as main consequences an increase in productivity and reduced operating costs. With the continuous price and size reduction and increasing computational power of wireless communications devices, we are witnessing a widespread use of such systems and their introduction in various application areas (e.g. healthcare, industry, business, etc.) as well as the emergence of various solutions on the market of tracking and identification.

This paper characterizes and analyzes the current situation with regard to such systems and suggests a solution to the problem under study providing differentiated solutions from the ones on the market.

The implemented solution differs from others currently on the market as it implements a set of innovative features, such as having in a single system the ability to perform indoor and outdoor tracking. The technologies (WiFi, 3G and GPS) that were adopted favor the configuration and system installation, network security, the use of other hardware features (e.g. Android smartphones which allow the exchange of messages among users of the system) as well as the use of software specific to the needs of this project.

Agradecimentos

Quero agradecer aos meus orientadores, Prof. José Ruela e Eng. Carlos Pinho por todo o tempo e ajuda disponibilizada no desenvolvimento do projecto e na elaboração deste documento.

Índice

Resumo	v
Abstract	vii
Agradecimentos	ix
Índice	xi
Lista de figuras	xiv
Lista de tabelas	xvii
Abreviaturas e Símbolos	xviii
Capítulo 1	21
Introdução	21
1.1 - Organização do documento	22
1.2 - Objectivos e contexto do problema	23
Capítulo 2	25
Estado da arte	25
2.1 - Levantamento de tecnologias	25
2.1.1 - RFID - Radio Frequency Identification	26
2.1.2 - ZigBee	28
2.1.3 - WiFi	30
2.1.4 - Comparação de tecnologias	33
2.2 - Técnicas de localização utilizadas em RTLS	36
2.2.1 - <i>Nearest Access Point</i>	36
2.2.2 - <i>Time Difference of Arrival (TDoA)</i>	37
2.2.3 - <i>Received Signal Strength Indicator (RSSI)</i>	37
2.3 - Levantamento de soluções	39
2.3.1 - RFID - Radio Frequency Identification	39
2.3.1.1 - BlueTag - Patient and Safety Security	39
2.3.1.2 - Kimaldi - “Controlo de vagueantes”	40
2.3.1.3 - Kimaldi - “Controlo de presença, acesso e recursos”	41
2.3.1.4 - Kimaldi - “Sistema de localização de pessoal hospitalar”	42
2.3.1.5 - Kimaldi - “Controlo de presença e rastreabilidade logística”	43
2.3.1.6 - RFID Centre - “Indoor RFID Tracking (TagMobile)”	43
2.3.2 - ZigBee	44
2.3.2.1 - CLEODE - “LifeNurse”	44

2.3.3 - WiFi	45
2.3.3.1 - Ekahau - “Real-Time Location System”	45
2.3.4 - Comparação das várias soluções.....	48
Capítulo 3	51
Descrição do sistema.....	51
3.1 - Listagem das funcionalidades	51
3.2 - Listagem de requisitos.....	52
3.2.1 - Requisitos funcionais	52
3.2.2 - Requisitos não funcionais	53
3.3 - Tecnologias e técnicas utilizadas	53
3.4 - Arquitectura do sistema	55
3.4.1 - Servidor Web com acesso à base de dados.....	56
3.4.2 - Pontos de acesso à rede de localização	57
3.4.3 - <i>Smartphones</i> com sistema operativo Android	58
Capítulo 4	61
Desenvolvimento do sistema	61
4.1 - Base de dados	61
4.1.1 - Mapeamento dos pontos de acesso.....	62
4.2 - Servidor Web	64
4.2.1 - Interface de administração do servidor <i>Web</i>	65
4.2.2 - Funcionamento do <i>parser</i> do servidor <i>Web</i>	66
4.3 - Aplicação Android	68
4.3.1 - Ecrã de autenticação	68
4.3.2 - Aba “Estado”.....	70
4.3.3 - Aba “Mensagens”.....	71
4.3.4 - Aba “Perfil”	74
4.3.5 - Serviços da aplicação Android	76
4.3.6 - Localização interior (Serviço de <i>handover</i> WiFi).....	78
4.3.7 - Localização exterior (Serviço de <i>handover</i> 3G)	81
4.3.8 - <i>Proxy</i> INESC Porto	82
Capítulo 5	85
Testes e análise de resultados	85
5.1 - Ambiente e condições de teste	85
5.2 - Autonomia	85
5.2.1 - Autonomia em <i>standby</i>	86
5.2.2 - Autonomia de localização interior	86
5.2.3 - Autonomia de localização exterior	86
5.3 - Precisão de localização.....	87
5.3.1 - Localização interior.....	87
5.3.1.1 - Teste 1: Teste genérico	87
5.3.1.2 - Teste 2: Teste com utilizador em movimento constante	88
5.3.1.3 - Teste 3: “Caso especial” Piso -1	90
5.3.1.4 - Teste 4: “Caso especial” Piso 3	92
5.3.2 - Localização exterior	93
5.3.2.1 - Teste: Percurso INESC Porto - Cantina FEUP	94
5.4 - Envio, recepção e outras funcionalidades de mensagens	97
5.4.1 - Envio e recepção de mensagens	98
5.4.2 - Notificações de recepção de mensagens	99
5.4.3 - Resposta e “resposta rápida” a mensagens.....	100
5.4.4 - Remoção de mensagens da caixa de entrada	101
Capítulo 6	103
Conclusões e trabalho futuro	103

Referências.....	105
Anexos.....	109
A - Modelo relacional	109
B - Modelo entidade associação	111

Lista de figuras

Figura 2.1 - Exemplo de arquitectura da tecnologia RFID.	27
Figura 2.2 - Diferentes topologias de uma rede <i>ZigBee</i>	30
Figura 2.3 - Modos de configuração básicos na tecnologia <i>WiFi</i>	31
Figura 2.4 - Canais <i>WiFi</i> disponíveis na frequência 2.4 GHz.	32
Figura 2.5 - Exemplificação do modo de funcionamento das técnicas RSSI e TDoA.	38
Figura 2.6 - Pulseira BlueTag.	39
Figura 2.7 - Aspecto geral da solução BlueTag.....	40
Figura 2.8 - <i>Reader</i> RFID SYRD245-1N e <i>tag</i> RFID activa SYTAG245245_TM.	40
Figura 2.9 - Aspecto do <i>reader</i> e <i>tags</i> utilizados.	42
Figura 2.10 - Exemplo de funcionamento do sistema LifeNurse.	44
Figura 2.11 - Pulseira ZCare, receptor Ubee e imagem do <i>software</i> CleoBee.....	45
Figura 2.12 - Arquitectura Ekahau RTLS.	46
Figura 2.13 - <i>Tag</i> Ekahau T301BD.	47
Figura 3.1 - Esquemático do sistema implementado (localização interior e exterior).	56
Figura 3.2 - Planta do piso 3 do edifício INESC Porto com os APs existentes assinalados.....	57
Figura 4.1 - Introdução de um novo ponto de acesso no sistema.	65
Figura 4.2 - Consulta das mensagens recebidas por um utilizador.	65
Figura 4.3 - Ligação do servidor <i>Web</i> à base de dados.	66
Figura 4.4 - <i>Parser</i> do servidor Web - Envio de mensagens.	66
Figura 4.5 - <i>Parser</i> do servidor Web - Listagem de mensagens recebidas.	67
Figura 4.6 - <i>Parser</i> do servidor Web - Remoção de mensagens.	67
Figura 4.7 - Ecrã inicial.	69

Figura 4.8 - Ecrã de definições.	70
Figura 4.9 - Aba de estado que é iniciada por omissão após autenticação.	71
Figura 4.10 - Aba que apresenta o menu de mensagens.	72
Figura 4.11 - Composição e recepção de mensagens.	73
Figura 4.12 - Interação com mensagens recebidas.....	74
Figura 4.13 - Ecrã de perfil	75
Figura 4.14 - Ecrã de escolha de um estado predefinido.....	76
Figura 4.15 - Notificação de mensagens por ler.	77
Figura 4.16 - Técnica de localização presente no serviço de <i>handover</i> <i>WiFi</i>	78
Figura 4.17 - Fluxograma do serviço de <i>handover</i> <i>WiFi</i>	79
Figura 4.18 - Fluxograma do mecanismo de <i>handover</i> 3G.....	82
Figura 5.1 - <i>Screenshot</i> dos resultados obtidos para o teste 1.	88
Figura 5.2 - <i>Screenshot</i> do resultado nº1 obtido para o teste 2.	89
Figura 5.3 - <i>Screenshot</i> do resultado nº2 obtido para o teste 2.	89
Figura 5.4 - <i>Screenshot</i> do resultado nº3 obtido para o teste 2.	89
Figura 5.5 - <i>Screenshot</i> do resultado com <i>handover</i> de 1 segundo obtido para o teste 2.....	90
Figura 5.6 - Mapa do piso -1.....	91
Figura 5.7 - <i>Screenshot</i> do resultado nº1 obtido para o teste 3.	91
Figura 5.8 - <i>Screenshot</i> do resultado nº2 obtido para o teste 3.	92
Figura 5.9 - <i>Screenshot</i> do resultado nº1 obtido para o teste 4.	92
Figura 5.10 - <i>Screenshot</i> do resultado nº2 obtido para o teste 4.	93
Figura 5.11 - <i>Screenshot</i> do resultado nº3 obtido para o teste 4.	93
Figura 5.12 - Figura demonstrativa do percurso efectuado (a amarelo).....	94
Figura 5.13 - Marcação dos pontos iniciais e finais registados pela aplicação (A' e B').	95
Figura 5.14 - <i>Screenshot</i> do resultado obtido para a localização exterior.	96
Figura 5.15 - Marcação dos pontos chaves medidos ao longo do percurso.	97
Figura 5.16 - Vista da mensagem enviada por Darth Vader e recebida por Luke Skywalker...	98
Figura 5.17 - Notificação de mensagens.	99
Figura 5.18 - Demonstração do mecanismo de resposta.....	100
Figura 5.19 - Mensagem pré-definida enviada através da resposta “rápida”.	101

Figura 5.20 - Mecanismo de remoção de mensagens.	102
--	------------

Lista de tabelas

Tabela 2.1 – Serviços/Soluções de localização.	26
Tabela 2.2 – Tabela comparativa das variantes da norma 802.11.....	31
Tabela 2.3 – Tabela comparativa de tecnologias de comunicação sem fios.	33
Tabela 2.4 – Tabela resumo de soluções analisadas.	48
Tabela 3.1 – Tabela comparativa dos vários sistemas operativos móveis considerados.	54
Tabela 3.2 – Quota global de mercado dos sistemas operativos móveis considerados.	54
Tabela 3.3 – Especificações técnicas do <i>smartphone</i> Samsung Galaxy S.	59
Tabela 4.1 – Mapeamento dos pontos de acesso com SSID INESCP-visita.	63
Tabela 4.2 – Descrição dos perfis predefinidos.	75
Tabela 4.3 – Exemplificação de situações de <i>handover WiFi</i>	81
Tabela 5.1 – Autonomia de localização interior.	86
Tabela 5.2 – Autonomia de localização exterior.	86
Tabela 5.3 – Comparação das coordenadas reais com as registadas.	95

Abreviaturas e Símbolos

Lista de abreviaturas (por ordem alfabética)

3G	<i>Third Generation</i>
AES	<i>Advanced Encryption Standard</i>
AoA	<i>Angle of Arrival</i>
AP	<i>Access Point</i>
BER	<i>Bit Error Ratio</i>
BSSID	<i>Basic Service Set Identifier</i>
CCK	<i>Complementary Code Keying</i>
CSMA/CA	<i>Carrier Sense Multiple Access with Collision Avoidance</i>
DSSS	<i>Direct Sequence Spread Spectrum</i>
FHSS	<i>Frequency Hopping Spread Spectrum</i>
GPS	<i>Global Positioning System</i>
HTML	<i>Hypertext Markup Language</i>
HTTP	<i>Hypertext Transfer Protocol</i>
IDE	<i>Integrated Development Environment</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IMEI	<i>International Mobile Equipment Identity</i>
ISM	<i>Industrial, Scientific and Medical</i>
JSON	<i>JavaScript Object Notation</i>
LBS	<i>Location Based Service</i>
LDPC	<i>Low Density Parity Check</i>
LoS	<i>Line of Sight</i>
MAC	<i>Medium Access Control</i>
MIMO	<i>Multiple Input Multiple Output</i>
NAP	<i>Nearest Access Point</i>
NFER	<i>Near-field Electromagnetic Ranging</i>
OFDM	<i>Orthogonal Frequency Division Multiplexing</i>
PDA	<i>Personal Digital Assistant</i>

PHP	<i>Hypertext Preprocessor</i>
PHY	<i>Physical Layer</i>
QoS	<i>Quality of Service</i>
RAID	<i>Redundant Array of Inexpensive Disks</i>
RCPI	<i>Received Channel Power Indicator</i>
RFID	<i>Radio Frequency Identification</i>
RSSI	<i>Received Signal Strength Indication</i>
RTLS	<i>Real Time Location Systems</i>
SGI	<i>Short Guard Intervals</i>
SIM	<i>Subscriber Identity Module</i>
SQL	<i>Structured Query Language</i>
SSID	<i>Service Set Identifier</i>
SSL	<i>Secure Sockets Layer</i>
ToA	<i>Time of Arrival</i>
TDoA	<i>Time Difference of Arrival</i>
TLS	<i>Transport Layer Security</i>
ToA	<i>Time of Arrival</i>
ToF	<i>Time of Flight</i>
TWR	<i>Two Way Ranging</i>
U-NII	<i>Unlicensed National Information Structure</i>
UPS	<i>Uninterruptible Power Supply</i>
UWB	<i>Ultra-wideband</i>
WAN	<i>Wide Area Network</i>
WiFi	<i>Wireless Fidelity</i>
WPA	<i>WiFi Protected Access</i>

Capítulo 1

Introdução

Num mercado cada vez mais competitivo, tem-se tornado cada vez mais importante apostar em sistemas apoiados em tecnologias que permitam o aumento de produtividade. É com esse objectivo em mente, que a nível mundial cada vez mais organizações apostam em sistemas que possibilitam o acesso em tempo real à identificação e localização de pessoas e bens. Essa necessidade enquadra-se numa lógica de operacionalização, rapidez de resposta e fidelização de clientes, em particular na indústria, e numa lógica de controlo de pessoas e activos, ao nível de prestadores de serviços, tendo como principais consequências o aumento da produtividade e a redução de custos operacionais.

Com a contínua redução do preço, de tamanho e o aumento do poder computacional dos dispositivos de comunicações sem fios, assiste-se a uma disseminação deste tipo de sistemas e à sua introdução em novas áreas de aplicação. A utilização de dispositivos com estas características para identificação e localização (*tracking*) de objectos e pessoas é uma das áreas de aplicação que têm merecido uma atenção especial recente por parte da indústria, existindo actualmente diversas soluções no mercado para este fim.

Entre as várias áreas passíveis de aplicação de sistemas de identificação e localização citam-se a área da saúde, nomeadamente clínicas e hospitais onde é necessário controlar permanentemente a localização de determinados grupos de pacientes, a área industrial onde podem ser utilizados para controlo do inventário disponível e localização de materiais, a área empresarial para controlo de pontualidade, assiduidade e localização de trabalhadores bem como a área da segurança, onde é possível, por exemplo, recolher informação sobre a localização de crianças de forma a garantir a sua protecção e até ajudar em caso de necessidade após um eventual rapto.

As tecnologias envolvidas neste tipo de soluções adoptadas pela indústria têm sofrido uma franca evolução nos últimos anos. Um desses exemplos é a tecnologia *WiFi* (*Wireless Fidelity*) cujo último protocolo aprovado (IEEE 802.11n), permite a utilização de 2 bandas de frequência diferentes (2,4 GHz e 5 GHz) de modo a minimizar interferências e suportar um débito de dados muito superior (até 600 Mbit/s) à norma anterior IEEE 802.11g (que suportava 54 Mbit/s). Relativamente à tecnologia RFID (*Radio Frequency Identification*), uma das grandes preocupações neste momento é a questão da segurança. Para solucionar essa fragilidade, estão a ser introduzidos novos mecanismos de segurança que procuram prevenir

ou minimizar ataques de *Denial of Service*, *Eavesdropping* e *Data Modification*. A tecnologia *ZigBee*, mais recente que qualquer uma das outras referidas anteriormente, encontra-se em rápida expansão devido às suas características de baixo consumo energético, custo de aquisição reduzido, elevada segurança integrada e fácil implementação. A sua utilização num vasto conjunto de aplicações, desde a domótica onde pode ser utilizada para controlo de luzes, temperatura e consumos passando pela área da saúde onde se encontra incorporada em dispositivos de monitorização de sinais vitais de pacientes até à utilização em sistemas de localização em tempo real de pessoas ou objectos tem trazido uma crescente visibilidade a esta tecnologia.

Existem actualmente no mercado várias soluções que respondem a muitas das necessidades anteriormente referidas (e.g. “Sistema de localização de pessoal hospitalar” [1] da Kimaldi). No entanto, e dependendo da área de aplicação, a muitas (senão todas) destas soluções faltam funcionalidades como:

- Capacidade de localizar utilizadores independentemente de se encontrarem dentro ou fora das instalações da organização.
- Possibilidade de efectuar a identificação e localização sem a necessidade do utilizador passar em pontos específicos (ao contrário do verificado nas soluções RFID passivas).
- Suporte à troca de mensagens entre utilizadores do sistema bem como o tipo (e.g., notificações, pessoal, etc.) e estado (e.g., mensagens lidas/não lidas, etc.) dessas mensagens.
- Capacidade de definir e utilizar perfis (e.g., notificações e sistema de localização activos) que correspondam às necessidades actuais do utilizador.
- Divulgação do estado em que o utilizador se encontra (e.g., ocupado, de férias, etc.).

Para além das funcionalidades é também importante considerar factores como o custo de aquisição e instalação de equipamentos, a capacidade de integração do sistema nas infra-estruturas existentes, a possibilidade de suportar novas aplicações e se o sistema é ou não facilmente escalável.

1.1 - Organização do documento

Este documento está organizado em seis capítulos. No capítulo 1 é efectuada uma introdução ao problema proposto e são descritos os objectivos a atingir e o contexto em que o projecto se enquadra. No capítulo 2 é feito um levantamento e comparação das tecnologias sem fios consideradas, uma análise das soluções actualmente existentes no mercado que se assemelham à solução a implementar e uma breve discussão acerca de técnicas de localização. No capítulo 3 são definidas as funcionalidades, os requisitos e a arquitectura do sistema, e justifica-se a decisão, com base numa análise de requisitos e funcionalidades, relativa às tecnologias e técnicas de localização adoptadas. O capítulo 4 contém a descrição completa do sistema do ponto de vista do desenvolvimento. Os testes e análises de resultados são efectuados no capítulo 5 e a conclusão e trabalho futuro são apresentados no capítulo 6.

1.2 - Objectivos e contexto do problema

Nesta dissertação foi proposto desenvolver um sistema que permita identificar e localizar pessoas em espaços interiores através da utilização de dispositivos baseados em tecnologias sem fios, como por exemplo RFID, ZigBee ou WiFi. Entre os objectivos propostos para implementação deste sistema incluem-se:

- Localização e identificação de utilizadores em tempo real, quer no interior de edifícios quer no exterior.
- Suporte à interacção entre agentes\utilizadores do sistema através do envio de mensagens.
- Possibilidade de escolha de perfis e estados que se adequem a situações predefinidas.
- Consulta de registos temporais com as localizações percorridas por cada utilizador.
- Capacidade de integração do sistema na infra-estrutura existente.
- Utilização de uma base de dados dedicada com capacidade de integração na base de dados institucional.
- Possibilidade de suportar outro tipo de aplicações futuras (e.g., controlo de assiduidade).
- Garantia de escalabilidade do sistema, custo e tempo de implementação “reduzidos”.

A implementação e testes desta solução foram realizados no edifício do INESC Porto tendo como objectivo a localização de colaboradores no interior do edifício. Apesar de não ser o foco essencial do problema o sistema complementa outras áreas de aplicação tais como a localização exterior. Tornou-se assim necessário definir os requisitos funcionais e não funcionais do sistema, efectuar a análise e selecção tecnológica, definir a arquitectura do sistema, especificar os meios de comunicação, assim como o *software* a utilizar para o desenvolvimento e testes a realizar.

Entre os obstáculos à implementação de soluções deste tipo encontram-se as limitações relativas à flexibilidade e adaptabilidade a diferentes cenários, assim como ao suporte de novas funcionalidades.

Outros desafios que se prendem com o problema proposto e que foram tidos em conta são a autonomia das baterias utilizadas e as interferências provocadas por ruído advindo de ambientes externos ao sistema.

Relativamente à segurança é importante garantir a protecção das comunicações efectuadas entre etiquetas (*tags*) e leitores (*readers*)¹ assim como dos *readers* com o servidor. Por fim é necessário não descurar a questão da privacidade dos utilizadores. A

¹ Neste documento serão utilizadas as palavras *tag* e *reader* por substituição de etiqueta e leitor respectivamente.

mesma deve ser garantida através da possibilidade da *tag* utilizada ser desactivada manualmente pelo utilizador em certos períodos de tempo. Todos estes factores são dependentes e variáveis de acordo com a tecnologia escolhida como base ao desenvolvimento do sistema.

Capítulo 2

Estado da arte

Este capítulo apresenta o estado da arte actual relativo a sistemas de identificação e localização baseados em dispositivos de comunicações sem fios. É efectuada uma análise às soluções semelhantes à que se pretende implementar e que se encontram actualmente disponíveis no mercado, assim como das tecnologias que as suportam e as técnicas de localização mais utilizadas. Com isto pretende-se chegar a conclusões sobre que tecnologias, funcionalidades e técnicas de localização deverão ser implementadas na solução que se pretende apresentar.

2.1 - Levantamento de tecnologias

A evolução e ampla divulgação e disseminação das tecnologias de comunicação sem fios, assim como dos dispositivos de computação móveis e da Internet, têm permitido desenvolver um novo conjunto de serviços e aplicações baseados em localização e identificação de pessoas e objectos. Por norma estes sistemas podem ser divididos em duas categorias distintas no que se refere à localização e identificação através de meios sem fios: i) sistemas RTLS (*Real Time Location System*) capazes de efectuar localização interior e exterior e ii) sistemas LBS (*Location Based Service*) que efectuem apenas localização exterior. Ao nível dos sistemas RTLS existem várias alternativas baseadas em tecnologias distintas como é o caso do RFID, *WiFi*, *Bluetooth*, *ZigBee*, UWB, infravermelhos etc.; já no caso dos sistemas LBS a tecnologia utilizada por excelência é o GPS (*Global Positioning System*) sendo também utilizada com alguma frequência a localização por triangulação de antenas através da rede móvel. A tabela 3.1 [2] faz uma breve caracterização dos casos anteriormente referidos.

Tabela 2.1 – Serviços/Soluções de localização.

	Sistemas RTLS	Satélite	Rede móvel
Tipo de localização	Tridimensional com comunicação local sem fios.	Tridimensional com mais de 24 satélites.	Bidimensional com estação base móvel.
Cobertura	Rede local (edifício, armazém, etc.)	Global	WAN
Precisão	< 10m	< 10 m	100 m - 1 km
Características	Várias aplicações. Bidireccional.	Aplicações limitadas. Unidireccional.	Aplicações limitadas. Bidireccional.
Tecnologia	RFID, <i>ZigBee</i> , <i>WiFi</i> , <i>Bluetooth</i> , <i>UWB</i> , etc.	GPS, Galileo, GLONASS, etc.	GSM, CDMA, DMB, <i>WiBro</i> / <i>WiMax</i> , etc.
Observações	Elevada precisão de localização a nível interior e exterior.	Localização exterior apenas.	Baixa precisão baseada em células móveis. Subscrição necessária.

Como o objectivo principal definido para o projecto se trata da implementação de um sistema que permita efectuar localização interior, a solução terá que passar obrigatoriamente pela utilização de um sistema RTLS. Por esse motivo torna-se relevante a análise que se segue, feita a tecnologias sem fios que podem ser utilizadas, assim como uma comparação das respectivas vantagens e desvantagens ao nível da utilização de RTLS para localização interior.

2.1.1 - RFID - Radio Frequency Identification

A tecnologia RFID baseia-se na comunicação através de sinais rádio para efectuar troca de informação entre um *reader* e uma *tag*. A *tag* pode ser acoplada a um objecto ou pessoa para fins de identificação e localização suportadas pelo *reader*. O funcionamento desta tecnologia não requer qualquer tipo de contacto, sendo um método conveniente para a captura de dados de forma simples. Considerada como uma das tecnologias *wireless* mais promissoras no futuro ao nível das aplicações de baixo consumo energético, é no entanto muito diferente de outros tipos de tecnologias *wireless* como as existentes nas comunicações móveis ou nas redes *wireless* de computadores. Ao contrário das tecnologias *wireless* utilizadas em comunicações móveis e redes de computadores, onde as comunicações são deliberadamente iniciadas e terminadas pelos utilizadores, nos sistemas RFID as comunicações são automaticamente iniciadas pelos *readers* ou pelas *tags* (no caso de *tags* activas), desde que

estejam ao alcance das ondas rádio emitidas pelos mesmos. Esta última característica levanta algumas questões ao nível da privacidade.

O princípio de funcionamento da tecnologia RFID pode ser descrito da seguinte forma: um *reader* RFID emite um sinal de radiofrequência com um determinado comprimento de onda e potência; caso o alcance do sinal seja suficiente para atingir uma *tag*, a mesma faz uso da energia fornecida pelo *reader* através do sinal (caso das *tags* passivas) para responder ao *reader*; o *reader* por sua vez capta o sinal de resposta, analisando-o e executando as acções predefinidas de acordo com a mensagem recebida e com o estabelecido pela aplicação que controla o sistema.

Um sistema RFID é composto essencialmente por três elementos principais: uma *tag* que geralmente contém um número de identificação e está acoplada aos objectos ou pessoas que pretende identificar, um *reader* que detecta as *tags* realizando determinadas operações sobre as mesmas e um sistema informático responsável pelo armazenamento e visualização de informação [3]. Tipicamente uma *tag* RFID pode ser dividida em três grupos distintos: *tags* RFID passivas, semi-passivas e activas [4].

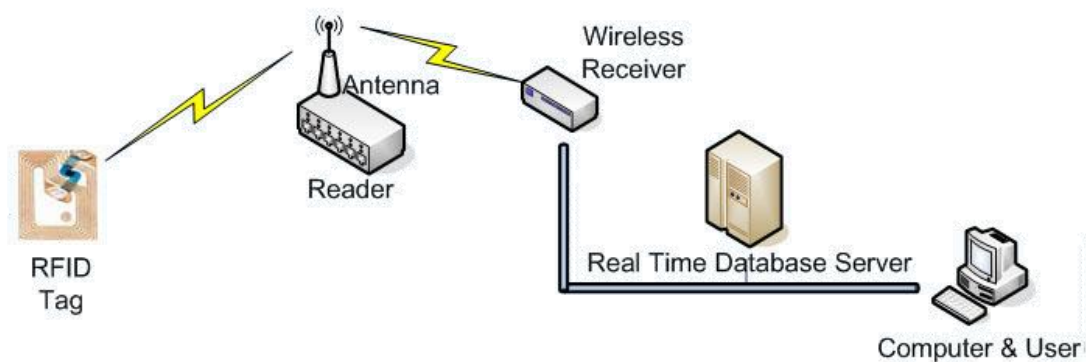


Figura 2.1 - Exemplo de arquitectura da tecnologia RFID.

As *tags* RFID passivas caracterizam-se por não possuírem fonte de energia própria. Alimentam-se através do sinal rádio emitido pelo *reader*, sendo que parte dessa energia é transformada em corrente eléctrica dentro da *tag*, que por sua vez gerará um sinal de resposta. Esta forma de funcionamento torna a *tag* menos complexa logo mais fácil e mais barata de produzir. Como inconveniente obriga a que o *reader* tenha maior potência de saída, pois apenas uma fracção da energia radiada é efectivamente utilizada na resposta da *tag* RFID. As *tags* RFID semi-passivas possuem uma bateria que apenas é utilizada quando recebe um sinal do *reader*. A bateria é normalmente utilizada somente para alimentar o *chip* que as *tags* possuem, enquanto a energia recebida do *reader* é utilizada para comunicação. As *tags* RFID activas possuem uma bateria utilizada para alimentar o *chip* interno e para fornecer energia para o sinal de comunicação. Este tipo de *tag* RFID consegue emitir continuamente o seu sinal, independentemente de ter recebido ou não um sinal de um *reader*. Possuem uma complexidade e custo mais elevado; no entanto, conseguem ser identificadas a distâncias maiores.

De notar que o *reader* é constituído por dois elementos, um leitor e uma antena. O leitor RFID realiza a codificação e decodificação dos sinais emitidos/recebidos, enquanto a antena RFID tem como função propagar o sinal de radiofrequência no meio.

Os sistemas RFID podem ser classificados de acordo com a gama de frequências que ocupam:

- *Low Frequency* (operação entre 100 e 150 kHz)
- *High Frequency* (operação por volta de 13,56 MHz)
- *Ultra High Frequency* (operação entre 900 MHz e 2,4 GHz)

Em relação aos três grupos referidos [3] [5] pode-se afirmar que os sistemas *Low Frequency* têm um alcance de operação curto que varia entre 2 e 15 cm e são normalmente utilizados para controlo de acessos, logística, identificação de produtos e animais. Já os sistemas *High Frequency* são caracterizados pela alta velocidade de transmissão de dados, têm um alcance de operação que varia entre 10 cm e 1,5 m e são utilizados para controlo de acesso a passaportes electrónicos, identificação de produtos, cartões bancários, classificação de sistemas e controlo tecnológico de processos. Os sistemas *Ultra High Frequency*, permitem uma maior distância de operação, até 7 m, sendo normalmente utilizados em logística, controlo de *stock* de armazéns e controlo de sistemas de estacionamento. De acordo com a finalidade pretendida (tipo de aplicação, velocidade de transmissão de dados necessária, etc.), deve-se escolher o grupo de frequências mais adequado.

O uso tão disseminado da tecnologia RFID nas mais variadas aplicações justifica-se pelas suas vantagens tais como: o funcionamento do sistema não requerer qualquer tipo de contacto nem campo de visão entre a *tag* e o *reader*; as *tags* poderem ser lidas de forma rápida e fiável; existir a possibilidade de actualização da informação presente em *tags* activas; a instalação das *tags* poder ficar escondida (mais no caso das *tags* activas); ser possível a transmissão de dados com velocidades até 650 kbit/s e a capacidade de cifrar os dados presentes nas *tags*. Existem no entanto algumas desvantagens tais como: o custo relativamente elevado por *tag* (0.07 a 3.67 €); incapacidade de operação em superfícies metálicas ou electro-condutivas; susceptibilidade a interferências de campos electromagnéticos vizinhos; colisões mútuas; possibilidade dos sistemas serem penetrados indevidamente através do uso de antenas (*grabbers*) que captem as ondas rádio.

2.1.2 - ZigBee

O *ZigBee* é uma norma sem fios proposta e mantida pela *Zigbee Alliance* [6] [7] com vista a satisfazer a necessidade de criação de redes de baixo custo e baixo consumo. Os sistemas *ZigBee* estão definidos segundo a norma IEEE 802.15.4 e operam em três bandas de frequência distintas de acordo com a localização geográfica:

- Banda dos 868 MHz (Europa)
- Banda dos 915 MHz (América do Norte\Sul e Austrália)
- Banda dos 2,4 GHz (reservada para uso a nível global)

O débito binário desta tecnologia encontra-se dependente da frequência e do número de canais utilizados. Na banda dos 2,4 GHz é possível obter um débito máximo de 250 kbit/s utilizando 16 canais, nos 915 MHz é possível obter 50 kbit/s fazendo uso de 10 canais e por

fim nos 868 MHz o débito é de 20 kbit/s para apenas 1 canal. As distâncias de transmissão de um sistema típico variam entre 10 e 100 metros, dependendo da potência e das condições do meio, sendo que o acesso ao canal é feito através de um protocolo CSMA/CA.

A norma IEEE 802.15.4 prima por adoptar uma tecnologia utilizada para transmissões sem fios de curtas distâncias, devido ao seu baixo consumo energético, o que permite a integração em pequenos dispositivos. Adicionalmente, como permite comunicação bidireccional, é indicada para utilização em sistemas de localização interior, como pretendido neste trabalho. A tecnologia *ZigBee* pode ser utilizada nas mais variadas áreas de aplicação que podem ser englobadas nos seguintes perfis [8] definidos:

- *Building Automation* (Espaços comerciais mais eficientes)
- *Remote Control* (Controlos remotos avançados)
- *Smart Energy* (Poupança energética)
- *Health Care* (Monitorização de sinais vitais)
- *Home Automation* (Casas inteligentes)
- *Input Device* (Dispositivos que proporcionam interactividade)
- *Retail Services* (Compras inteligentes)
- *Telecom Services* (Serviços de valor acrescentado)
- *3D Sync* (Experiência de visionamento 3D)

Como exemplos de aplicações práticas da tecnologia em alguns dos perfis referidos tem-se o uso de sensores para medição remota de sinais vitais de pacientes no perfil *Health Care*, o controlo remoto de dispositivos eléctricos presentes numa casa no perfil *Home Automation*, a utilização de cartões SIM *ZigBee* para efectuar o pagamento de serviços ou produtos no perfil *Telecom Services* e a localização em tempo real de pessoas e objectos no perfil *Retail Services*.

Um sistema *ZigBee* pode ser constituído por três tipos diferentes de dispositivos: coordenador *ZigBee*, *router ZigBee* e *ZigBee end device* [9]. O coordenador *ZigBee* é o dispositivo mais capacitado do ponto de vista energético (e eventualmente de processamento e memória), sendo a raiz da rede; através dele é possível fazer *bridging* para outras redes. Apenas pode existir um coordenador *ZigBee* em cada rede visto que também é o responsável pela criação da rede. Entre outras funcionalidades, o coordenador tem a capacidade de guardar informação sobre a rede, actuar como *trust center* e repositório de chaves de segurança, sendo apenas necessário um por cada rede. O *router ZigBee* actua como encaminhador intermediário, redireccionando o fluxo de dados para outros dispositivos e efectua a atribuição de endereços locais. O *ZigBee end device* pode conter sensores de luminosidade, temperatura, movimento, ou outros, sendo apenas capaz de comunicar com o nó pai (coordenador ou *router*), não conseguindo fazer o *relay* de dados de outros dispositivos da rede. Esta relação permite que o nó esteja em modo *sleep* na maior parte do tempo, o que garante um tempo de vida da bateria superior. Dos três dispositivos referidos, o *ZigBee end device* é o que requer menos memória, sendo portanto o mais barato de produzir. As características *ZigBee* permitem uma excelente comunicação *peer-to-peer*. A camada superior da rede, definida pela especificação *ZigBee*, assegura a capacidade de extensão da rede sendo suportados três tipos de topologias: estrela, árvore e malha. Cada rede pode suportar até 65535 nós, com uma estrutura auto-organizável e auto-reparável, que permite o *relay* de dados através de *multi-hop* entre quaisquer dois nós [6] [10].

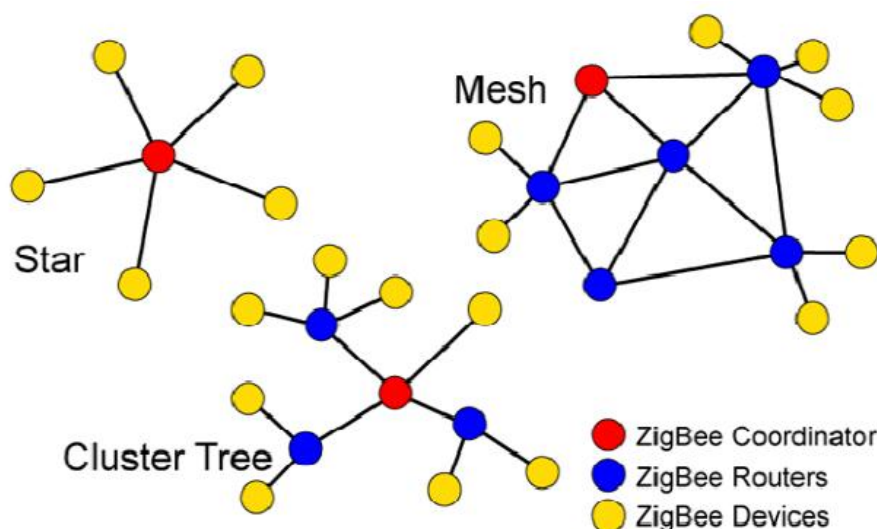


Figura 2.2 - Diferentes topologias de uma rede ZigBee.

Um dos pontos fortes da tecnologia *ZigBee* é a possibilidade de serem utilizadas múltiplas topologias de rede como, por exemplo, ponto-a-ponto, ponto-a-multiponto e malha. O baixo *duty cycle* que permite um tempo de vida de bateria superior, a baixa latência e a utilização de *Direct Sequence Spread Spectrum* (DSSS) são outros dos pontos fortes a favor desta tecnologia. Como métodos de tratamento de erros o *ZigBee* implementa *collision avoidance* e mensagens de controlo com *retries* e *acknowledgements*, sendo que ao nível da segurança existe a possibilidade de cifragem com algoritmo de chave simétrica *Advanced Encryption Standard* de 128 bits (AES-128) para conexões de dados seguras. Por fim é também importante salientar a auto-configuração da rede emalhada (que permite reduzir custos de manutenção) e a interoperabilidade de produtos *ZigBee* independentemente do fabricante. Existem no entanto algumas desvantagens, como um alcance algo limitado (20 a 30 m) e um baixo débito binário (250 kbit/s) quando comparado com outras tecnologias *wireless*.

2.1.3 - WiFi

O *WiFi* é uma tecnologia sem fios que permite a criação de uma rede baseada na norma IEEE 802.11 (e suas variantes). O seu princípio de funcionamento tem por base a existência de pelo menos duas estações equipadas com uma placa *wireless* capaz de comunicar através de um dos protocolos IEEE 802.11 normalizados [11].

A comunicação entre estações de uma rede *WiFi* é estabelecida através de um dos dois modos de configuração básicos existentes: i) *infrastructure* onde as estações comunicam através dum ponto de acesso central (AP - *Access Point*), tipicamente ligado a uma rede cablada ou ii) *ad-hoc* onde as estações comunicam directamente entre si, sem a necessidade de um *Access Point* operar como intermediário [12]. A figura 3.3 exemplifica estes dois modos.

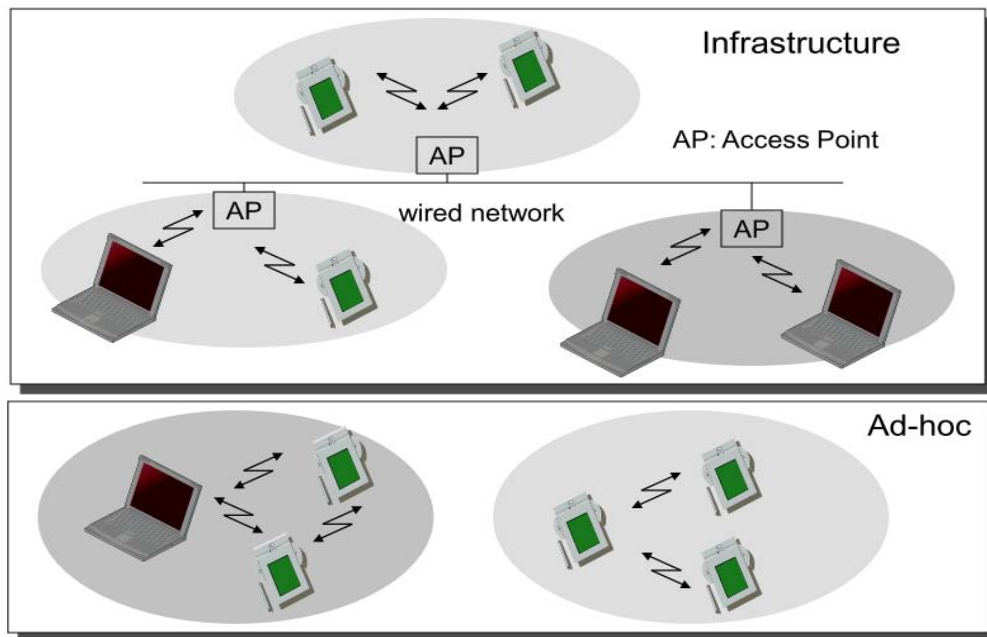


Figura 2.3 - Modos de configuração básicos na tecnologia WiFi.

Ao longo dos anos, a norma IEEE 802.11 tem incorporado diversas variantes que se distinguem em parâmetros como a frequência de operação, a modulação, o número de canais utilizados e o débito binário. O protocolo inicial 802.11 especifica débitos binários de 1 e 2 Mbit/s para três camadas físicas (PHY) diferentes, baseadas em *Direct Sequence Spread Spectrum* (DSSS), *Frequency Hopping Spread Spectrum* (FHSS) e *Infrared Techniques* (IR). Mais tarde foram adicionadas ao protocolo novas especificações da camada PHY o que permitiu o aparecimento de dois novos protocolos: o IEEE 802.11b e o IEEE 802.11a.

Tabela 2.2 – Tabela comparativa das variantes da norma 802.11.

Protocolo WiFi	Frequência de operação	Débito binário máximo
802.11a	5 GHz	54 Mbit/s
802.11b	2,4 GHz	11 Mbit/s
802.11g	2,4 GHz	54 Mbit/s
802.11n	2,4 GHz 2,4 ou 5 GHz (seleccionáveis) 2,4 e 5 GHz (em simultâneo)	600 Mbit/s

O protocolo IEEE 802.11b define uma operação na frequência ISM (*Industrial Scientific and Medical*) dos 2,4 GHz, permite um débito binário até 11 Mbit/s e utiliza DSSS com modulação *Complementary Code Keying* (CCK). O protocolo IEEE 802.11a especifica uma modulação *Orthogonal Frequency Division Multiplex* (OFDM) permitindo um débito binário até 54 Mbit/s e opera na banda *Unlicensed National Information Infrastructure* (U-NII) dos 5 GHz. Em DSSS a sequência de bits modula uma portadora, enquanto que na modulação OFDM

o *stream* de bits original é dividido em 52 sequências individuais, sendo cada uma delas transportada numa sub-portadora.

O protocolo que se seguiu foi o IEEE 802.11g. Este protocolo usa a mesma técnica de OFDM adoptada no 802.11a e garante ainda a retro compatibilidade com dispositivos 802.11b. Em teoria, tanto o 802.11g como o 802.11a deveriam ter o mesmo desempenho ao nível do débito binário, até 54 Mbit/s, pois utilizam as mesmas especificações da camada PHY e têm um *Bit Error Ratio* (BER) semelhante. Na prática o débito binário do 802.11g é, em condições normais, ligeiramente inferior ao do 802.11a. Tal deve-se ao facto do protocolo 802.11g operar na frequência de 2,4 GHz, que é ocupada por muitos outros dispositivos que operam na mesma frequência, tais como aparelhos de microondas, dispositivos *Bluetooth* e telefones sem fios, provocando interferências significativas e a degradação de desempenho.

Outro factor que penaliza o protocolo 802.11g relativamente ao 802.11a, é o facto de existirem menos canais disponíveis na banda dos 2,4 GHz comparativamente com a banda dos 5 GHz. Existem 13 canais que não se sobrepõem na banda dos 5 GHz, enquanto na banda dos 2,4 GHz apenas existem 3 canais não sobrepostos. A utilização de canais que se sobrepõem aumenta a interferência provocada na rede leva a uma degradação do desempenho [13] [14].

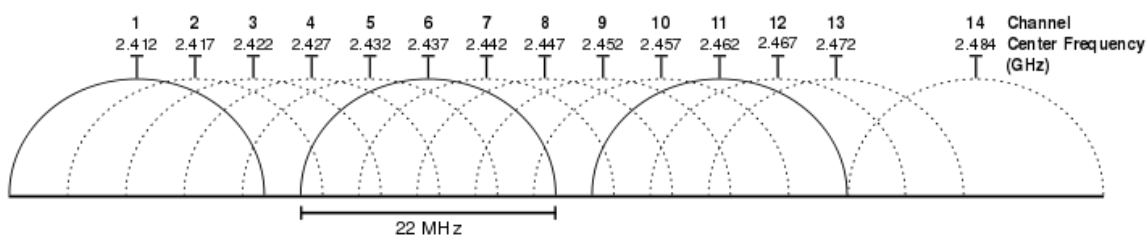


Figura 2.4 - Canais *WiFi* disponíveis na frequência 2.4 GHz.

O mais recente protocolo a ser aprovado foi o IEEE 802.11n que permite a operação nas frequências dos 2,4 e 5 GHz. Para além disso incorporou melhoramentos nas camadas MAC e PHY, o que possibilitou o aumento do débito binário, melhor *Quality of Service* (QoS) e retro compatibilidade com todos os dispositivos que utilizem protocolos anteriores (IEEE 802.11a/b/g). Na camada PHY a utilização da técnica *Multiple Input Multiple Output* (MIMO) juntamente com OFDM (MIMO-OFDM) e a duplicação da largura de banda do canal de 20 para 40 MHz, tornou possível aumentar o débito binário da camada até aos 600 Mbit/s. Outras características introduzidas foram a multiplexagem espacial, com obrigatoriedade de utilização de 1 ou 2 fluxos espaciais e 3 ou 4 fluxos espaciais de forma opcional, correcção de erros obrigatória com código de convolucional e *Low Density Parity Check* (LDPC) como opcional e a utilização de *Short Guard Intervals* (SGI) de 400ns de forma a reduzir a interferência existente. A utilização de SGIs de 400 ns (metade do valor utilizado nos protocolos anteriores), permite o aumento de débito binário, tendo como contrapartida o ligeiro aumento da interferência intersimbólica. Caso se reduza demasiado o valor de SGI, a interferência aumentará de tal forma, que o próprio débito binário será inferior ao verificado com SGIs maiores [15] [16] [17].

2.1.4 - Comparação de tecnologias

Nesta secção comparam-se as tecnologias de comunicação sem fios referidas ao longo deste capítulo. A comparação dos vários parâmetros está sintetizada na tabela 3.3, sendo de seguida discutidas as vantagens e desvantagens de cada uma das tecnologias.

Tabela 2.3 – Tabela comparativa de tecnologias de comunicação sem fios.

	RFID ²	ZigBee	WiFi
Frequência de operação	100-150 kHz 13.56 MHz 900 MHz-2.4 GHz	2,4 GHz	2,4 GHz (802.11b/g) 5 GHz (802.11a) 2,4 GHz e/ou 5 GHz (802.11n)
Débito binário	40-650 kbit/s	250 kbit/s	11 Mbit/s (802.11b) 54 Mbit/s (802.11a/g) 600 Mbit/s (802.11n)
Alcance (interior)	2-15 cm (passiva) 10-30 m (activa)	20-30 m	10 - 60 m
Precisão média	1.3 m	1.5 m	3 m
Autonomia média (tag)	Ilimitada (passiva) 365 dias (activa)	1000 dias	5 dias
Custo médio relativo do hardware	Médio	Baixo	Elevado
Segurança	AES-128	AES-128	WPAv2
Tecnologia proprietária	Não	Não	Não

Na tabela 2.3 encontram-se resumidas as características mais importantes de cada uma das tecnologias cuja síntese é baseada nas referências [18] [19] [20] [21] [22] [23]. De notar que não foi possível encontrar valores específicos para o custo do *hardware*, ficando apenas uma comparação relativa e não quantitativa entre as várias tecnologias.

Como referido anteriormente, a tecnologia RFID pode ser dividida em dois grandes tipos: RFID passiva e RFID activa. No caso do tipo passivo as *tags* são fabricadas com um baixo custo e têm uma autonomia ilimitada. No entanto, ao nível do alcance, da capacidade de troca de informação e da segurança esta solução revela-se inferior em comparação com as outras estudadas. Estas *tags* são normalmente muito básicas suportando apenas a função de leitura, o que limita e muito as funcionalidades possíveis de implementar num sistema deste tipo. No caso da tecnologia RFID activa, as *tags* utilizam alimentação própria para transmitir o sinal, o que permite um conjunto maior de funcionalidades, um alcance superior, bem como a

² Contempla características do RFID passivo e activo.

implementação de alguns algoritmos de segurança eficazes na protecção contra *eavesdropping*. Como desvantagens encontra-se o facto de serem mais complexas de fabricar e como tal mais onerosas. Em comparação com as *tags* passivas, a autonomia passa de teoricamente ilimitada para cerca de 365 dias. Na conjuntura dos dois tipos (activa e passiva) existem também outras vantagens, como o funcionamento sem estar em linha de vista e a capacidade de leitura das *tags* ser praticamente independente da orientação do portador da *tag*. A leitura simultânea de várias *tags* é outra das vantagens desta tecnologia, no entanto, tem o contra de provocar o chamado *reader collision problem* que ocorre quando existe a necessidade de utilizar mais que um *reader* em simultâneo e que por vezes obriga à utilização de mecanismos para minimizar a ocorrência do mesmo. Outra desvantagem é a aplicação de mecanismos de acesso múltiplo, baseados em tempo, frequência, *code division* ou *carrier sensing* directamente no RFID ser de difícil implementação. Por fim a susceptibilidade a interferências originadas por outros materiais é outra das desvantagens [24].

A tecnologia *ZigBee* está por norma associada a redes emalhadas de sensores e monitorização. Os dispositivos *ZigBee* possuem um baixo custo de produção, tamanho reduzido e dispõem da autonomia mais elevada devido ao baixo consumo provocado pela utilização de ciclos *sleep* que permitem poupar energia quando não existe a necessidade de transmissão de informação. No que se refere a características mensuráveis, o alcance que é possível atingir (20 a 30 m) é idêntico ao do RFID passivo (10 a 30 m) mas inferior ao do *WiFi* (10 a 60 m). Também o débito binário (250 kbit/s) é muito inferior ao atingido pela norma 802.11n (600 Mbit/s). No entanto, no que se refere à precisão em sistemas de localização o *ZigBee* distingue-se claramente do *WiFi* pelo facto de ter uma precisão duas vezes superior (1,5 m vs 3 m). O fácil acréscimo e configuração dos nós da rede, a capacidade de comunicação bidireccional (ao contrário da tecnologia RFID em que a comunicação é apenas unidireccional), a possibilidade de auto-configuração da rede emalhada (que permite a diminuição de intervenções de manutenção), a baixa latência, bem como a utilização para efeitos de segurança do algoritmo de chave simétrica AES-128 são outras das vantagens. Ao nível das desvantagens tem-se a interferência provocada por operar na banda de frequências mais utilizada (2,4 GHz), a elevada sobrecarga na rede devido à descoberta de rotas, a necessidade de espaço para guardar as tabelas de encaminhamento, alguma dificuldade em manter a potência do sinal constante, e susceptibilidade a interferências providas do ambiente adjacente [10] [25] [26].

A tecnologia *WiFi* é a mais divulgada e aquela cujos equipamentos compatíveis são mais fáceis de encontrar no mercado. De todas as tecnologias estudadas é aquela com maior débito binário (até 600 Mbit/s) o que pode ser essencial para a introdução de funcionalidades mais avançadas, sendo também aquela cuja segurança é a mais elevada o que a torna mais indicada para certas aplicações, como é o caso de um sistema de localização onde a segurança relativamente à privacidade dos utilizadores é muito importante. Esta tecnologia é frequentemente utilizada em sistemas de localização em parte devido ao facto de ser escalável e de fácil configuração e não tanto pela sua precisão. Os sistemas que utilizam esta tecnologia como forma de efectuar a localização, fazem uso de dados de diferentes pontos de acesso bem como de parâmetros gerais como RSSI (*Received Signal Strength Indication*) ou TDOA (*Time Difference of Arrival*). Os sistemas *WiFi* são essencialmente atractivos pela facilidade e baixo custo de implementação recorrendo-se frequentemente à infra-estrutura

existente (a probabilidade de existir uma rede *WiFi* instalada é elevada, visto ser uma tecnologia *mainstream*). No entanto a precisão de localização deste tipo de sistemas está longe de ser a ideal (3 m) muito por culpa de perdas por propagação, topologias de edifícios não orientadas à transmissão de sinal e mudanças incontrolláveis no ambiente adjacente ao sistema (pessoas, dispositivos móveis que utilizam a mesma banda de frequências, etc.) que provocam variações indesejadas no sinal *WiFi*. O excessivo consumo energético que faz com que os dispositivos móveis *WiFi* utilizados para localização tenham uma baixa autonomia e o elevado preço dos dispositivos *WiFi* quando comparado com as tecnologias *RFID* e *ZigBee* são outras das desvantagens desta tecnologia [24] [27] [28]. No entanto, hoje em dia é cada vez mais raro encontrar um local no qual um sistema *WiFi* não esteja instalado e, caso seja possível utilizar o sistema existente, é possível poupar nos custos tornando assim esta opção mais barata que as outras, apesar do preço dos equipamentos ser mais elevado. Para além disso, hoje em dia proliferam dispositivos móveis que cumprem a norma IEEE 802.11 (computadores portáteis, *smartphones*, etc.) que têm o potencial de ser utilizados como *tags*, promovendo assim ainda mais a redução do custo de implementação deste sistema.

Apesar de não referenciada anteriormente, foi também considerada a tecnologia proprietária Crossbow MICA2, pois já existia no INESC Porto um *kit* completo que poderia ser utilizado para implementação do sistema. Nesta tecnologia, tem-se como grandes vantagens a precisão de 1 m (que é a melhor de todos os sistemas consideradas), a segurança (permite a implementação de AES-64 bits) e o alcance (3 a 61m). A operação em frequências alternativas à frequência 2,4 GHz, 315 MHz, 433 MHz, 868-916 MHz, permite reduzir a interferência provocada pelo ambiente circundante; o facto das *tags* conterem sensores de luminosidade, temperatura e som, permite acrescentar ao sistema um conjunto de funcionalidades interessantes. É no entanto uma tecnologia bastante dispendiosa; para além disso, os componentes são muito específicos e difíceis de encontrar, o que dificulta a interoperabilidade. Outras desvantagens são o baixo débito binário (40 kbit/s) e de os sensores móveis de localização serem bastante volumosos, o que se torna pouco prático para o efeito que se pretende (o utilizador andar sempre com a *tag*).

2.2 - Técnicas de localização utilizadas em RTLS

Após abordagem às tecnologias sem fios consideradas mais indicadas para o desenvolvimento do sistema, será agora realizada a discussão acerca das técnicas de localização existentes. Ao fazer esta análise convém ter em mente o grau de precisão de localização que este projecto requer. Na verdade, para a precisão exigida no projecto não existe interesse em saber se o utilizador se encontra “encostado à parede de uma sala, ou a 1m da mesma”. O objectivo é o sistema ser capaz de detectar se o utilizador se encontra em primeiro lugar dentro do edifício, em que piso está e por fim a sala em que se encontra. Pode-se neste caso falar de uma precisão ao nível do piso/sala. Entre as várias técnicas de localização existentes citam-se as seguintes:

- *Angle of Arrival (AoA)*
- *Line of Sight (LoS)*
- *Time of Arrival (ToA)*
- *Time Difference of Arrival (TDoA)*
- *Nearest Access Point (NAP)*
- *Received Channel Power Indicator (RCPI)*
- *Received Signal Strength Indication (RSSI)*
- *Time of Flight (ToF)*
- *Two Way Ranging (TWR)*
- *Near-field Electromagnetic Ranging (NFER)*

Das técnicas referidas [29], serão analisadas as seguintes: *Nearest Access Point*, *Time Difference of Arrival* e *Received Signal Strength Indication*. A análise da técnica NAP prende-se com o facto de ser mais adequada para a implementação em causa, enquanto que TDoA e RSSI são segundo a literatura as que apresentam maior potencial.

2.2.1 - *Nearest Access Point*

Esta técnica é essencialmente um indicador booleano que confirma se o terminal se encontra ou não ao alcance de um determinado ponto de acesso. Apesar de tal situação poder ser suficiente para determinar a localização aproximada de um dispositivo sem fios, não fornece a precisão suficiente requerida para determinar a localização exacta ou mesmo a sala em que o utilizador se possa encontrar [29].

Esta solução oferece uma fraca precisão sendo no entanto a mais fácil de implementar, não requerendo qualquer tipo de *hardware* ou *software* adicional.

2.2.2 - *Time Difference of Arrival (TDoA)*

A técnica TDoA caracteriza-se por calcular o tempo que um pacote demora desde que é enviado por um dispositivo sem fios, até ser recebido por um ponto de acesso. Através deste tempo é possível calcular a distância entre os dois dispositivos. Para esta técnica ser o mais eficaz e preciso possível, é aconselhável a utilização de três ou mais pontos de acesso, calculando-se a diferença de tempo de chegada aos diferentes receptores (figura 3.5). É ainda necessária a sincronização temporal entre os vários pontos de acesso, o que torna este método dependente de *hardware* e como tal uma solução mais dispendiosa.

As desvantagens desta técnica encontram-se na sua aplicação em termos de localização interior, onde, devido aos numerosos pontos de acesso e dispositivos sem fios existentes, os sinais são reflectidos nos obstáculos existentes como paredes, mobílias e até mesmo pessoas. Estas reflexões provocam o aparecimento de “fantasmas” que introduzem erros nos cálculos efectuados, retornando assim posições imprecisas. Por este motivo, este método é sobretudo utilizado em localização exterior [29] [30].

2.2.3 - *Received Signal Strength Indicator (RSSI)*

A técnica RSSI utiliza sinais indicadores da potência do sinal para determinar e actualizar a localização de um dispositivo sem fios. Esta técnica torna-se mais simples de implementar comparativamente ao TDoA, pois é possível obter facilmente a informação da potência do sinal a partir de qualquer ponto de acesso. Quão mais longe o receptor se encontra do emissor, mais fraca é a potência do sinal recebido e maior é a distância a que se encontra o utilizador do dispositivo móvel. Sabendo o valor de RSSI do dispositivo móvel, é possível determinar a distância entre o mesmo e o ponto de acesso, pois as coordenadas radiais são conhecidas. No entanto, como o ângulo do sinal não é conhecido, para determinar a posição actual e absoluta do utilizador é necessário que o dispositivo móvel se encontre ao alcance de pelo menos três (idealmente mais) pontos de acesso, sendo o resultado obtido através de um algoritmo de triangulação como se pode observar na figura 2.5.

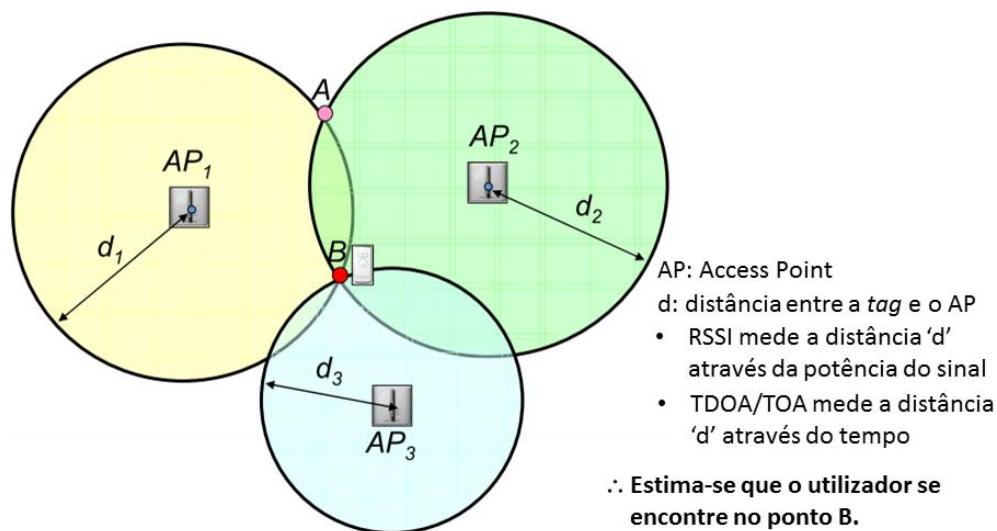


Figura 2.5 - Exemplificação do modo de funcionamento das técnicas RSSI e TDoA.

Este método é mais robusto que o TDoA para utilizações interiores e quando combinado com *fingerprinting* (divisão de um espaço em vários subespaços com mapeamento de potências) é possível refinar ainda mais a precisão do sistema.

Como desvantagem encontram-se as reflexões de sinal que por norma ocorrem, o que poderá levar à necessidade de adaptação da relação entre a atenuação do sinal, a distância entre o ponto de acesso e o dispositivo móvel de acordo com o local onde será aplicado o método [29] [30].

2.3 - Levantamento de soluções

Nesta secção será efectuada uma breve descrição das soluções existentes no mercado que tenham uma finalidade próxima da pretendida no âmbito da dissertação, ordenada pelas tecnologias que lhes servem de base. No final é apresentada uma tabela resumo com as várias soluções analisadas.

2.3.1 - RFID - Radio Frequency Identification

2.3.1.1 - BlueTag - Patient and Safety Security

Trata-se de uma solução oferecida pela empresa LogicPulse [31], desenvolvida para ambientes clínicos e que consiste em proteger as unidades de saúde de riscos de fuga, rapto e troca de recém-nascidos ou pessoas vulneráveis. Essa protecção é garantida através da colocação no pulso ou tornozelo de uma pulseira hipoalergénica, que possui um circuito electrónico codificado (RFID - *Radio Frequency Identification*) que permite a localização da mesma. A solução BlueTag é essencialmente constituída pelos seguintes módulos: Pulseira BlueTag, Posto de controlo, Receptores e Alarme.



Figura 2.6 - Pulseira BlueTag.

A pulseira Bluetag é um identificador constituído por uma caixa que contém tecnologia RFID activa, alimentada por uma bateria (com duração estimada de 18 meses), que envia um sinal único a cada segundo. A pulseira é fabricada de modo a ser leve, hipoalergénica, confortável e reutilizável, sendo possível a colocação no pulso ou no tornozelo do paciente.

O posto de controlo contém *software* que permite gerir as associações entre a *tag* e o paciente e as saídas provisórias ou definitivas. O posto de controlo pode utilizar um ecrã táctil com discos redundantes (RAID) e alimentação de emergência (UPS).

Os receptores responsáveis por cobrir a zona a proteger e receber o sinal das *tags*, estão todo interligados através da rede e estão associados a um alarme autónomo do posto de controlo para aumentar a fiabilidade do sistema de segurança. Os receptores de longa distância (círculos azuis na figura 2.7) são destinados a cobrir toda a zona a proteger. Cada receptor abrange em média um círculo com 30m de diâmetro. Tem um funcionamento

temporizado para evitar o envio de alarmes intempestivos (30 segundos parametrizáveis). Os receptores de curto alcance (círculos vermelhos na figura 2.7) protegem as saídas, sendo o seu alcance ajustável de 3 a 15 m. O envio do alarme é instantâneo.

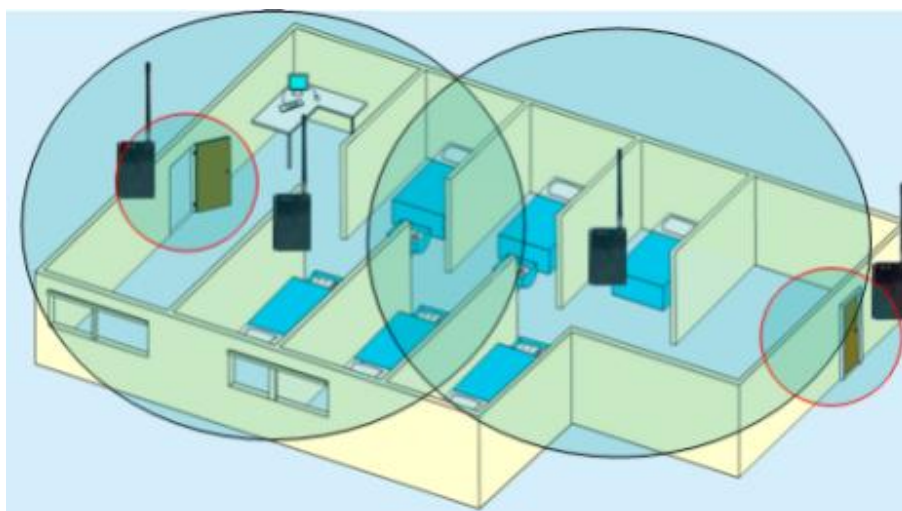


Figura 2.7 - Aspecto geral da solução BlueTag.

É possível configurar o sistema com vários tipos de alarmes sonoros e visuais. O alerta é desencadeado quando uma pulseira passa uma saída protegida ou é cortada/aberta.

2.3.1.2 - Kimaldi - “Controlo de vageantes”

A aplicação “Controlo de vageantes baseado na tecnologia RFID activa” [32] é uma aplicação desenvolvida pela empresa Kimaldi que utiliza tecnologia RFID activa para controlar a posição de alguns pacientes concretos. Estes pacientes são pessoas com problemas de orientação ou com doenças de memória, como Alzheimer. Controlando estas zonas críticas evita-se que essas pessoas se possam perder. Tal controlo realiza-se de forma imperceptível para o paciente, com elevada segurança e conservando um ambiente aberto e descontraído.



Figura 2.8 - Reader RFID SYRD245-1N e tag RFID activa SYTAG245245_TM.

Este sistema de controlo foi desenvolvido com os *readers* RFID activos SYRD245-1N, que estão ligados à rede *Ethernet* do local e enviam resultados das leituras realizadas nas zonas controladas em tempo real. Os pacientes, e também o pessoal do centro, são portadores de uma *tag* activa que periodicamente envia um sinal ao *reader*; o sistema conhece a localização de cada pessoa dependendo do *reader* que leu o sinal e da potência do referido sinal.

O *software* permite gerir em tempo real e de forma centralizada os avisos ao pessoal do centro, alarmes, controlo de portas e activação de protocolos que se considerem oportunos. Caso se verifique uma fuga ou situação irregular é activado um alarme no sistema.

2.3.1.3 - Kimaldi - “Controlo de presença, acesso e recursos”

A solução de controlo de presença da Kimaldi [33] procura garantir que só os utilizadores autorizados acessem às instalações (controlo de acesso), que os clientes só acessem às instalações nos horários que reservaram (controlo horário), que seja possível detectar a presença dos clientes nos diferentes espaços (controlo de presença) tendo em conta os privilégios que estes têm e que seja ainda possível gerir o uso que os clientes fazem dos recursos informáticos (controlo de recursos).

Cada utilizador tem uma *tag* activa, que é um dispositivo de reduzidas dimensões que transmite periodicamente um sinal a 2,4 GHz de fraca potência (72 mW). Os sinais emitidos pelas *tags* são lidos por *readers* de *tags* RFID activos. Em cada acesso ou zona que se queira controlar instala-se um destes *readers* (por exemplo no tecto falso). Os *readers* de *tags* RFID activos ligam-se a um servidor por Ethernet, RS-232 ou RS-485 e enviam em tempo real as leituras de todas as *tags*. Além disso, estes *readers* podem guardar um registo dos eventos produzidos.

Como exemplo, numa instalação realizada pela Kimaldi em Portugal, as *tags* activas foram utilizadas para detectar a presença dos clientes; controlar os pontos de entrada e saída, gerar um registo da presença e entrada/saída de curta duração; autorizar o *login* aos sistemas informáticos só depois de os clientes premirem um botão de chamada presente em cada *tag* activa; para aceder ao edifício, existe um sistema complementar baseado num teclado onde os utilizadores introduzem o seu código. O sistema necessita de detectar a *tag* e verificar o código para permitir o acesso.

Todo o sistema é gerido por *software* que efectua o controlo de faltas, horas extra, turnos, férias, etc., assim como a integração no sistema de facturação; controlo de acesso das portas, declaração das regras e direitos de cada cliente, empregados e gestores; controlo do *login* aos recursos informáticos. Cada utilizador pode alterar o seu número de identificação pessoal (NIP) e abrir à distância a porta de entrada, uma função ergonómica que alivia a pressão devida à grande rotação das entradas e saídas.

2.3.1.4 - Kimaldi - “Sistema de localização de pessoal hospitalar”

Esta solução permite que os utentes de um hospital possam ser localizados e receber ajuda em qualquer situação de emergência. A solução baseia-se na tecnologia RFID activa para identificar o pessoal mediante o uso de uma *tag*, que inclui um botão de alerta de emergência [1].



Figura 2.9 - Aspecto do reader e tags utilizados.

A identificação efectua-se através de uma *tag* RFID que a pessoa transporta permanentemente e que transmite os dados que contém quando detecta que está a ser interrogada por um *reader* RFID. A *tag* é codificada com um identificador único (ID), o que permite que as leituras das diferentes *tags* RFID fiquem associadas à identificação individual. Os *readers* identificam a *tag* no momento em que um utilizador prima o botão de aviso. Este sinal de alarme é enviado ao *software* de controlo que apresenta no ecrã a informação associada à *tag* (nome do utilizador e outros dados considerados relevantes), assim como a localização do mesmo.

O sistema dispõe de um nível de segurança que identifica o utilizador que tenha tirado a pulseira e localiza-o dentro do recinto de controlo. O alarme é emitido através de uma mensagem e é recebido como um aviso sonoro e visual num posto de controlo (computador). No programa de gestão presente no computador, o alarme pode ser visualizado de três formas distintas: num painel de controlo, num histórico e/ou num sinóptico. É possível visualizar no ecrã duas vistas de cada vez no modo de ecrã dividido: na vista sinóptica, a exactidão da identificação depende da zona de localização onde se encontre o sujeito, o número de *readers* que se tenham instalado, etc.; na vista de painel é apresentada de forma inequívoca a zona de onde foi lançado o alarme. Há uma terceira vista onde, no modo de histórico, são listados todos os alertas que se tenham produzido, indicando o utilizador que os lançou, a hora, a data e a zona de localização.

Os alertas são registados no *software* indicando, de forma automática, a data e hora, assim como o utilizador que realizou a acção. Toda esta informação fica registada para poder ser processada conjuntamente quando tal for necessário. É importante, portanto, que todos os utilizadores se registem de forma individual ao aceder à aplicação.

A comunicação dos alertas a partir dos *readers* RFID até aos equipamentos de processamento (computadores) é efectuada em *WiFi*. Para isso, cada *reader* possui um conversor *Ethernet/WiFi* e dever-se-á cobrir o edifício de forma conveniente para que o sinal de alarme chegue sem problemas até ao servidor. Qualquer terminal ligado ao sistema recebe a mesma informação no mesmo instante. O alerta pode ser aceite a partir de qualquer

terminal, eliminando-se da vista actual e passando ao histórico. É registado o utilizador que aceitou o alerta, assim como a hora e data em que o efectuou.

2.3.1.5 - Kimaldi - “Controlo de presença e rastreabilidade logística”

A solução “Controlo de presença e rastreabilidade logística” [34] permite realizar um seguimento de rastreio e controlo de presença de qualquer objecto ou pessoa. Centrado no controlo de presença e acompanhamento a partir de um reproduzidor visual em tempo real, este sistema permite supervisionar e cronometrar os processos industriais, os transportes de materiais, os movimentos de objectos, bem como as voltas (rondas) que as pessoas podem realizar. Oferece um controlo de presença contínuo, bem como um controlo horário mediante o qual se pode conhecer o tempo de permanência de uma pessoa num determinado lugar ou a hora de entrada e/ou saída. Esta solução é útil para a localização de mercadorias ou para gerir a logística interna e externa de uma empresa.

O funcionamento desta solução é visual e intuitiva, permitindo ser adaptada a qualquer tipo de empresa. O seu funcionamento pode ser descrito da seguinte forma: a cada elemento ou pessoa associa-se uma *tag* (emissor de impulsos RFID a 2,45 GHz); as *tags* são representadas sobre planos, mapas e/ou esquemas livres, das instalações ou processos; os ícones das *tags* mudam de posição em tempo real, de acordo com os movimentos dos objectos ou pessoas seguidos.

As suas funções básicas centram-se na cronometragem, supervisão de rondas, seguimento e rastreio de itinerários logísticos em tempo real. Algumas das características do sistema são a fácil instalação em qualquer PC ligado à rede, ligação à rede local via TCP/IP, ser baseado no standard RFID activo a 2,45 GHz, possibilidade de obtenção de estatísticas detalhadas sob a forma de gráfico, impressão e exportação, acesso aos dados a partir de qualquer PC e elevada adaptabilidade.

2.3.1.6 - RFID Centre - “Indoor RFID Tracking (TagMobile)”

A solução “TagMobile”[35] é um produto de rastreio em tempo real, desenvolvido pela empresa RFID Centre, que utiliza tecnologia RFID activa e que utiliza *hardware* e *software* numa solução integrada. Trata-se de um sistema configurável que oferece detecção de posição em ambientes interiores.

Através da utilização de tecnologia RFID activa, é possível efectuar rastreio em tempo real em áreas maiores ou mais complexas, como dentro de um edifício hospitalar, industrial ou escritório com muitos corredores. As *tags* activas, ao serem alimentadas por baterias, têm um alcance de sinal muito superior às *tags* passivas, sendo que os *readers* activos são geralmente mais baratos, tornando-se regra geral mais barato de implementar o sistema completo comparativamente a sistemas RFID passivos.

A solução TagMobile é escalável e pode ser personalizada para atender às necessidades específicas de cada utilizador. Pode ser instalada como um sistema totalmente sem fios

usando *WiFi* ou *Ethernet* (sendo usado TCP/IP) ou ainda uma combinação dos dois para enviar dados de posição de volta para o sistema central com menores custos de implementação. Através da utilização de uma senha de segurança, o pessoal autorizado pode aceder ao servidor para consultar a localização dos bens ou pessoas em qualquer lugar dentro da organização.

Algumas das funcionalidades oferecidas pela solução TagMobile são a localização de pessoas e activos, protecção de materiais, gestão de evacuações, visualização dos tempos de deslocação, o controlo de acessos bem como a optimização de recursos móveis. Com a utilização desta solução advêm benefícios como a protecção das instalações, reforço da segurança pessoal, redução da perda de activos, localização de equipamentos, aumento de produtividade da força de trabalho, capacidade de controlar o *stock* em tempo real e a melhoria na utilização de espaços.

2.3.2 - ZigBee

2.3.2.1 - CLEODE - “LifeNurse”

A solução Lifenurse[36] baseia-se na utilização da tecnologia *ZigBee* para o controlo de sinais vitais e a localização de pacientes, utilizando para isso um conjunto de pulseiras, *readers* e *software*.

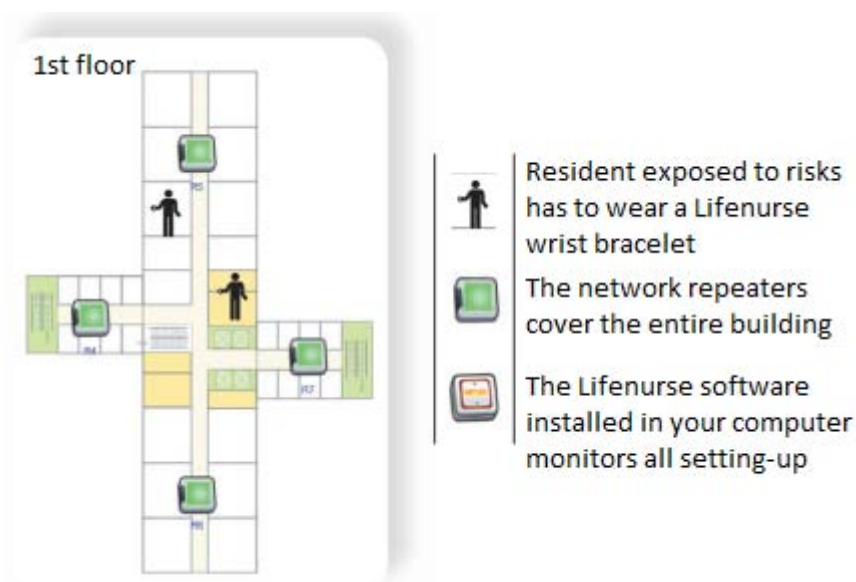


Figura 2.10 - Exemplo de funcionamento do sistema LifeNurse.

A pulseira Lifenurse detecta e confirma a situação de um paciente em perigo (e.g., sinais vitais abaixo do limiar definido), sendo enviado automaticamente um alerta para o Lifenurse *software*, sem que seja preciso que a vítima peça ajuda. O alerta é imediatamente

transmitido através da rede sem fio Lifenurse para a equipa médica; a equipa médica recebe o nome do paciente, a sua localização e a natureza do alerta dentro do edifício, sob o formato escolhido anteriormente (SMS, *beeper*, chamadas telefónicas, etc.), podendo de seguida prestar assistência ao paciente.



Figura 2.11 - Pulseira ZCare, receptor Ubee e imagem do *software* CleoBee.

Esta solução é constituída por 3 componentes: pulseira ZCare, receptor Ubee e o *software* CleoBee. A pulseira ZCare é um detector de queda e pulsação que pode comunicar de acordo com a norma *ZigBee*: em caso de queda transmite um alarme para um coordenador *ZigBee* e o utilizador pode pressionar o botão de emergência presente na pulseira para alertar o pessoal médico. A pulseira ZCare funciona com uma pilha CR2477 o que lhe permite obter uma autonomia de até 6 meses de funcionamento. O receptor Ubee é um dispositivo USB que é usado para controlar uma rede sem fios *ZigBee*, podendo ser utilizado em sistemas operativos Windows, Linux ou MacOS. Quando usado em conjunto com o *software* de gestão de rede CleoBee, Ubee providencia uma solução adequada para coordenação dos vários sensores numa rede *ZigBee*. O *software* CleoBee permite a visualização de uma rede *ZigBee* e a interacção com objectos (como por exemplo a sua localização), sem ser necessário qualquer conhecimento ao nível da programação.

2.3.3 - WiFi

2.3.3.1 - Ekahau - “Real-Time Location System”

Trata-se de um sistema de localização em tempo real, desenvolvido pela empresa Ekahau [37], que utiliza tecnologia *WiFi* capaz de interoperar com qualquer produto *WiFi* de outras marcas e diferentes normas, oferecendo uma precisão ao nível da sala. A solução Ekahau baseia-se nas normas *WiFi* e não requer *readers*, nova cablagem ou barreiras de detecção. O sistema pode ser facilmente instalado, ficando a funcionar em poucos dias ou semanas.



Figura 2.12 - Arquitetura Ekahau RTLS.

O sistema Ekahau utiliza *tags WiFi* para transmitir as localizações dos utilizadores. Essa transmissão opera sobre (as possivelmente já existentes) infra-estruturas *WiFi*, sendo depois toda a informação processada por *software* instalado em computadores específicos.

O *software* Ekahau Vision é uma aplicação Web, acessível através de um qualquer browser Web, e que permite localização e gestão de pessoas ou objectos. Ao utilizar plantas reais do edifício, a interface visual apresenta informação precisa em tempo real, sobre certo utilizador tal como a localização actual, por onde e a que horas passou. Baseia-se em algoritmos que calculam a localização dos objectos a serem monitorizados e é facilmente escalável suportando dezenas de milhares de *tags* num único servidor. O *software* dispõe ainda de alertas automáticos, que notificam o utilizador de acontecimentos baseado nos parâmetros anteriormente configurados.



Figura 2.13 - Tag Ekahau T301BD.

Ao nível das *tags*, é possível escolher várias opções no entanto a mais completa será a *tag* Ekahau T301BD. Trata-se de um dispositivo de localização que permite ao utilizadores enviar e receber mensagens de texto. Essas mensagens podem ser baseadas em eventos predefinidos, estados, localizações ou ainda outros parâmetros definidos no sistema RTLS Ekahau. É possível enviar/receber mensagens a partir de aplicações exteriores ao sistema. A *tag* oferece ainda um botão de pânico para alarme e localização imediata do utilizador e ainda uma bateria recarregável.

Nas zonas em que a precisão de localização seja crítica (nível de precisão inferior a 1m), é possível instalar *location beacons*. Estes transmissores infravermelhos alimentados por baterias permitem assegurar o funcionamento do sistema em zonas cuja cobertura *WiFi* é fraca ao ponto de não permitir a utilização do sistema. A sua instalação não requer qualquer tipo de cablagem nem de uma ligação *WiFi* permanente, o que permite que estes dispositivos sejam levados para outros locais de acordo com as necessidades do momento.

2.3.4 - Comparação das várias soluções

Esta secção apresenta uma comparação das várias soluções analisadas. A tabela resumo organiza as soluções segundo os seguintes parâmetros: i) tecnologia utilizada, ii) área de operação e iii) funcionalidades chave suportadas por cada uma delas.

Tabela 2.4 – Tabela resumo de soluções analisadas.

Solução	Tecnologia	Área	Funcionalidades suportadas
BlueTag - Patient and safety Security	RFID activo	Saúde	- Alertas em caso de saídas ou remoção de <i>tags</i> não autorizadas e bateria fraca na <i>tag</i> - Software que processa o alerta e apresenta a ficha do paciente
Kimaldi - Controlo de vagueantes	RFID activo	Saúde	- Detecção do posicionamento do paciente através da potência do sinal emitido pela <i>tag</i> - Software que gere em tempo real e de forma centralizada avisos ao pessoal do centro, alarmes e controlo de portas
Kimaldi - Controlo de presença, acesso e recursos	RFID activo	Empresarial Segurança	- Leituras das <i>tags</i> enviadas em tempo real - Histórico dos eventos ocorridos - Limitação do acesso a infra-estruturas e recursos informáticos a utilizadores autorizados
Kimaldi - Sistema de localização de pessoal hospitalar	RFID activo	Saúde	<i>Tag</i> com botão de emergência - Localização imediata de todo o pessoal médico - Não tem limite de utilizadores ou zonas - Sistema multi-leitura que permite identificar mais que uma <i>tag</i> ao mesmo tempo - Detecção de perda ou não utilização da <i>tag</i>
Kimaldi - Controlo de presença e rastreabilidade logística	RFID activo	Empresarial	- Software que permite supervisionar e controlar processos industriais em tempo real - Controlo horário de presença - Dados acessíveis a partir de qualquer computador - Estatísticas detalhadas

RFID Centre - Indoor RFID Tracking (TagMobile)	RFID activo	Empresarial Industrial Saúde Segurança	• Localização e protecção de pessoas ou bens em tempo real • Controlo de acessos e gestão de evacuações • Controlo de inventários em tempo real
CLEODE - LifeNurse	ZigBee	Saúde	• <i>Tag</i> com botão de alarme e LED de estado • Detecção de quedas e problemas cardíacos de pacientes • Recepção do alerta com o nome do paciente, posição dentro do edifício e a natureza do alerta no software de controlo
Ekahau - Real-Time Location System	WiFi	Empresarial Industrial Saúde	• Comunicação bidireccional entre <i>tags</i> e <i>readers</i> que permite o envio e recepção de mensagens • <i>Tags</i> com bateria recarregável o que elimina a necessidade de compra e troca de pilhas • Sistema instalável em qualquer rede <i>WiFi</i> existente • Possibilidade de instalação de <i>location beacons</i> para maior precisão de localização

Pela análise da tabela verifica-se o predomínio da tecnologia RFID activa perante as outras tecnologias referidas. Tal facto poder-se-á dever à maior divulgação desta tecnologia para os propósitos de localização e identificação de pessoas e bens. A área de aplicação de excelência destas soluções é a da saúde, onde estes sistemas são utilizados para controlo de pacientes críticos, quer ao nível de localização e identificação de pacientes, quer ao nível de envio de pedidos de auxílio e monitorização de sinais vitais. Existem no entanto outras áreas de interesse como a empresarial, a industrial e a de segurança onde também se tira grande partido da implementação destes sistemas. Em relação às funcionalidades base verifica-se a sua repetição em várias soluções diferentes, existindo no entanto soluções que possuem funcionalidades mais avançadas que outras, sendo um exemplo disso a comunicação bidireccional entre *tags* e *readers*.

Capítulo 3

Descrição do sistema

Neste capítulo são apresentadas as funcionalidades e os requisitos pretendidos para o sistema. Após essa enumeração é efectuada a escolha das tecnologias a utilizar para desenvolvimento. No final é feita a caracterização da arquitectura do sistema.

3.1 - Listagem das funcionalidades

Apresenta-se de seguida a lista de funcionalidades consideradas mais relevantes para o sistema, classificadas de acordo com a sua importância: **I.E.** - Implementação Essencial; **I.I.** - Implementação Importante; **I.O.** - Implementação opcional.

- Localização e identificação de utilizadores em tempo-real a nível interior (**I.E.**)
- Registos temporais de entrada/saída dos utilizadores do sistema (**I.E.**)
- Registos dos percursos efectuados com associação dos locais frequentados ao longo do tempo (**I.E.**)
- Troca de mensagens entre agentes do sistema (**I.I.**)
- Implementação de perfis de utilizador (**I.I.**)
- Localização e identificação de utilizadores em tempo-real a nível exterior (**I.I.**)
- Informação específica orientada ao local onde o utilizador se encontra (e.g., horário de atendimento dos serviços de informática, contactos dos recursos humanos etc.) (**I.O.**)
- Possibilidade de controlo de iluminação/temperatura do local onde se encontra (**I.O.**)

- Visualização no dispositivo de localização de um mapa com POI (*Points of Interest*), como casas de banho, máquinas multibanco, salas de reunião etc. (I.O.)

3.2 - Listagem de requisitos

Nesta secção é apresentada a listagem dos requisitos (divididos em funcionais e não funcionais) que o sistema deve cumprir.

3.2.1 - Requisitos funcionais

Os requisitos funcionais são aqueles que descrevem o comportamento do sistema, ou seja, funções ou serviços que o sistema dever ser capaz de realizar. Apresentam-se de seguida os considerados para o sistema:

- Comunicação entre os vários agentes constituintes do sistema.
- Distribuição de *readers* de forma a cobrir a área desejada para implementação do sistema.
- Efectuar localização de utilizadores a nível interior.
- Efectuar localização de utilizadores a nível exterior.
- Ligação à Internet de forma a ser possível a interacção com o sistema a partir de localizações remotas (e.g. 3G).
- Controlo remoto do sistema
 - Os administradores devem poder ligar/desligar o sistema e configurar os parâmetros que influenciam o funcionamento do sistema.
 - Os utilizadores comuns devem conseguir configurar se desejam ou não receber notificações, se querem poder ser localizados e ainda ter a possibilidade de enviar e receber mensagens.
- Arquivo de dados na base de dados
 - Do ponto de vista do administrador deve ser possível a consulta das localizações, dos registos das horas de entrada e saída bem como do histórico de mensagens enviadas e recebidas entre utilizador e servidor.
 - Do ponto de vista do utilizador deve ser possível a consulta das localizações e dos registos das horas de entrada e saída do próprio, assim como as mensagens trocadas entre servidor e utilizador e entre utilizadores.
 - Devem ser armazenados na base de dados as contas, perfis, grupos e estados dos utilizadores, o registo das mensagens trocadas entre agentes do sistema,

a topologia de localizações (internas e externas) através do mapeamento de pontos de acesso ou coordenadas GPS e o histórico das localizações dos utilizadores ao longo do tempo.

3.2.2 - Requisitos não funcionais

Os requisitos não funcionais são requisitos que impõem restrições, ou atributos de qualidade ao sistema como segurança, precisão e desempenho. Listam-se de seguida os considerados para o sistema:

- Dispositivos com autonomia mínima de 8 horas.
- Precisão média mínima de localização de 1 piso.
- Acessos aos dados de utilizadores devem estar protegidos por palavras-passe.

3.3 - Tecnologias e técnicas utilizadas

Nesta secção são demonstradas e devidamente fundamentadas as escolhas feitas relativamente às tecnologias e técnicas de localização a utilizar.

Tendo em conta as tecnologias estudadas no capítulo 3, pode-se afirmar que a tecnologia *ZigBee* será provavelmente a mais equilibrada, reunindo um conjunto interessante de características para o sistema que se pretende implementar. No entanto, os terminais móveis com tecnologia *ZigBee* são rudimentares em termos das funcionalidades e interactividade que podem oferecer. Para além disso, a tecnologia *ZigBee*, obriga os utilizadores a trazerem consigo um dispositivo extra para envio da posição do utilizador, envio e recepção de notificações. De forma a contornar essas desvantagens, optou-se por escolher a tecnologia *WiFi* para implementação do sistema, pois quando emparelhada com um *smartphone* (com suporte *WiFi*) é possível obter uma maior interactividade entre utilizadores do sistema, usufruir de funcionalidades mais avançadas e suporte de uma apresentação da informação trocada mais amigável (*user friendly*) quando comparado com as outras opções estudadas, tal como definido pelos requisitos do sistema descritos na secção anterior. De notar ainda que os *smartphones* com suporte *WiFi* possuem (por norma) ligações 3G e GPS, o que permite a implementação de localização exterior. Esta escolha prova também ser acertada do ponto de vista da redução do custo e tempo de implementação, pois ao utilizar *smartphones* compatíveis com o protocolo IEEE 802.11 (fáceis de obter no mercado a preços competitivos), evita-se a compra de dispositivos específicos (que demorariam tempo a chegar) e ainda se beneficia do facto do local de instalação do sistema já dispor de uma rede *WiFi* funcional que cobre todo o edifício.

Tomada a decisão de utilizar a tecnologia *WiFi* conjuntamente com um *smartphone* será agora discutido qual o sistema operativo de móvel mais indicado para esta aplicação. Nas tabelas seguintes são efectuados a comparação de vários parâmetros relevantes para a implementação que se pretende.

Tabela 3.1 – Tabela comparativa dos vários sistemas operativos móveis considerados.

	Android 2.2	Apple iOS 4.2	Windows Phone 7
Sistema Operativo Open Source	Sim	Não	Não
Custo médio de um equipamento	Médio	Elevado	Elevado
Multitasking	Sim	Sim	Não
Suporte Flash	Sim	Não	Não
Suporte HTML 5	Sim	Sim	Não
WiFi Hotspot	Sim	Não	Não

O sistema operativo Android é o único que é *Open Source* e que permite o desenvolvimento e publicação de aplicações sem qualquer tipo de restrição ao nível de licenças e aprovação do mercado de aplicações. Este sistema operativo é também o único a suportar *Adobe Flash*, que é, nos dias que correm uma das linguagens mais usadas ao nível do desenvolvimento de aplicações interactivas. É também o único sistema que suporta a funcionalidade de *WiFi Hotspot* (que permite transformar o *smartphone* num ponto de acesso para outros *smartphones* que queiram aceder à rede), podendo assim ajudar à localização de utilizadores. A juntar a todas estas vantagens, o sistema operativo Android já tem modelos de *smartphones* a preços bastante competitivos (na ordem dos 150 €). Por observação da tabela verifica-se que o sistema operativo Windows Phone 7 é mais limitado que os seus concorrentes directos em termos de funcionalidades, ao que não estará alheio o facto de ser um sistema operativo mais recente que os outros referidos [7] [38].

Tabela 3.2 – Quota global de mercado dos sistemas operativos móveis considerados.

	Android	Apple iOS	Windows Phone
Quota de mercado global em 2009	4 %	14 %	9 %
Quota de mercado global em 2010	17 %	15 %	5 %
Quota de mercado global prevista para 2011	22 %	17 %	5 %
Quota de mercado global prevista para 2014	30 %	15 %	4 %

Através da tabela da quota de mercado global [39], verifica-se que o Android é o sistema operativo com maior expressão, com tendência para alargar ainda mais o seu domínio comparativamente aos outros nos próximos anos. O sistema operativo da *Apple* possuiu também uma quota significativa que no entanto parece ter estabilizado. Já o *Windows Phone* tem uma quota de mercado relativamente baixa com tendência a ser ainda mais pequena no futuro. Após estas observações, pode-se afirmar que dos três sistemas operativos móveis considerados, o sistema Android é aquele que apresenta as melhores características.

Pelos motivos acima descritos, decidiu-se utilizar um *smartphone* compatível com tecnologia *WiFi* e sistema operativo Android para a implementação deste sistema.

Relativamente às técnicas de localização discutidas na secção 2.2, foi logo excluída à partida a técnica TDoA pois a mesma não é adequada para ambientes interiores. Também não foi considerada a técnica NAP pois apesar da precisão definida nos requisitos não ser elevada, esta técnica por si só não assegura essa precisão. Restava a técnica RSSI que é demasiado complexa de implementar devido à obrigatoriedade de ter nas imediações três ou mais APs de forma a ser possível efectuar uma triangulação. Assim sendo optou-se por combinar a técnica NAP com RSSI. Esta combinação permite obter uma maior precisão, sem trazer para o sistema a complexidade extra introduzida pela aplicação de RSSI na sua totalidade. Esta técnica será explicada com mais detalhe no capítulo 4.

3.4 - Arquitectura do sistema

Tendo em conta as funcionalidades e os requisitos funcionais e não funcionais conjugados com as vantagens das tecnologias e técnicas escolhidas (*WiFi*, Android, NAP+RSSI), apresenta-se de seguida o resumo da arquitectura. O sistema a implementar será constituído pelos seguintes elementos base:

- Servidor Web com acesso a base de dados relacional
- Pontos de acesso *WiFi* à rede de localização
- Smartphones com sistema operativo Android

Na figura 3.1 pode-se observar a maneira como cada um dos elementos do sistema se interliga.

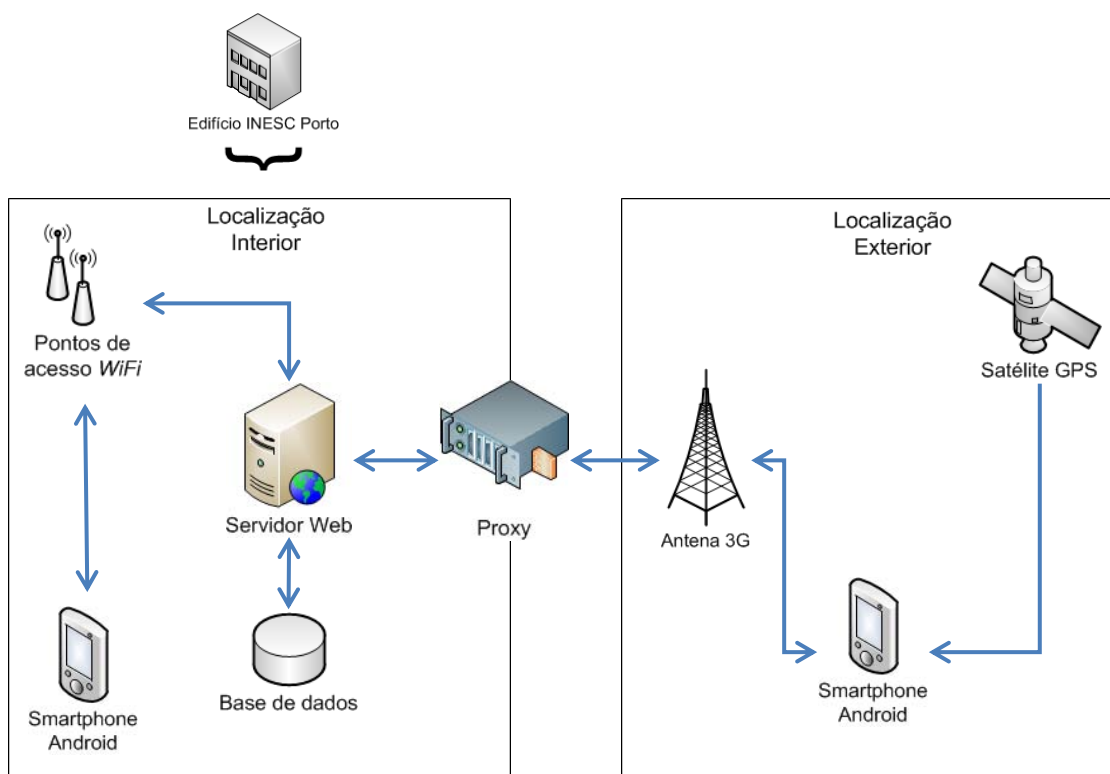


Figura 3.1 - Esquemático do sistema implementado (localização interior e exterior).

Com base na figura 3.1 pode-se afirmar que o sistema se encontra dividido em duas partes: i) localização interior e ii) localização exterior. Em i) o *smartphone* Android encontra-se dentro do edifício do INESC Porto e comunica a sua posição com os pontos de acesso *WiFi* localizados nos vários pisos. Os pontos de acesso por sua vez comunicam a posição do *smartphone* à base de dados, fazendo para isso uso do servidor Web implementado. Em ii) o *smartphone* encontra-se numa localização exterior ao edifício do INESC Porto. O satélite GPS indica ao *smartphone* as coordenadas em que o utilizador se encontra, sendo que o *smartphone* faz uso da ligação 3G para comunicar com o servidor Web e base de dados existentes no edifício.

3.4.1 - Servidor Web com acesso à base de dados

O servidor Web tem por objectivo permitir o acesso e gestão do sistema de forma remota. Este servidor (alojado num computador) é sustentado por uma base de dados e é responsável por ligar ou desligar o sistema, associar ou remover dispositivos (sejam *smartphones* ou pontos de acesso) da rede do sistema, armazenar e listar a topologia da rede através dos endereços BSSID (*Basic Service Set Identifier*) dos dispositivos e guardar um histórico temporal das localizações frequentadas por um utilizador e das mensagens trocadas dentro do sistema.

Em termos do *software* utilizado para a implementação do servidor *Web*, optou-se pela instalação do servidor HTTP (Hypertext Transfer Protocol) Apache [40] por ser uma alternativa gratuita *open source* e por ter suporte da linguagem PHP (*Hypertext Preprocessor*) [41] e dos módulos de segurança TLS (*Transport Layer Security*) e SSL (*Secure Sockets Layer*). Relativamente à base de dados a escolha recaiu na base de dados relacional PostgreSQL (versão 9.0.4) [42] devido a ser uma solução gratuita e *open source* fiável que garante a integridade dos dados e pela documentação e suporte disponibilizados, sendo que para interface visual da base de dados foi instalado o *software* phpPgAdmin (versão 5.0.2) [43]. Por fim instalou-se a linguagem PHP (versão 5.3.3) por conter *drivers* que permitem a manipulação de bases de dados PostgreSQL e a troca de dados através da utilização de *Web Services*.

Ao nível das linguagens de programação utilizadas, os mecanismos de interacção do servidor foram escritos em PHP e JSON e a base de dados criada utilizando a linguagem SQL.

3.4.2 - Pontos de acesso à rede de localização

Os pontos de acesso funcionam como *gateways* de acesso à rede de localização para os *smartphones* Android. Deve ser assegurada a existência de um número de pontos de acesso suficiente (neste caso utilizaram-se os que já existem no edifício), para que a cobertura da rede sem fios seja o mais abrangente possível de modo a que a localização e identificação dos utilizadores ocorra sem falhas. Estes dispositivos são por norma APs ou *routers* que trazem integrado *software* disponibilizado pelos fabricantes.

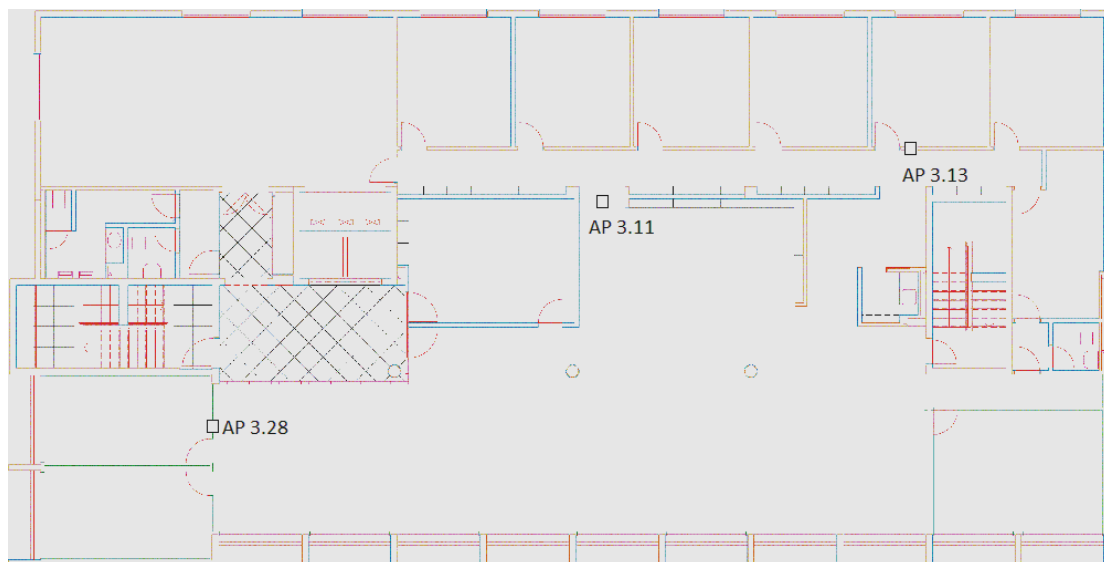


Figura 3.2 - Planta do piso 3 do edifício INESC Porto com os APs existentes assinalados.

Na figura 3.2 que corresponde ao piso 3 do edifício do INESC Porto verifica-se a existência de três pontos de acesso *WiFi* que asseguram a cobertura de rede no piso inteiro. Os pontos de acesso foram nomeados de acordo com a sala em que se encontram (caso dos APs 3.28 e

3.13), ou a sala imediatamente mais próxima (AP 3.11). Os outros pisos encontram-se igualmente cobertos, embora em localizações diferentes, sendo que a nomenclatura utilizada é semelhante à utilizada para o piso 3. O mapeamento dos pontos de acesso é discutido na subsecção 5.1.1.

3.4.3 - *Smartphones* com sistema operativo Android

Estes são os dispositivos que estarão em contacto directo com o utilizador e que tratam de enviar a informação com a localização para o ponto de acesso a que se encontram ligados e consequentemente para o servidor de controlo. Dependendo da capacidade destes dispositivos poderá ser possível receber/enviar mensagens ou até outros parâmetros como a temperatura registada. O modelo utilizado para desenvolvimento e testes foi o Samsung Galaxy S I9000 com sistema operativo Android versão 2.2, tendo-se utilizado este modelo pelo facto de já existir um que era propriedade do INESC Porto. Convém no entanto referir que todos os *smartphones* Android actualmente no mercado contam com as tecnologias GPS, 3G e *WiFi* pelo que seria possível a utilização de outros modelos. As características do modelo utilizado estão descritas na tabela 3.3.

Tabela 3.3 – Especificações técnicas do *smartphone* Samsung Galaxy S.

Rede	2G	GSM 850/900/1800/1900 MHz
	3G	HSDPA 900/1900/2100 MHz
Tamanho	Dimensões	122.4 x 64.2 x 9.9 mm
	Peso	119 g
Bateria	Tipo	Li-Ion 1500 mAh
	Standby	Até 750 h (2G) / Até 576 h (3G)
	Tempo de conversação	Até 13 h 30 min (2G) / Até 6 h 30 min (3G)
Ecrã	Tipo	Super AMOLED ecrã táctil capacitivo com 16 milhões de cores
	Tamanho	4.0 polegadas
	Resolução	480 x 800 pixéis
Processador		1 GHz ARM Cortex-A8, PowerVR SGX540 GPU, Hummingbird chipset
Memória	RAM	512 MB
	ROM	2 GB
	Interna	8 GB
	Expansão	microSD até 32 GB
Transmissão de dados	GPRS	Class 12 (4+1/3+2/2+3/1+4 slots), 32 - 48 kbps
	3G	HSDPA - 7.2 Mbit/s; HSUPA - 5.76 Mbit/s
	WLAN	WiFi 802.11 b/g/n; DLNA; WiFi hotspot
	USB	v2.0 Micro USB
Outros	GPS	Com suporte para GPS assistido

A programação para Android foi feita seguindo as recomendações dos desenvolvedores do sistema operativo, utilizando para isso o IDE Eclipse com o *plugin* ADT Android. A linguagem de programação utilizada é uma conjugação de Java com XML, sendo o Java utilizado para criar funções e variáveis enquanto que o XML é dedicado a definir o *layout* da aplicação e quais as permissões da aplicação desenvolvida (acesso à Internet, acesso a configurações do *smartphone*, etc.).

Capítulo 4

Desenvolvimento do sistema

Neste capítulo é apresentada informação acerca da abordagem e desenvolvimento dos vários componentes do sistema.

4.1 - Base de dados

Nesta secção é feita a descrição da base de dados ao nível das suas funcionalidades e da estrutura implementada. Entre a informação armazenada na base de dados encontram-se as contas dos utilizadores, perfis, grupos e estados dos utilizadores, o registo das mensagens trocadas entre agentes do sistema, a topologia de localizações (internas e externas) através do mapeamento de pontos de acesso ou coordenadas GPS e o histórico das localizações dos utilizadores ao longo do tempo. Para o desenvolvimento e melhor percepção da estrutura da base de dados foram criados dois modelos, um modelo relacional e um modelo entidade associação que se encontram nos anexos deste documento.

Ao nível da estrutura da base de dados, a mesma encontra-se dividida em doze tabelas: “GrupoUtilizador”, “PerfilUtilizador”, “EstadoUtilizador”, “Utilizador”, “TipoMensagem”, “Mensagem”, “Edifício”, “Piso”, “Sala”, “PontoAcesso”, “Externa” e “Encontra_se”. A tabela “GrupoUtilizador” contém os grupos a que cada utilizador pode pertencer, como por exemplo os grupos Administrador, Visitante ou Regular. A tabela “Utilizador” contém o registo dos utilizadores que podem usufruir do sistema. A cada utilizador está associado um identificador único, um endereço de *email* e *password* assim como o número e o IMEI do *smartphone* desse utilizador que irá aceder ao sistema. Na tabela “PerfilUtilizador” estão armazenados os vários perfis que cada utilizador pode activar num determinado momento no programa Android, de forma a indicar se pretende, por exemplo, ter o *tracker* e as notificações activas. Na tabela “EstadoUtilizador” encontram-se os vários estados em que o utilizador se pode encontrar, tal como Em Reunião ou Férias. As mensagens trocadas entre os vários agentes do sistema ficam guardadas na tabela “Mensagem” onde estão presentes os campos remetente e destinatário

(*username* respectivo dos utilizadores), o conteúdo, o estado da mensagem (lida ou não lida), a data e hora da mensagem bem como se esta se encontra apagada ou não. Dependendo do tipo de mensagem, elas podem ser enviadas de forma automática (notificações) ou por utilizadores (pessoal), estando os tipos de mensagens existentes armazenados na tabela “TipoMensagem”. As tabelas “Edifício”, “Piso”, “Sala” e “PontoAcesso” relacionam-se entre si de forma a ser possível saber que certo ponto de acesso se encontra em determinada sala, piso e edifício. Na tabela “PontoAcesso” são registados os parâmetros SSID e BSSID da rede à qual se encontram ligados os pontos de acesso. A tabela “Externa” é responsável pelo armazenamento de localizações exteriores à organização onde se encontra implementado o sistema e tem como atributos o nome da localização, o BSSID e SSID do ponto de acesso a que se encontra ligado o *smartphone* (se aplicável), ou as coordenadas GPS (se aplicável). Na tabela “Encontra_se” estão armazenados os registos das localizações percorridas pelos utilizadores ao longo do tempo. Esse registo é conseguido através da introdução na base de dados da data e hora e qual o ponto de acesso (ou localização externa) a que certo utilizador se encontrava ligado. Como atributos desta tabela tem-se o IMEI do *smartphone* do utilizador, o identificador do ponto de acesso associado a esse registo, o identificador da localização externa (se aplicável) assim como a data e a hora aquando a introdução do registo na base de dados.

4.1.1 - Mapeamento dos pontos de acesso

O mapeamento do sistema foi efectuado percorrendo todos os pisos do edifício INESC Porto, utilizando o *smartphone* com a aplicação “WiFi Analyzer” [44] activa para encontrar os pontos de acesso que fizessem o *broadcast* do SSID INESCP-visita³. A cada ponto de acesso encontrado associou-se o piso, o local (que corresponde à sala ou sala mais próxima onde o ponto de acesso se encontra instalado), o BSSID e o canal utilizado que poderá vir a ser utilizado mais tarde para explicar alguns dos resultados obtidos na fase de testes. O resultado do mapeamento efectuado está disposto na tabela 4.1.

³ Foi utilizada esta rede devido a incompatibilidade do sistema operativo Android com o protocolo MS-CHAP utilizado na rede institucional “inescporto”.

Tabela 4.1 – Mapeamento dos pontos de acesso com SSID INESCP-visita.

Piso	Local	BSSID	Canal <i>WiFi</i>
4	Sala 4.20	00:12:d9:42:99:71	6
4	Sala 4.26	00:24:c4:8e:66:c1	1
3	Sala 3.28	00:12:d9:42:93:81	6
3	Sala 3.11	00:0e:83:c8:e0:41	1
3	Sala 3.13	00:12:d9:42:9a:21	11
2	Sala 2.19	00:12:d9:42:9a:41	6
1	Sala 1.28	00:12:d9:42:95:b1	1
1	Sala 1.9	00:12:d9:42:92:81	1
1	Sala 1.13	00:12:d9:42:99:b1	1
0	Recepção	00:0e:83:cc:04:d1	6
-1	Sala C.8	00:24:c4:1c:99:a1	1
-1	Sala C.4	00:24:c4:1c:97:51	6

Em relação aos resultados obtidos deve ser feita uma pequena ressalva. Estes foram os pontos de acesso mapeados encontrados pelo utilizador que percorreu os vários pisos, utilizando a aplicação “*WiFi Analyzer*”. No entanto isso não quer dizer que tenham sido mapeados todos os existentes, quer devido à aplicação não ter detectado, quer ao facto de durante o mapeamento eventualmente não se ter passado por alguma zona específica. No futuro de forma a prevenir esta situação e para se obter um sistema mais completo, deverá ser desenvolvida uma forma de integração com uma base de dados institucional que contenha informação acerca dos APs a utilizar.

4.2 - Servidor Web

Esta secção faz uma abordagem ao servidor que permite a administração do sistema e que serve de intermediário às comunicações entre a base de dados e a aplicação. O servidor encontra-se alojado no mesmo computador que a base de dados (apesar de tal não ser obrigatório).

A administração do sistema é efectuada no servidor *Web* utilizando a interface “phpPgAdmin” instalada, onde é possível do ponto de vista de um administrador adicionar/remover/modificar utilizadores ou pontos de acesso e do ponto de vista de um utilizador verificar quais os estados e perfis de cada utilizador, assim como as mensagens trocadas entre os agentes do sistema. De forma a garantir maior segurança e privacidade dos dados presentes, cada utilizador deve ter uma conta com nome de utilizador e palavra-passe únicos onde se encontram definidas as permissões desse utilizador.

A comunicação do servidor com a base de dados é efectuada através dos *drivers* (PDO_PGSQL) disponibilizados pela própria linguagem PHP para comunicação com bases de dados PostgreSQL. Em relação à comunicação do servidor com a aplicação Android a mesma é feita recorrendo a *Web Services* utilizando o protocolo HTTP. Numa primeira fase pensou-se integrar o processamento da comunicação com a base de dados (*parser*) directamente na aplicação Android, evitando assim a necessidade de existir um terceiro agente no sistema. No entanto tal alternativa revelou-se pouco indicada por três motivos: i) baixo desempenho, ii) segurança reduzida e iii) sobrecarga da rede *WiFi*.

No caso i) o desempenho da aplicação é afectado negativamente, pois a introdução do código directamente na aplicação faz com que a mesma passe a ocupar mais espaço em disco e em memória. A fluidez com que a aplicação corre é também afectada devido à totalidade do processamento da comunicação com a base de dados ser efectuada do lado do cliente (aplicação), o que (principalmente) em *smartphones* de gamas inferiores tem graves consequências ao nível da usabilidade e *multitasking*. No caso ii) a introdução de um terceiro agente no sistema que faz uso de *Web Services* para comunicação, adiciona uma camada extra de segurança que não existiria se fossem utilizados os *drivers* Java na aplicação (alternativa pensada inicialmente) para comunicação com a base de dados. No caso iii) como o sistema passaria a ter uma comunicação descentralizada com a base de dados, existiria o problema de garantir a integridade dos dados presentes na mesma, o que obrigaria à utilização de mensagens de sincronização e controlo que mediante o número de dispositivos ligados ao sistema, poderiam provocar o congestionamento da rede utilizada.

Resumindo, associado ao servidor Web foi necessário desenvolver um *parser* que processa os pedidos vindos da aplicação Android e os converte numa linguagem capaz de ser processada pela base de dados. A resposta da base de dados para a aplicação é também convertida pelo *parser*, de forma a que a aplicação possa representar no ecrã a informação recebida.

4.2.1 - Interface de administração do servidor *Web*

Como foi referido anteriormente existe uma interface Web que permite a execução de tarefas de administração ou simples consulta. Na figura 4.1 é possível verificar a adição de um ponto de acesso por um administrador.

PostgreSQL 9.0.4 running on 127.0.0.1:5432 — You are logged in as user "postgres"

phpPgAdmin: PostgreSQL: sisloc: public: pontoacesso:

Insert row?

Column	Type	Format	Null	Value
id_ponto	integer	Expression		nextval('pontoacesso_id_ponto_seq::regc')
bssid	character varying(40)	Value		00:12:d9:42:99:71
ssid	character varying(40)	Value		INESC-visita
id_sala	bigint	Value		1

Insert Insert & Repeat Cancel ☒ Enable

id_sala	nome_sala	id_piso
1	C.4	1
2	C.8	1

Next >>

Figura 4.1 - Introdução de um novo ponto de acesso no sistema.

Aos utilizadores comuns é dado acesso para por exemplo consultarem as mensagens que receberam ou enviaram como se pode observar na figura 4.2.

id_mensagem	remetente	destinatario	conteudo
1	yoda@faraway.sw	luceskywalker@tatooine.sw	Hard to see, the dark side is.
4	chewbacca@millenniumfalcon.sw	luceskywalker@tatooine.sw	Rrrrrrr-ghghghghgh!
10	darthvader@deathstar.sw	luceskywalker@tatooine.sw	You cannot hide forever, Luke.
11	darthvader@deathstar.sw	luceskywalker@tatooine.sw	There is no escape! Dont make me destroy you. Luke, you do not yet realize your importance. You haveve only begun to discover your power! Join me, and I will complete your training! With our combined strength, we can end this destructive conflict, and bring order to the galaxy.
13	darthvader@deathstar.sw	luceskywalker@tatooine.sw	Luke I am your father!

Figura 4.2 - Consulta das mensagens recebidas por um utilizador.

Na figura é possível observar todas as mensagens recebidas pelo utilizador com o endereço de *email* "luceskywalker@tatooine.sw". De notar que não estão presentes detalhes como a hora a que foi recebida a mensagem, o tipo e o estado para facilitar a visualização da imagem que de outra forma ficaria com letra demasiado pequena.

4.2.2 - Funcionamento do *parser* do servidor *Web*

Nesta secção serão demonstrados exemplos, acompanhados por código, do modo de funcionamento do *parser* do servidor.

Numa fase inicial é necessário estabelecer a ligação do servidor à base de dados. Para isso é utilizado o código PHP presente na figura 4.3 onde é definido o endereço IP (neste caso a própria máquina), a porta e o nome da base de dados. Se por algum motivo a tentativa de conexão falhar, o servidor retorna erro.

```
$conn = pg_connect("host=127.0.0.1 port=5432 dbname=sisloc
user=postgres password=root");
if (!$conn) {
    echo "Não foi possível estabelecer a ligação à base de
dados.\n";
    exit;
}
```

Figura 4.3 - Ligação do servidor *Web* à base de dados.

Como exemplo do papel desempenhado pelo *parser* numa funcionalidade específica suportada pelo sistema, será descrito o envio, consulta e remoção de mensagens. Inicialmente o *parser* recebe da aplicação Android os parâmetros que indicam que o utilizador pretende escrever uma mensagem (“destinatário”, “remetente” e “conteúdo”). Após recepção dos parâmetros, o *parser* verifica que eles dizem respeito ao excerto de código representado na figura 4.4 e executa a respectiva *query* (neste caso um INSERT) com os parâmetros recebidos na base de dados.

```
if($_REQUEST['destinatario'] && $_REQUEST['remetente'] &&
$_REQUEST['conteudo']){
    $db_insert_msg=pg_query("INSERT INTO Mensagem
(remetente, destinatario, conteudo, estado,apagada) VALUES
('".$_REQUEST['remetente']."'','".$_REQUEST['destinatario']."'','".$_R
EQUEST['conteudo']."'','Não lida',FALSE)");
}
```

Figura 4.4 - *Parser* do servidor *Web* - Envio de mensagens.

Para listar as mensagens presentes na caixa de entrada de um utilizador, basta passar ao *parser* os parâmetros “email” e “remetente” que executam o código da figura 4.5.

```
if($_REQUEST['email'] && $_REQUEST['remetente']){  
    $db_msg=pg_query("SELECT *,to_char(data_hora, 'DD-MM-  
YYYY | HH24:MI:SS') FROM utilizador JOIN mensagem ON email=remetente  
WHERE destinatario = '". $_REQUEST['email']."' AND apagada=FALSE  
ORDER BY id_mensagem DESC");  
    while($e=pg_fetch_assoc($db_msg))  
        $output[]=$e;  
  
    print(json_encode($output));  
}
```

Figura 4.5 - Parser do servidor Web - Listagem de mensagens recebidas.

A *query* executada realiza um SELECT, que neste caso, retorna todos os campos das mensagens armazenadas na tabela “Mensagem” respeitantes ao utilizador do parâmetro “email”, cabendo depois à aplicação filtrar os campos de interesse. De notar ainda que o resultado desta listagem é apresentado sob o formato codificado JSON de modo a facilitar a leitura por parte da aplicação Android.

Para a remoção de mensagens a aplicação envia os parâmetros correspondentes a esse pedido, neste caso “email” e “apagada”, sendo executado o código visível na figura 4.6.

```
if($_REQUEST['email'] && $_REQUEST['apagada'] &&  
$_REQUEST['id_mensagem']){  
    $db_apagar_mensagem=pg_query("UPDATE mensagem SET  
apagada='". $_REQUEST['apagada']."' WHERE  
id_mensagem='". $_REQUEST['id_mensagem']."'");  
}
```

Figura 4.6 - Parser do servidor Web - Remoção de mensagens.

Este excerto de código executa um UPDATE no parâmetro “apagada” colocando-o como verdadeiro (trata-se de um booleano) na mensagem que se deseja apagar. Por motivos de integridade da base de dados, a mensagem irá continuar a existir na base de dados, simplesmente o utilizador não a irá ver pois ela ficará invisível para a aplicação Android.

4.3 - Aplicação Android

Esta secção consiste na apresentação da aplicação Android desenvolvida (de nome SisLoc); serão explicadas cada uma das vistas, bem como o modo de funcionamento e as dificuldades encontradas no desenvolvimento da aplicação.

A aplicação SisLoc encontra-se dividida em dois ecrãs principais, um ecrã de autenticação e um ecrã constituído por três abas: “Estado”, “Mensagens” e “Perfil”.

4.3.1 - Ecrã de autenticação

Neste ecrã são apresentados dois campos de introdução de texto (nome de utilizador e palavra passe) e três botões (“Entrar”, “Definições” e “Sair”). Após introdução de um par nome de utilizador e palavra passe válidos nos campos de texto e clique no botão “Entrar”, é dado ao utilizador acesso ao sistema como se verifica na figura 4.7 a). Caso os valores introduzidos sejam incorrectos o utilizador é alertado através de uma mensagem que surge na parte inferior do ecrã como se pode observar na figura 4.7 b). O último botão presente no ecrã de autenticação é o botão “Sair” que ao ser pressionado termina a aplicação e volta ao ecrã principal do *smartphone*.



Figura 4.7 - Ecrã inicial.

a) Autenticação efectuada com sucesso. b) Autenticação falhada.

Ao pressionar o botão “Definições”, é apresentada uma nova vista, figura 4.8 a), onde é dado ao utilizador a possibilidade de configurar o endereço do servidor ao qual se quer ligar. Nesta vista existe o botão “Servidor *default*” que coloca o endereço do servidor com as configurações originais.

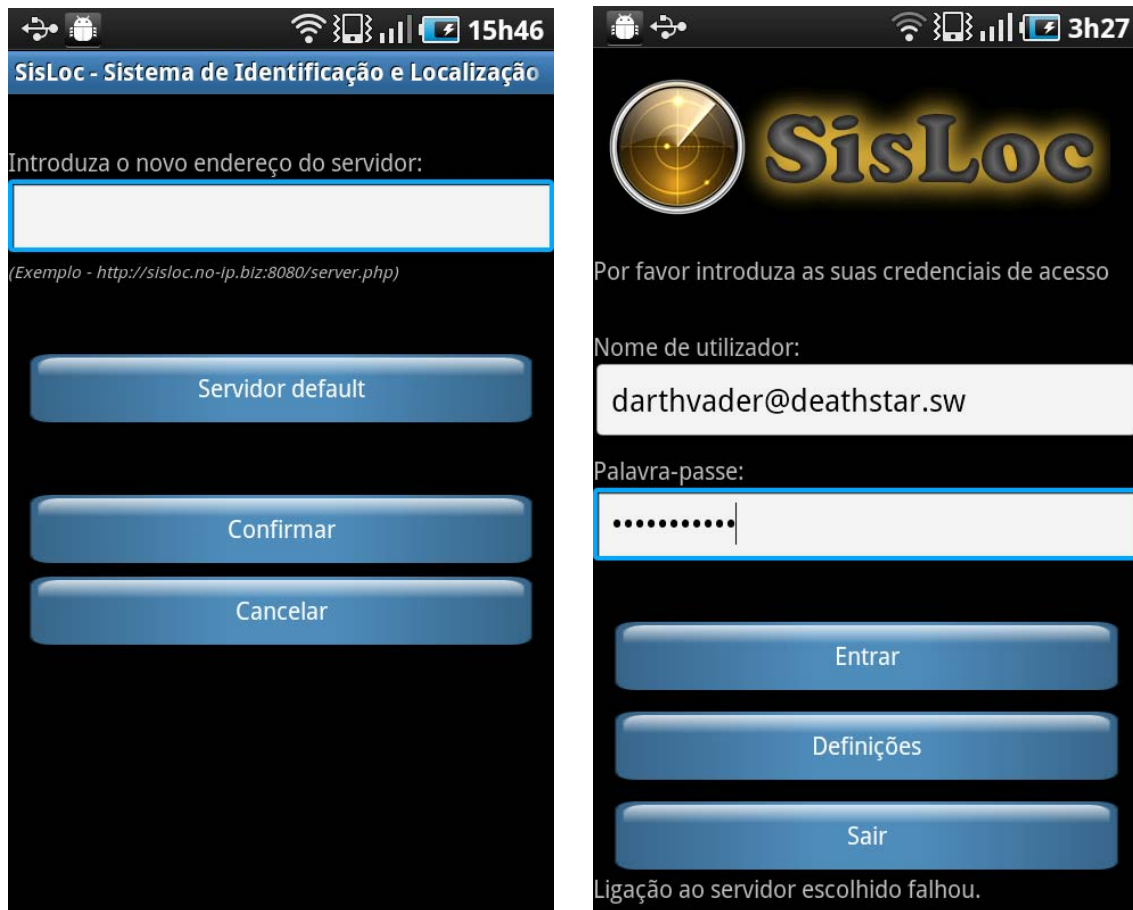


Figura 4.8 - Ecrã de definições.

a) Alteração do endereço de servidor. b) Ligação falhada.

Caso o endereço de servidor introduzido seja inválido, o utilizador será alertado para esse pormenor aquando a tentativa de autenticação, através de um alerta na parte inferior do ecrã como se pode observar na figura 4.8 b).

4.3.2 - Aba “Estado”

A aba apresentada por omissão aquando da autenticação com sucesso no sistema é a aba de “Estado” (figura 4.9).

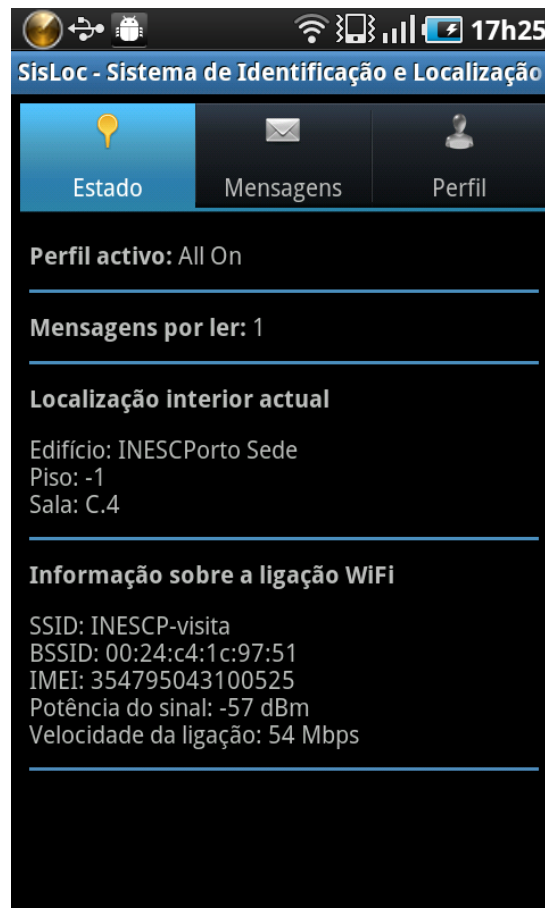


Figura 4.9 - Aba de estado que é iniciada por omissão após autenticação.

Nesta aba são disponibilizadas informações acerca do estado do sistema e do utilizador, como o perfil activo de momento, o número de mensagens por ler, o estado da ligação a que o *smartphone* se encontra ligado bem como a localização do utilizador, de acordo com o mapeamento efectuado aos pontos de acesso.

4.3.3 - Aba “Mensagens”

Na aba mensagens (figura 4.10) são apresentados três botões: i) “Criar Mensagem” ii) “Caixa de Entrada” e iii) “Caixa de Saída”.



Figura 4.10 - Aba que apresenta o menu de mensagens.

Em i) é dada a possibilidade ao utilizador de escrever uma mensagem (figura 4.11 a)) e enviá-la para um destinatário através da introdução do seu endereço ou utilizando os endereços presentes na lista de contactos. Em ii) entra-se na caixa de entrada (figura 4.11 b)) onde são visíveis todas as mensagens enviadas para o utilizador autenticado. Nesta vista em lista é possível verificar o remetente da mensagem, a data e hora a que a mensagem foi enviada e o estado da mensagem (lida ou não lida). Em iii) tem-se a caixa de saída cuja apresentação é igual à da caixa de entrada, só que apresenta todas mensagens enviadas pelo utilizador. Nesta vista em lista estão presentes dados como o destinatário da mensagem e a data e hora a que a mensagem foi enviada.

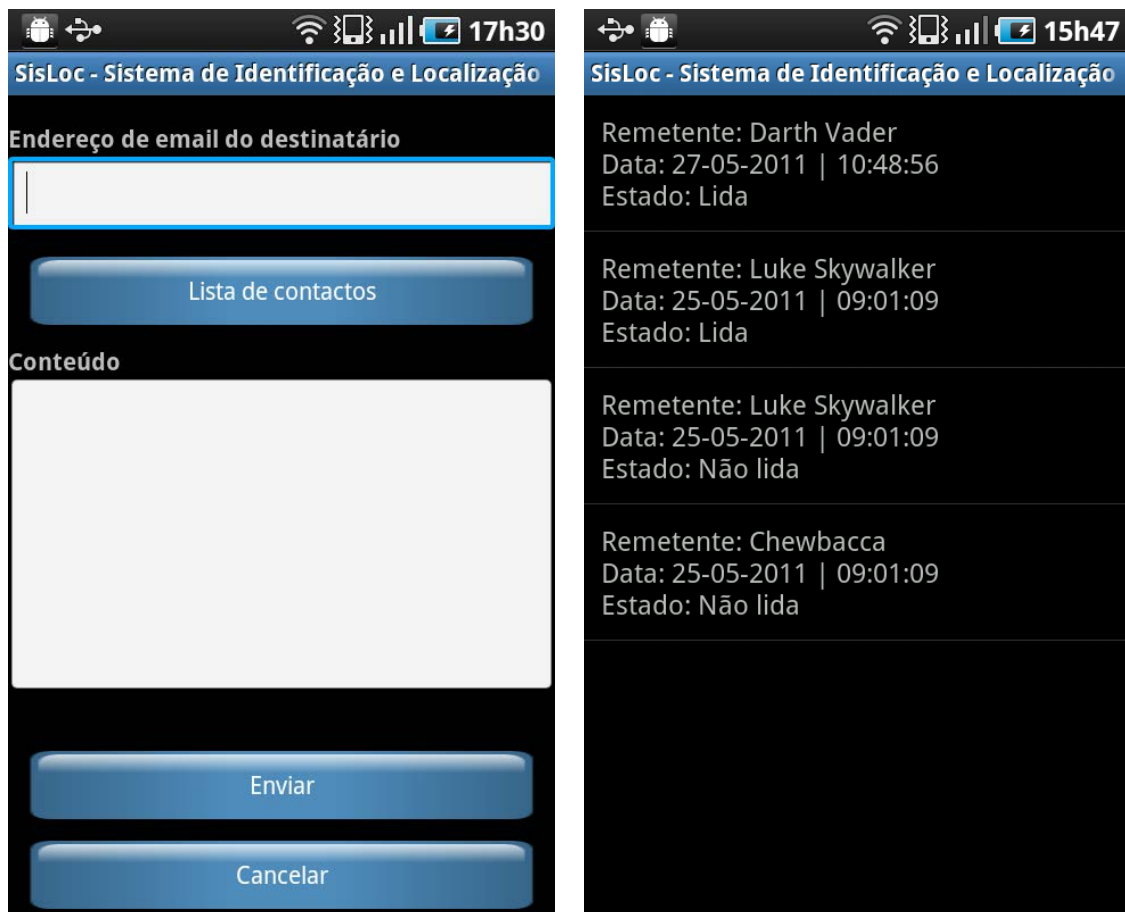


Figura 4.11 - Composição e recepção de mensagens.

a) Ecrã de envio de mensagens. b) Ecrã de mensagens recebidas.

Após efectuar um clique na mensagem pretendida, entra-se na vista de mensagem onde se tem acesso a todos os dados anteriormente referidos, bem como ao conteúdo enviado na mensagem. Nesta vista (figura 4.12 a)) existe um botão de resposta, um botão de resposta rápida e um botão de apagar mensagem.

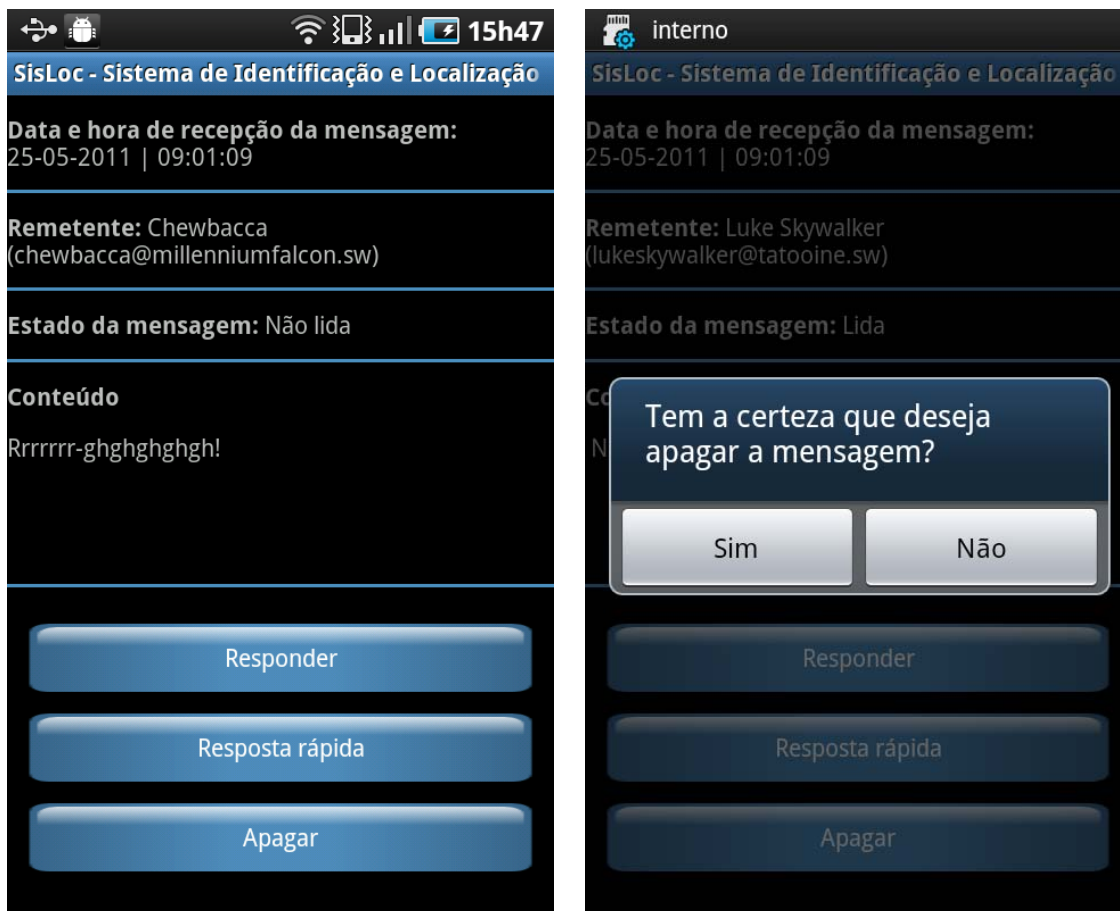


Figura 4.12 - Interacção com mensagens recebidas.

a) Visualização de uma mensagem recebida. b) *Popup* de confirmação de remoção de mensagens.

O botão de resposta permite o envio de uma mensagem personalizada em que o campo de destinatário aparece automaticamente preenchido, de acordo com o remetente da mensagem a quem se quer responder.

O botão de resposta rápida envia uma mensagem automática predefinida para o remetente da mensagem original, sendo este mecanismo útil para casos em que o utilizador não pode redigir uma mensagem (e.g., encontra-se em reunião).

O último botão permite apagar a mensagem e possui um *popup* de confirmação de modo a evitar remoção de mensagens por engano (figura 4.12 b)).

4.3.4 - Aba “Perfil”

Na aba perfil, o utilizador tem a possibilidade de escolher o perfil pretendido e o estado de utilizador, bem como consultar dados tais como o nome do utilizador, o número de telemóvel e o grupo em que está inserido (figura 4.13 a)).

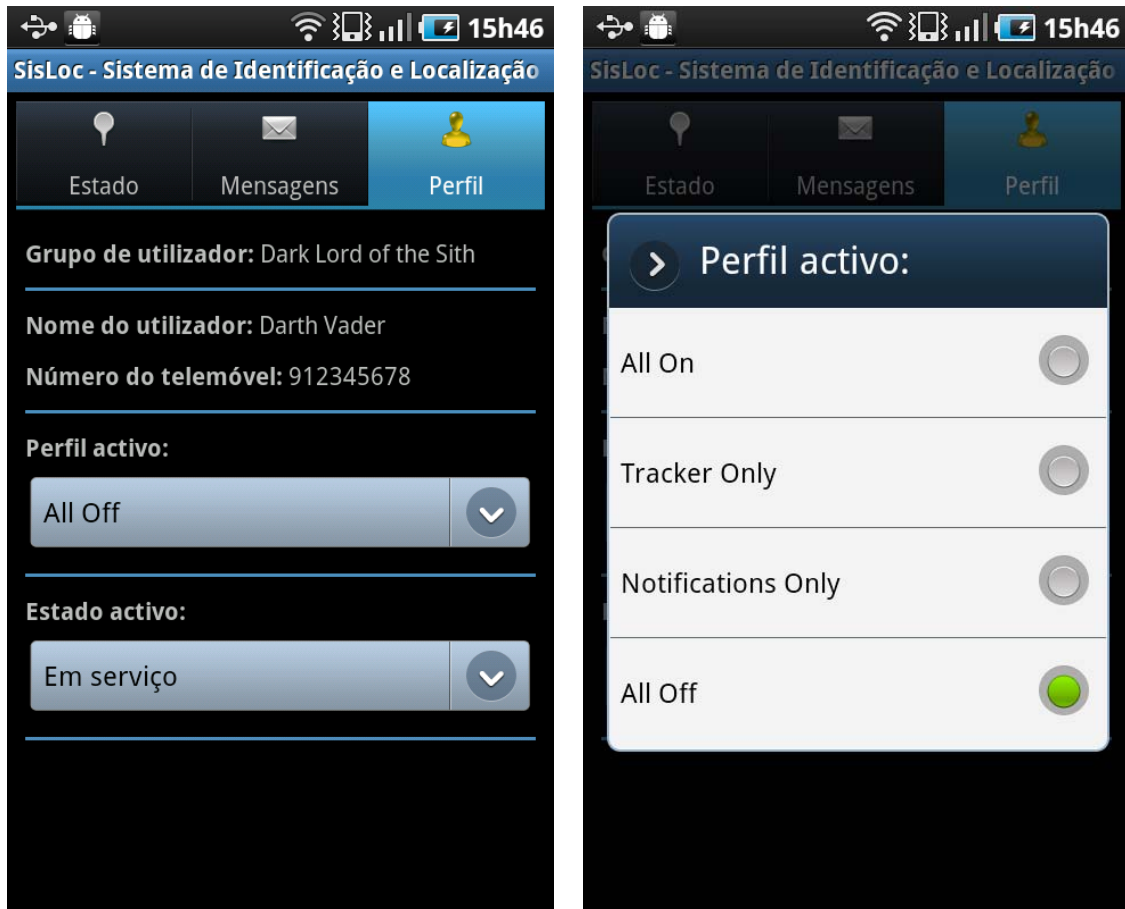


Figura 4.13 - Ecrã de perfil

a) Informação presente no ecrã de perfil. b) Escolha de um perfil predefinido.

No menu *dropdown* dos perfis pode ser escolhido um dos quatro disponíveis (figura 4.13 b)), “All On”, “Tracker Only”, “Notifications Only” e “All Off”. O perfil “All On” activa o serviço de localização (interior e exterior) e o serviço de notificação de mensagens, sendo que o perfil “All Off” faz o inverso. O perfil “Tracker Only” activa o sistema de localização mantendo o de notificação de mensagens desligado e o perfil “Notifications Only”, liga as notificações e desliga o sistema de localização. A descrição dos perfis encontra-se na tabela 4.2.

Tabela 4.2 – Descrição dos perfis predefinidos.

Nome do Perfil	Tracker	Notificações
All On	Activo	Activo
Tracker Only	Activo	Inactivo
Notifications Only	Inactivo	Activo
All Off	Inactivo	Inactivo

Relativamente ao menu *dropdown* dos estados, existem vários estados predefinidos que indicam a disponibilidade do utilizador em determinadas situações (figura 4.14).

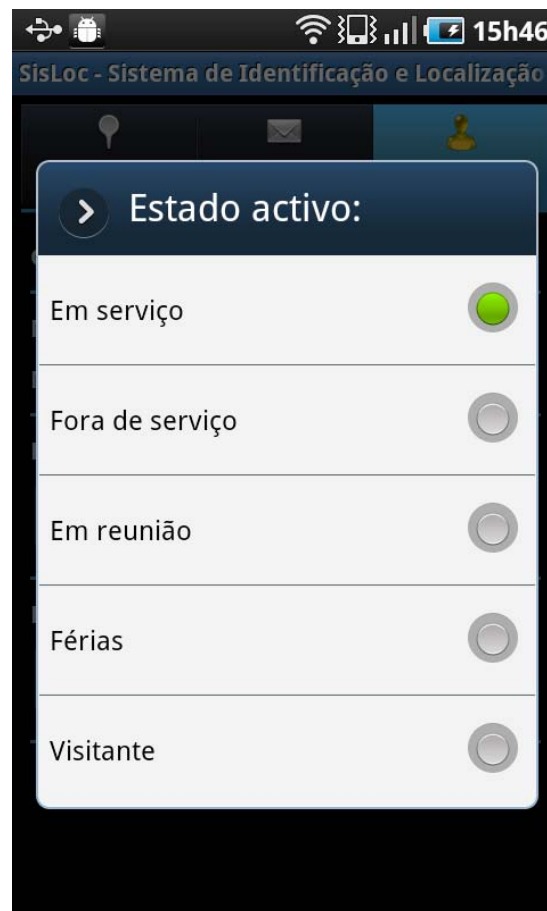


Figura 4.14 - Ecrã de escolha de um estado predefinido.

Desta forma o sistema pode utilizar esta informação para, por exemplo, não enviar notificações se o utilizador se encontrar fora de serviço ou de férias. Neste momento apenas o administrador pode adicionar novos estados ou perfis.

4.3.5 - Serviços da aplicação Android

Para além dos ecrãs e funcionalidades descritos a aplicação contém três serviços a correr em *background*, sendo eles:

- Serviço de *handover* WiFi
- Serviço de *handover* 3G
- Serviço de notificação de mensagens

O serviço de *handover* WiFi é responsável pelo registo na base de dados da localização interior do utilizador, sempre que o mesmo se encontre ligado à rede INESCP-visita. Este serviço foi programado para ocorrer a cada 10 segundos.

O serviço de *handover* 3G regista na base de dados as coordenadas GPS da localização exterior do utilizador, sempre que detecte que o *smartphone* não se encontra ligado à rede *WiFi* INESCP-visita. Este serviço foi programado para ocorrer a cada 60 segundos.

O serviço de notificação de mensagens alerta o utilizador para a existência de mensagens novas através da vibração do *smartphone*, de uma notificação sonora ou de uma notificação visual no topo do ecrã (figura 4.15). Este serviço executa um *polling* à base de dados a cada segundo de modo a verificar a existência ou não de novas mensagens para determinado utilizador.

A periodicidade de execução dos serviços mencionados é configurável tendo sido definida com os valores referidos apenas por motivos de teste. Em “ambientes reais” poderá não haver interesse numa periodicidade tão elevada, sendo aconselhável a sua redução para diminuir o seu peso no consumo de recursos do sistema (processamento, memória e bateria).

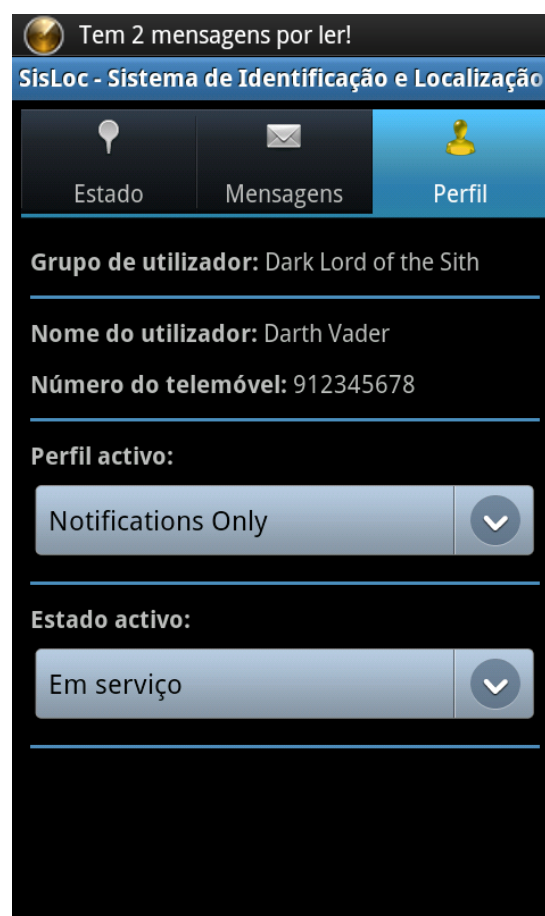


Figura 4.15 - Notificação de mensagens por ler.

Convém ter em atenção que os serviços mencionados só são executados mediante o cumprimento de certas condições. Em primeiro lugar é preciso que o utilizador tenha activo na aplicação Android um perfil que permita executar o serviço desejado (o perfil “All On” executa todos os serviços). Em segundo lugar os serviços de *handover* só podem ser executados pela aplicação, se o utilizador habilitar no sistema operativo Android a utilização de *WiFi* (*handover WiFi*) ou a utilização de 3G e GPS (*handover 3G*). Tal situação prende-se com políticas de segurança do sistema operativo, que não confere à aplicação poderes para

habilitar essas opções. Os serviços de *handover* referidos serão detalhados nas próximas secções.

4.3.6 - Localização interior (Serviço de *handover* WiFi)

Nesta secção é explicado o desenvolvimento da funcionalidade de localização interior. Para implementação desta funcionalidade foi criado um serviço que verifica se existe uma ligação WiFi activa na rede INESCP-visita. Se tal se verificar significa que o utilizador se encontra no edifício do INESC, sendo então dado início ao processo que permitirá registar essa localização. Este serviço será detalhado após a discussão da técnica de localização utilizada.

De acordo com as técnicas de localização discutidas na secção 2.2, optou-se por implementar um mecanismo que combina a técnica NAP (*Nearest Access Point*) com a técnica RSSI (*Received Signal Strength Indication*). Desta forma é possível obter uma maior precisão comparativamente com NAP, sem no entanto trazer para o sistema a complexidade extra introduzida pela aplicação total de RSSI, que obriga à triangulação entre três ou mais pontos de acesso. A figura 4.16 exemplifica o método implementado.

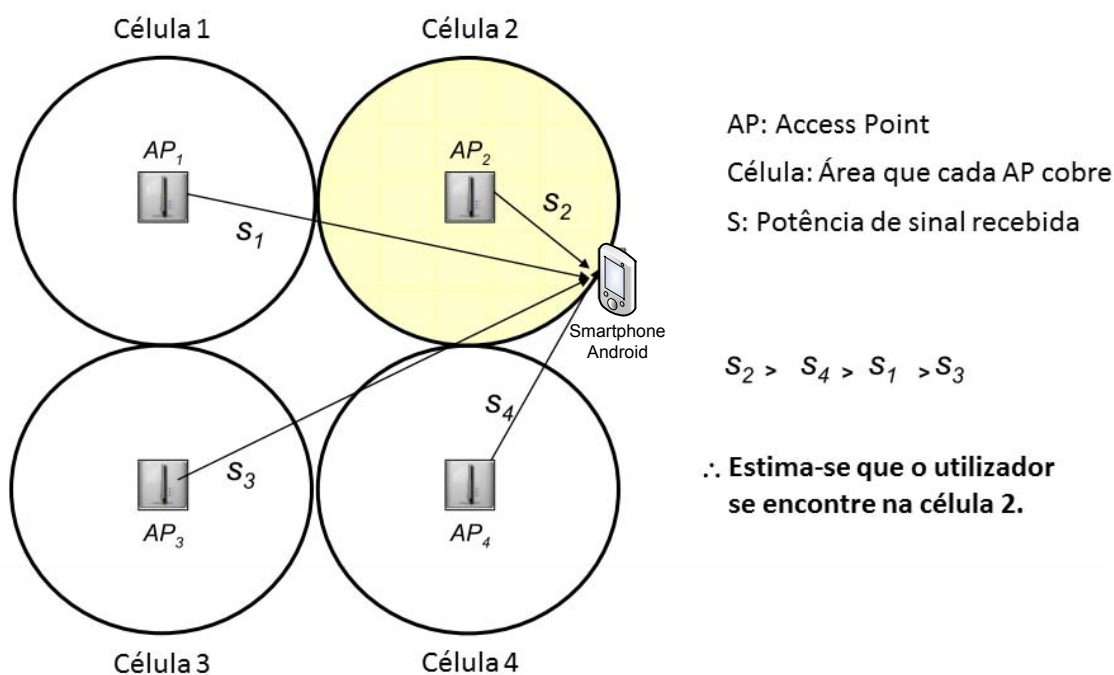


Figura 4.16 - Técnica de localização presente no serviço de *handover* WiFi.

Encontram-se representados na figura quatro pontos de acesso (AP₁ a AP₄), sendo que a cada um desses pontos de acesso está associada uma determinada localização espacial (Célula 1 a Célula 4). O *smartphone* encontra-se num local onde através de um *scan* à rede WiFi detecta os 4 pontos de acesso. Esse *scan* permite analisar a potência de sinal de cada um dos pontos de acesso (S₁ a S₄). Após efectuada a comparação das potências recebidas, o *smartphone* verifica que a potência de sinal do AP₂ é superior às restantes significando que o

utilizador se encontra na Célula 2. Assim sendo o *smartphone* dá instruções para que seja registado como localização interior na base de dados o valor da Célula 2.

Ao nível de programação foi ainda adicionado um mecanismo de optimização que se encontra descrito no fluxograma 4.17.

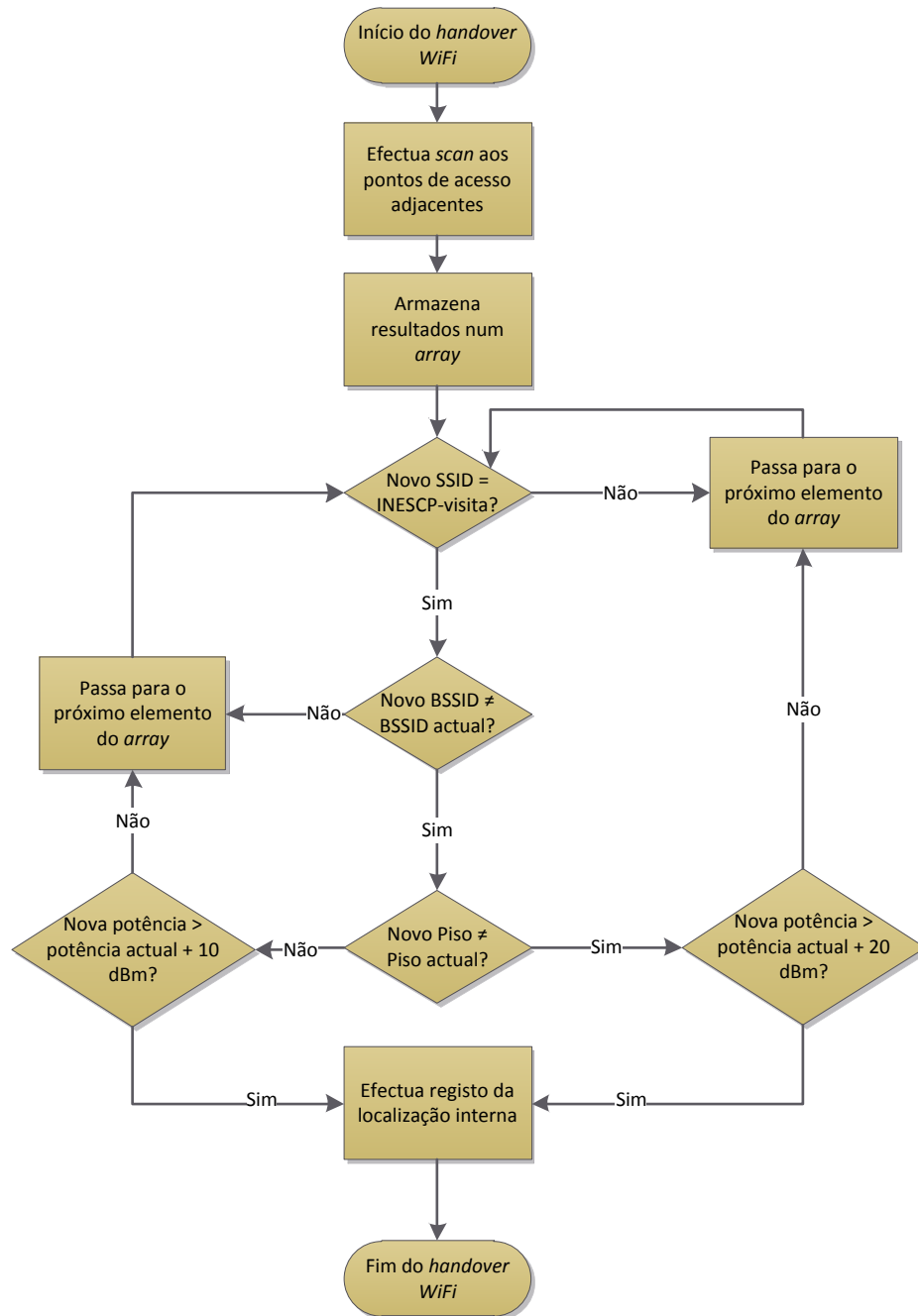


Figura 4.17 - Fluxograma do serviço de *handover* WiFi⁴

⁴ No fluxograma estão presentes dois blocos “Passa para o próximo elemento do array” apenas para não complicar visualmente o esquemático. Na verdade representam um só bloco.

Numa primeira fase o serviço de *handover WiFi* efectua um *scan* de todos os pontos de acesso que conseguir detectar armazenando-os num *array*. Em seguida é feita uma comparação do SSID do primeiro elemento do *array* com o SSID INESCP-visita. Esta comparação é feita pelo motivo de que só é útil efectuar o *handover WiFi* se o utilizador se encontrar na rede mapeada INESCP-visita. Se o resultado dessa comparação for falso, o serviço descarta o elemento actual e vai buscar o próximo elemento armazenado no *array*.

Se o resultado da comparação for verdadeiro, é executada a comparação seguinte que verifica se o BSSID do elemento do *array* é diferente do BSSID do ponto de acesso ao qual o *smartphone* se encontra actualmente ligado. Esta comparação é feita para garantir que se trata de um ponto de acesso diferente do actual, evitando assim a repetição de registos de localização na base de dados. Na eventualidade dessa comparação ser falsa, o serviço retorna ao *array* anterior onde vai buscar o próximo elemento. Se o resultado da comparação for verdadeiro, significa que se trata de um novo ponto de acesso e que portanto existe a possibilidade de o utilizador ter mudado de localização.

Os próximos dois passos estão relacionados com o mecanismo de optimização referido anteriormente. A potência de sinal apesar de ser um bom indicador da distância a que o utilizador se encontra de um AP, é um indicador muito volátil, no sentido em que está sujeito a variações que, mediante o ambiente que rodeia o sistema, podem ser bastante bruscas. Para dotar o sistema de alguma insensibilidade em relação a essas variações, foi acrescentado um filtro para evitar dois tipos de situações: i) situação em que apesar do utilizador se encontrar num determinado piso, a potência do AP do piso imediatamente acima é registada com maior valor e ii) situação em que o utilizador se encontra parado e devido a uma interferência momentânea, um AP do mesmo piso subitamente regista maior potência do que o AP que de facto se encontra mais próximo do utilizador.

No caso i) (e continuando agora a situação descrita pelo fluxograma), o serviço verifica se o piso do novo AP é diferente do actual. Se assim for, é feita uma comparação da potência do AP actual com a do novo AP detectado, à qual se acrescentam 20 dBm⁵. Ao obrigar que a potência do novo AP seja maior que a actual em 20 dBm, protege-se o sistema contra flutuações de potência de sinal que poderiam induzir o mesmo em erro registando uma localização errada. O caso ii) é em tudo semelhante ao i) com excepção que o acréscimo de potência feito à potência do novo AP é de apenas 10 dBm. Este valor é inferior, pois existe uma maior probabilidade de deslocação do utilizador entre APs do mesmo piso do que entre APs de pisos diferentes. Se nenhuma das comparações de potência for verdadeira, volta-se ao *array* e escolhe-se o elemento seguinte. Caso o resultado de uma das comparações seja verdadeira, é assumido que o utilizador mudou de localização e a mesma é registada na base de dados.

Na tabela 4.3 são apresentados exemplos práticos das decisões tomadas para efectuar o registo de localização interior.

⁵ Os valores 20 dBm e 10 dBm foram obtidos por tentativa e erro. Ao utilizá-los o sistema demonstrou precisão e como tal foram mantidos.

Tabela 4.3 – Exemplificação de situações de *handover* WiFi.

Potência do AP actual	Piso do AP actual	Potência do novo AP	Piso do novo AP	Efectua registo de localização?
-75 dBm	4	-70 dBm	4	Não
-75 dBm	4	-70 dBm	3	Não
-75 dBm	4	-60 dBm	4	Sim
-75 dBm	4	-60 dBm	3	Não
-75 dBm	4	-50 dBm	4	Sim
-75 dBm	4	-50 dBm	3	Sim

Os valores de potência e pisos presentes na tabela foram atribuídos aleatoriamente e servem apenas para exemplificação. Tal como referido anteriormente, verifica-se na tabela que o registo de localização só é efectuado quando existe uma diferença de mais de 10 dbm para APs que se encontrem no mesmo piso ou uma diferença de mais 20 dBm para APs de pisos diferentes.

4.3.7 - Localização exterior (Serviço de *handover* 3G)

Nesta secção é explicado o desenvolvimento da funcionalidade de localização exterior. Para implementação desta funcionalidade criou-se um serviço que verifica se existe uma ligação *WiFi* activa na rede INESCP-visita. Se tal não se verificar significa que o utilizador se encontra numa localização exterior ao edificio INESC, sendo então necessário dar início ao processo que permitirá registar essa localização. O fluxograma apresentado na figura 4.18 explica o funcionamento deste serviço.

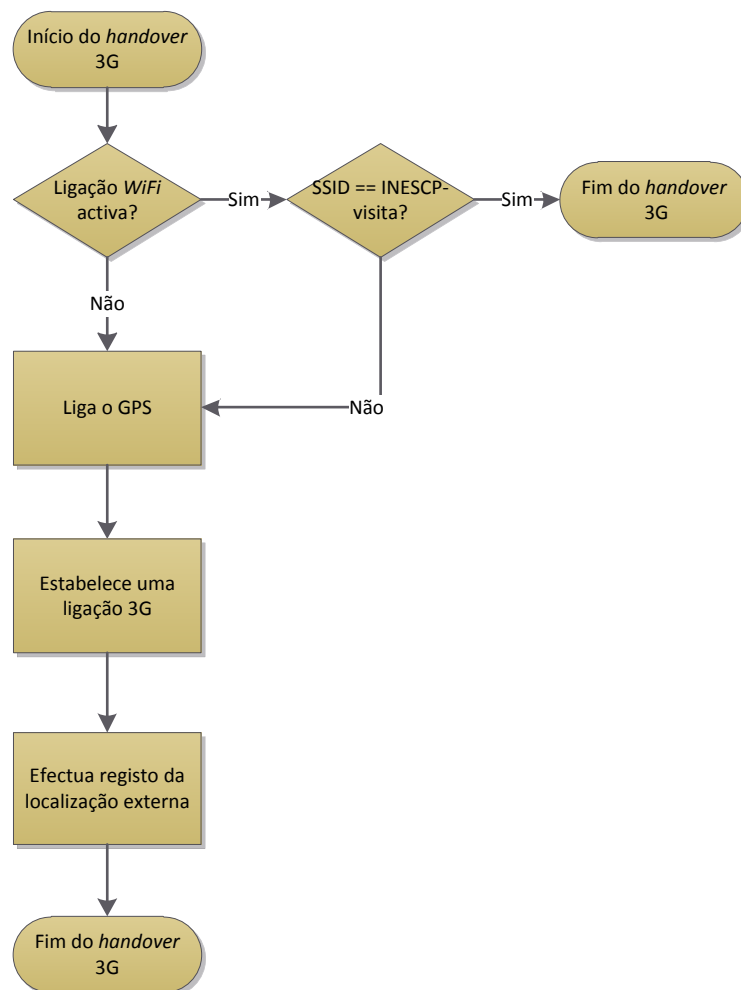


Figura 4.18 - Fluxograma do mecanismo de *handover* 3G.

Inicialmente, o serviço verifica se existe uma ligação *WiFi* activa. Se a mesma existir e o seu SSID for INESCP-visita então o processo de *handover* 3G é imediatamente terminado pois o utilizador encontra-se no interior do edifício do INESC. Caso contrário o utilizador encontra-se numa localização externa, fazendo com que o processo de *handover* continue o seu curso.

Em seguida é activado o GPS e estabelecida uma ligação 3G de modo a que as coordenadas dadas pelo GPS possam ser registadas na base de dados. O GPS encontra-se programado para apresentar coordenadas de 1 em 1 segundo, sendo as mesmas registadas na base de dados.

Este processo de *handover* 3G só termina quando o serviço detectar que o utilizador se encontra ligado à rede *WiFi* INESCP-visita (passando a efectuar localização interior), ou se o utilizador mudar o perfil activo da aplicação desabilitando a localização.

4.3.8 - Proxy INESC Porto

Outra das limitações do sistema operativo Android 2.2 é a sua (fraca) interacção com *proxies*. Neste momento apenas é possível configurar a utilização de *proxy* para o *browser*

Web. Como a rede *WiFi* da instituição se encontra por detrás de um *proxy*, foi necessário arranjar forma de ultrapassar esta limitação do sistema operativo. Numa primeira abordagem tentou-se programar directamente na aplicação a configuração do *proxy*. No entanto devido a políticas da Google, responsável pela criação e gestão do sistema operativo Android, a zona de configuração do *proxy* encontra-se protegida, sendo apenas possível a sua leitura e a única forma de obter permissões de escrita é tendo uma licença especial por parte da Google. Sendo impossível contornar o problema do *proxy* a nível de programação, o próximo passo foi procurar uma aplicação já existente no mercado que permitisse a configuração do *proxy*. Para tal efeito foi utilizada a aplicação “Transparent Proxy” [45] que permitiu sem qualquer tipo de problema a configuração do *proxy* (endereço e porta). Após configuração do *proxy* a localização interior da aplicação SisLoc funcionou sem qualquer tipo de problema na rede *WiFi* do INESC Porto.

Apesar do significativo avanço na resolução do problema da configuração do *proxy* foi descoberto mais tarde um outro. A aplicação “Transparent Proxy” não faz a distinção entre a configuração de *proxies* para a rede *WiFi* ou para a rede de dados 3G, querendo isto dizer que assume que o *proxy* é o mesmo para os dois tipos de ligações. Este facto tem consequências na localização exterior, pois assim que o *smartphone* se encontra no exterior e não detecta a rede *WiFi* da instituição, faz uma tentativa de se ligar à rede 3G, mas como tem configurado como *proxy* da rede 3G o *proxy* da instituição, esta ligação não é bem sucedida. Chegou a ser equacionado programar na aplicação SisLoc uma forma de chamar a aplicação “Transparent Proxy” e alterar o *proxy* conforme fosse utilizada a rede *WiFi* ou a rede 3G, mas tal procedimento era de complexidade elevada e exigiria um dispêndio de tempo considerável pois obrigaria a uma análise profunda do código fonte da aplicação “Transparent Proxy”. Assim sendo, a única forma encontrada para resolver este problema é através da acção do próprio utilizador que, quando se desloca para o exterior da instituição, tem que desactivar o *proxy* na aplicação “Transparent Proxy”.

Capítulo 5

Testes e análise de resultados

Neste capítulo são apresentados os testes de autonomia, precisão e funcionalidade do sistema.

5.1 - Ambiente e condições de teste

Os testes que pretendem aferir a autonomia do sistema foram sempre iniciados com um nível de bateria inicial do *smartphone* de 100%, tentando sempre reduzir ao máximo qualquer outra actividade no *smartphone* que não fosse parte integrante do sistema. Ao nível dos testes de precisão de localização, os de localização interior foram conduzidos no edifício do INESC Porto sendo percorridos os seis pisos mapeados, sendo que os de localização exterior ocorreram no exterior do edifício do INESC Porto, no campus da FEUP e na cantina da FEUP.

5.2 - Autonomia

Nesta secção são apresentados os testes efectuados em vários cenários para testar a autonomia do sistema. De modo a conseguir obter os valores de autonomia foi utilizada a aplicação “Android Battery Dog”, que faz uma monitorização constante do nível da bateria ao longo do tempo, gerando um *log* com os resultados em formato “.csv”. Todos os testes efectuados nesta secção (com excepção do teste da autonomia em *standby*) partem do princípio que o nível de bateria inicial do *smartphone* é de 100%. De notar que a utilização desta aplicação provoca, como seria de esperar, um consumo acrescido de energia no *smartphone*, facto que deverá ser tido em conta aquando da análise dos resultados.

5.2.1 - Autonomia em *standby*

Como o valor da autonomia em *standby* para este *smartphone* é segundo o fabricante de cerca de 576h [46] (aproximadamente 23 dias com ligação 3G activa), não foi feita a medição real deste parâmetro, pois tal medição implicaria ficar com o *smartphone* imobilizado durante esse tempo, o que se mostrou impraticável devido a ser necessário a utilização do *smartphone* para outros testes. Assim sendo e partindo do princípio que a bateria do *smartphone* se encontra em boas condições, será assumido como valor de autonomia em *standby* as 576h indicadas pelo fabricante.

5.2.2 - Autonomia de localização interior

Este teste incidiu apenas na autonomia da localização interior e para tal efeito, colocou-se a aplicação a correr apenas com o *tracker WiFi* activo (GPS, ligação 3G e notificações inactivas), sendo que o *smartphone* andou sempre com um utilizador que esteve o dia inteiro no edifício do INESC Porto e que frequentou os vários pisos do edifício.

Tabela 5.1 – Autonomia de localização interior.

Nível da bateria	Data e hora
100 %	10-06-2011 04:26
0 %	11-06-2011 02:40

A autonomia da aplicação para a localização interior é de 22h14m, isto é, cerca de 1 dia.

5.2.3 - Autonomia de localização exterior

Este teste teve como objectivo testar a autonomia da localização exterior e para tal efeito, colocou-se a aplicação a correr com o *tracker GPS* e a ligação 3G activos (*WiFi* e notificações inactivas). O *smartphone* andou sempre junto a um utilizador que passou o dia fora das instalações do INESC Porto.

Tabela 5.2 – Autonomia de localização exterior.

Nível da bateria	Data e hora
100 %	11-06-2011 09:01
0 %	11-06-2011 18:47

A autonomia da aplicação para a localização exterior é de 9h46m.

5.3 - Precisão de localização

5.3.1 - Localização interior

Para os testes de localização interior, configurou-se um *handover* WiFi de 10 segundos. Quer isto dizer que existe um serviço da aplicação Android a correr em *background* que de 10 em 10 segundos trata de todos os procedimentos necessários para registar a localização interior do utilizador na base de dados. O tempo de *handover* é totalmente configurável tendo sido escolhido um período de 10 segundos para que os testes possam ser realizados de forma mais expedita. Para utilização real, é recomendável o aumento deste tempo de forma a poupar a bateria do *smartphone*, até porque em princípio não haverá interesse em aferir a localização de utilizadores em tão curtos espaços de tempo. Todos os testes começaram no ponto de acesso C.4 (piso -1) e acabaram no mesmo sítio, sendo as medições feitas com o utilizador a passar na proximidade dos pontos de acesso, com excepção dos APs Recepção e 4.26, onde tal não é possível. Para apresentação dos resultados foram tirados *screenshots* aos registos apresentadas pela aplicação “phpPgAdmin”. Nesses *screenshots* são apresentados os parâmetros da base de dados “nome” (nome do utilizador autenticado na aplicação), “imei” (identificador do *smartphone*), “nome_sala”, “nome_piso” e “nome_edifício” (local onde se encontra o utilizador) e “data_hora” (data e hora a que foi registada a ocorrência).

5.3.1.1 - Teste 1: Teste genérico

Este primeiro teste efectuou-se percorrendo todos os pontos de acesso mapeados no edifício do INESC Porto, começando na sala C.4 do piso -1 e indo até ao piso 4 utilizando as escadas. No final apanhou-se o elevador no piso 4 e voltou-se à sala C.4 no piso -1. Este teste realizou-se com o utilizador a passar na proximidade dos pontos de acesso (tão próximo quanto possível), permanecendo em cada um deles no mínimo 20 segundos, de modo a garantir que o serviço de *handover* tivesse tempo de ser executado. O percurso completo teve a seguinte ordem: C.4->C.8->Recepção->1.28->1.9->1.13->2.19->3.13->3.11->3.28->4.26->4.20->C.4. Convém referir que a lógica da numeração “a.b” é a seguinte: “a” representa o número do piso no edifício (“C” é de cave e significa o piso -1) e “b” é o número da sala. O resultado obtido encontra-se representado na figura 5.1.

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-05-25 16:38:14.388
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-05-25 16:38:47.465
Darth Vader	354795043100525	Recepção	0	INESCPorto Sede	2011-05-25 16:39:43.253
Darth Vader	354795043100525	1.28	1	INESCPorto Sede	2011-05-25 16:41:11.202
Darth Vader	354795043100525	1.9	1	INESCPorto Sede	2011-05-25 16:42:09.404
Darth Vader	354795043100525	1.13	1	INESCPorto Sede	2011-05-25 16:43:06.009
Darth Vader	354795043100525	2.19	2	INESCPorto Sede	2011-05-25 16:45:34.635
Darth Vader	354795043100525	3.13	3	INESCPorto Sede	2011-05-25 16:47:03.677
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 16:47:54.63
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-05-25 16:48:43.899
Darth Vader	354795043100525	4.20	4	INESCPorto Sede	2011-05-25 16:51:16.57
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-05-25 16:52:47.711
Darth Vader	354795043100525	Recepção	0	INESCPorto Sede	2011-05-25 16:59:44.749
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-05-25 17:47:06.528
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-05-25 17:47:34.335

Figura 5.1 - Screenshot dos resultados obtidos para o teste 1.

Através da figura 5.1 obtida na base de dados, verifica-se que o percurso teve início às 16h:38m e que terminou às 16h:52m. Todos os pontos de acessos percorridos foram registados com sucesso com excepção do AP da sala 4.26. A explicação reside no facto deste ponto de acesso se encontrar numa sala de reuniões onde por norma não é possível a entrada, o que provoca que não seja possível passar imediatamente ao lado do ponto de acesso (tal como referido na secção 5.3.1). No lado exterior da sala o *smartphone* captava o sinal do ponto de acesso existente; no entanto, como a potência do sinal era inferior à do ponto de acesso 4.20, não existiu handover, e o registo de localização permaneceu no ponto de acesso 4.20.

Na mesma situação que o ponto de acesso da sala 4.26 encontra-se o da Recepção. No entanto, este foi detectado correctamente, pois no piso 0 apenas existe esse ponto de acesso; logo, por omissão, e a não ser que os pontos de acesso de pisos adjacentes tenham uma potência superior anormal, o *smartphone* terá sempre que se ligar ao ponto da Recepção.

De notar ainda a presença das últimas três entradas, que dizem respeito a uma saída do utilizador, que se ausentou do edifício às 16h:59m (Recepção), tendo regressado à sala aonde se encontrava (C.4) às 17h:47m.

5.3.1.2 - Teste 2: Teste com utilizador em movimento constante

Este teste realizou-se com o utilizador a percorrer todos os pontos de acesso do edifício (tal como no teste nº1), mas agora sem nunca parar. O objectivo é aferir qual a capacidade do sistema de responder a variações bruscas de posição. Tal como no teste anterior, o serviço de *handover WiFi* encontrava-se a funcionar de 10 em 10 segundos. Foram efectuados três testes:

Resultado nº 1 - Início às 08h:53m

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-06-07 08:53:46.145
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-06-07 08:54:45.728
Darth Vader	354795043100525	1.13	1	INESCPorto Sede	2011-06-07 08:56:46.394
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-06-07 08:57:47.565
Darth Vader	354795043100525	4.26	4	INESCPorto Sede	2011-06-07 08:59:09.85
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-06-07 09:00:38.539

Figura 5.2 - Screenshot do resultado nº1 obtido para o teste 2.

Resultado nº 2 - Início às 09h:05m

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-06-07 09:05:46.33
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-06-07 09:06:36.368
Darth Vader	354795043100525	1.28	1	INESCPorto Sede	2011-06-07 09:07:28.937
Darth Vader	354795043100525	1.13	1	INESCPorto Sede	2011-06-07 09:08:29.877
Darth Vader	354795043100525	2.19	2	INESCPorto Sede	2011-06-07 09:09:29.264
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-06-07 09:11:13.64
Darth Vader	354795043100525	4.20	4	INESCPorto Sede	2011-06-07 09:12:15.996
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-06-07 09:13:26.209

Figura 5.3 - Screenshot do resultado nº2 obtido para o teste 2.

Resultado nº 3 - Início às 09h:44m

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-06-07 09:44:36.02
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-06-07 09:45:15.1
Darth Vader	354795043100525	1.28	1	INESCPorto Sede	2011-06-07 09:46:27.864
Darth Vader	354795043100525	1.13	1	INESCPorto Sede	2011-06-07 09:47:15.386
Darth Vader	354795043100525	2.19	2	INESCPorto Sede	2011-06-07 09:48:31.992
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-06-07 09:49:16.493
Darth Vader	354795043100525	4.26	4	INESCPorto Sede	2011-06-07 09:51:07.094
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-06-07 09:51:55.112

Figura 5.4 - Screenshot do resultado nº3 obtido para o teste 2.

Em nenhum dos três resultados apresentados foram detectados todos os pontos de acesso, sendo que os da Recepção, sala 1.9 e sala 3.13 nunca chegaram sequer a ser detectados. Assim verifica-se que o sistema é sensível a variações de posição bruscas, não sendo capaz de detectar os pontos de acesso na totalidade. No entanto, e considerando as aplicações pretendidas para esta implementação, onde é suposto os utilizadores permanecerem durante um período mínimo no mesmo local, os resultados obtidos são satisfatórios.

Por curiosidade, efectuou-se um teste com *handover* de 1 em 1 segundo, pois em teoria seriam detectados mais pontos de acesso devido à aplicação procurar com maior frequência um ponto de acesso com potência superior.

Resultado

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-06-09 10:04:20.546
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-06-09 10:04:58.887
Darth Vader	354795043100525	2.19	2	INESCPorto Sede	2011-06-09 10:07:37.524
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-06-09 10:08:34.433
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-06-09 10:09:16.649
Darth Vader	354795043100525	4.20	4	INESCPorto Sede	2011-06-09 10:10:01.768
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-06-09 10:11:02.409

Figura 5.5 - Screenshot do resultado com *handover* de 1 segundo obtido para o teste 2.

No entanto, observa-se que tal não aconteceu. A explicação para tal situação poderá dever-se ao facto de o *scan* que procura APs nas imediações demorar mais de 1 segundo a ser executado. Um outro factor a ter em conta é a perda de conectividade entre mudanças de piso. Nos testes anteriores esse factor não foi relevante devido ao utilizador esperar debaixo dos APs cerca de 20 segundos, o que garantia tempo suficiente para a ligação ser restabelecida, o que nesta situação não acontece. Assim sendo, conclui-se que não é possível ter o serviço de *handover WiFi* a funcionar com uma periodicidade tão baixa.

Para os testes que se seguem voltou-se a adoptar a situação inicial em que o utilizador espera junto a um AP pelo menos 20 segundos de forma a garantir que o serviço de *handover WiFi* tem tempo de actuar.

5.3.1.3 - Teste 3: “Caso especial” Piso -1

No piso -1 encontram-se mapeados apenas dois pontos de acesso. No entanto, este piso tem uma particularidade que mais nenhum tem, pois é o único piso com uma zona *WiFi* “cega” (sem conectividade *WiFi*) entre pontos de acesso. Na figura 5.6 encontram-se representados os dois pontos de acesso neste piso, estando um na sala C.4 (cor amarela) e outro na sala C.8 (cor verde). Os raios de cobertura destes pontos de acesso encontram-se representados por figuras circulares da cor de cada ponto de acesso respectivo. A zona cega (de interesse para o percurso) está representada por linhas diagonais pretas. Neste teste (e nos que se seguem) voltou-se à situação inicial em que o utilizador permaneceu em cada ponto de acesso durante pelo menos 20 segundos, de forma a garantir que o serviço de *handover WiFi* tivesse tempo de ser iniciado.

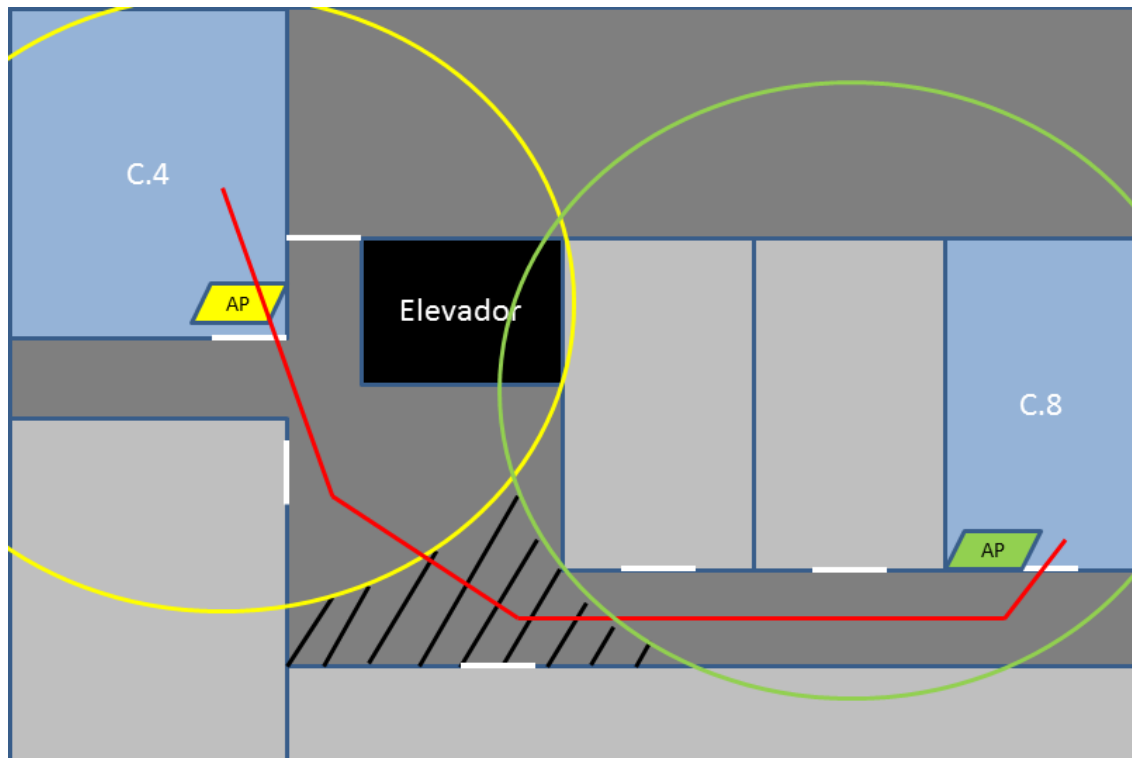


Figura 5.6 - Mapa do piso -1.

Este teste teve como objectivo verificar se apesar da perda momentânea de conectividade, o sistema era capaz de detectar correctamente os pontos de acesso no percurso (representado a vermelho na figura) foi o seguinte: C.4->C.8->C.4->C.8->C.4.

Resultado nº 1 - Início às 09h:09m

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-05-24 09:09:44.424
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-05-24 09:10:33.582
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-05-24 09:11:15.461
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-05-24 09:11:54.705
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-05-24 09:12:41.555

Figura 5.7 - Screenshot do resultado nº1 obtido para o teste 3.

Por observação da tabela verifica-se que o utilizador “Darth Vader” possuidor do *smartphone* com o IMEI indicado, fez o percurso predefinido com uma precisão de 100% no período temporal acima apresentado.

Resultado nº 2 - início às 13h:33m

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-05-25 13:33:32.128
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-05-25 13:34:12.247
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-05-25 13:34:41.796
Darth Vader	354795043100525	C.8	-1	INESCPorto Sede	2011-05-25 13:35:11.919
Darth Vader	354795043100525	C.4	-1	INESCPorto Sede	2011-05-25 13:35:41.966

Figura 5.8 - Screenshot do resultado nº2 obtido para o teste 3.

A tabela acima confirma os resultados obtidos anteriormente comprovando o bom funcionamento do sistema.

5.3.1.4 - Teste 4: “Caso especial” Piso 3

O piso 3 do edifício do INESC Porto é outro “caso especial”, pois nele se encontra a Unidade de Telecomunicações e Multimédia, que faz um uso abundante das ligações sem fios, seja através do uso de portáteis e periféricos sem fios, seja através do uso de *routers* sem fios para desenvolvimentos e testes em vários projectos. Para além disso, tem a particularidade de ser o único piso que contém três pontos de acesso divididos por três canais diferentes. Outra situação especial que faz sentido referir sobre este caso tem a ver com o período horário, pois de manhã cedo existem muito menos dispositivos sem fios ligados o que reduz significativamente a interferência sentida. Como tal, e devido à forte interferência existente neste piso, é importante aferir a precisão do sistema nestas condições. Neste teste foi feito o seguinte percurso: 3.28->3.11->3.13->3.11->3.28->3.11.

Resultado nº 1 - início às 09h:12m

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-05-25 09:12:36.677
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 09:12:57.342
Darth Vader	354795043100525	3.13	3	INESCPorto Sede	2011-05-25 09:14:37.854
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 09:15:07.507
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-05-25 09:16:07.629
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 09:16:37.754

Figura 5.9 - Screenshot do resultado nº1 obtido para o teste 4.

O trajecto a efectuar pressupunha a existência de seis linhas na figura 5.9, o que se veio a verificar. O percurso teve início na sala 3.28, passando de seguida pelas salas 3.11 e 3.13, algo que a base de dados registou sem problemas. O próximo passo foi voltar às salas 3.11 e 3.28, terminando o percurso onde foi iniciado na sala 3.28. Todas estas passagens foram registadas com sucesso. No entanto convém referir que esta medição foi feita durante

o período matinal menos movimentado (entre as 8 e as 10h), o que significa que a interferência electromagnética provocada no sinal *WiFi* era relativamente reduzida.

Resultado nº 2 - início às 13h:41m

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-05-25 13:41:10.298
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 13:42:00.882
Darth Vader	354795043100525	3.13	3	INESCPorto Sede	2011-05-25 13:43:21.474
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 13:44:30.001
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-05-25 13:45:11.74
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 13:45:52.711

Figura 5.10 - Screenshot do resultado nº2 obtido para o teste 4.

O segundo resultado obtido fazendo o mesmo percurso num horário mais tardio confirma os resultados obtidos anteriormente. Também neste caso a quantidade de elementos capazes de introduzir ruído na recepção do sinal *WiFi* era reduzida, pois ocorreu durante o período de almoço. Em seguida foi um teste durante a chamada “hora de ponta” de modo a testar a sensibilidade do sistema a ruído externo.

Resultado nº 3 - Início às 15h56m

nome	imei	nome_sala	nome_piso	nome_edificio	data_hora
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-05-25 15:56:23.321
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 15:57:25.139
Darth Vader	354795043100525	3.13	3	INESCPorto Sede	2011-05-25 15:58:33.486
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 15:59:53.478
Darth Vader	354795043100525	3.28	3	INESCPorto Sede	2011-05-25 16:00:33.595
Darth Vader	354795043100525	3.11	3	INESCPorto Sede	2011-05-25 16:01:45.488

Figura 5.11 - Screenshot do resultado nº3 obtido para o teste 4.

Os últimos resultados foram obtidos numa altura em que o piso se encontrava cheio, logo as potenciais interferências no sistema seriam mais prováveis. No entanto, através da figura 5.11, verifica-se que os resultados obtidos são exactamente os mesmos que os obtidos nos dois testes anteriores. Pode-se então afirmar que neste conjunto de testes o sistema teve uma precisão de 100%.

5.3.2 - Localização exterior

O teste que se segue tem por objectivo verificar a precisão do sistema ao nível da localização exterior. O serviço *handover* 3G foi programado para ocorrer de 60 em 60 segundos, verificando durante esse período se existe uma ligação *WiFi* válida que possa utilizar para mapeamento. Caso essa ligação não exista, é activado o GPS e estabelecida uma ligação 3G para registar a localização exterior na base de dados. A partir do momento em que a localização exterior estiver activa, e sempre que o GPS devolver uma posição válida, a

mesma é registada na base de dados. Como o utilizador durante a grande maioria do percurso estará em movimento, é esperado que sejam introduzidos novos valores na base de dados de segundo em segundo pois é o ritmo a que o GPS, por predefinição, verifica se existiu mudança de posição. Convém referir que esta periodicidade do GPS, apesar de oferecer maior precisão, torna-se dispendiosa a nível de recursos (bateria, quantidade de dados trocados via 3G, processamento no *smartphone* e servidor). No futuro para reduzir o consumo de recursos, poderá considerar-se baixar a periodicidade a que o GPS verifica a existência de uma nova posição.

5.3.2.1 - Teste: Percurso INESC Porto - Cantina FEUP

Neste teste foi efectuado o percurso desde a entrada do edifício do INESC Porto até à cantina da FEUP. Para um melhor entendimento, o percurso está reproduzido na figura 5.12. O percurso teve início no ponto A (INESC Porto) e fim no ponto B (Cantina FEUP). O caminho intermédio está assinalado através de uma linha amarela que liga os dois pontos.



Figura 5.12 - Figura demonstrativa do percurso efectuado (a amarelo).

Na tabela 5.3 encontram-se as coordenadas obtidas para os dois pontos. As coordenadas reais são obtidas utilizando a aplicação “Google Maps” e as coordenadas aplicação foram as que a aplicação obteve e registou na base de dados. Observando os valores para os pontos A e B verifica-se que existem discrepâncias entre os dois tipos de valores registados.

Tabela 5.3 – Comparação das coordenadas reais com as registadas.

	Latitude	Longitude
Coordenadas reais		
Ponto A	41.179361	-8.595434
Ponto B	41.176336	-8.595192
Coordenadas aplicação		
Ponto A'	41.17958056000255	-8.595267922278708
Ponto B'	41.17608054884035	-8.595452749116523

A figura 5.13 mostra no mapa o desfaseamento observado na tabela 5.3, sendo que se encontram marcados com fundo verde e as letras A e B as coordenadas reais e com as setas e letras A' e B' as coordenadas registadas pela aplicação.



Figura 5.13 - Marcação dos pontos iniciais e finais registados pela aplicação (A' e B').

No total durante este percurso foram registadas 221 entradas na base de dados, estando de seguida representadas na figura 5.14 as entradas mais susceptíveis de análise.

Nestes *screenshots* estão presentes os parâmetros de base de dados “id_externa” (*serial* que indica qual o número do registo da localização), “nome” (nome do utilizador autenticado na aplicação), “imei” (identificador do *smartphone*), “latitude”, “longitude” e “data_hora” (data e hora a que foi efectuado o registo na aplicação).

id_externa	nome	imei	latitude	longitude	data_hora
2	Darth Vader	354795043100525	41.17958056000255	-8.595267922278708	2011-05-24 11:58:17.345
40	Darth Vader	354795043100525	41.178998973972156	-8.594981726210916	2011-05-24 11:59:17.443
88	Darth Vader	354795043100525	41.17852416037243	-8.594961953153708	2011-05-24 12:00:40.93
89	Darth Vader	354795043100525	41.178488209401955	-8.595577770648324	2011-05-24 12:02:43.196
89	Darth Vader	354795043100525	41.178488209401955	-8.595577770648324	2011-05-24 12:02:47.696
112	Darth Vader	354795043100525	41.17766303400574	-8.59452806045975	2011-05-24 12:03:47.196
161	Darth Vader	354795043100525	41.17734491110833	-8.594413435556538	2011-05-24 12:04:47.183
177	Darth Vader	354795043100525	41.17717149610512	-8.594438364937377	2011-05-24 12:05:08.273
179	Darth Vader	354795043100525	41.176515854037916	-8.594906970878176	2011-05-24 12:06:04.276
179	Darth Vader	354795043100525	41.176515854037916	-8.594906970878176	2011-05-24 12:06:05.805
179	Darth Vader	354795043100525	41.176515854037916	-8.594906970878176	2011-05-24 12:06:07.126
179	Darth Vader	354795043100525	41.176515854037916	-8.594906970878176	2011-05-24 12:06:08.457
179	Darth Vader	354795043100525	41.176515854037916	-8.594906970878176	2011-05-24 12:06:09.976
179	Darth Vader	354795043100525	41.176515854037916	-8.594906970878176	2011-05-24 12:06:11.344
222	Darth Vader	354795043100525	41.17608054884035	-8.595452749116523	2011-05-24 12:07:07.824

Figura 5.14 - Screenshot do resultado obtido para a localização exterior.

A primeira entrada (id_externa=2)⁶ corresponde ao ponto A' e ocorreu sensivelmente às 11h:58m. A última entrada (id_externa=222) corresponde ao ponto B' e ocorreu aproximadamente às 12h:07m. Daqui é possível inferir que o trajecto percorrido demorou cerca de 9 minutos a ser completado. Uma das particularidades observadas dá-se quando o id_externa passa de 88 para 89; aí verifica-se que existe um intervalo de cerca de 2 minutos sem que sejam registados quaisquer novas entradas. Esta particularidade ocorreu porque durante esse período o percurso teve lugar dentro de um edifício da faculdade que bloqueou o sinal GPS, logo não foi registado na base de dados qualquer entrada durante esse período. De notar que a id_externa 179 é repetida cinco vezes e isso acontece porque o utilizador parou no mesmo sítio durante cerca de 6 segundos. A figura ilustra a representação gráfica dos pontos da tabela anterior. Os pontos iniciais e finais são A' e B' que correspondem respectivamente a id_externa 2 e 222. Os outros pontos estão marcados na figura de acordo com o seu número de id_externa.

⁶ A variável “id_externa” encontra-se com o valor 2 porque o valor 1 estava reservado para efeitos de teste.



Figura 5.15 - Marcação dos pontos chave medidos ao longo do percurso.

Observando a imagem verifica-se que os pontos com “id_externa” 40, 88, 112, 161, 177 e 179 foram mapeados de forma correcta. Os únicos pontos que falharam em termos de precisão são A', B' e o ponto 89. No caso do ponto 89 é fácil de explicar, pois teve a ver com a entrada num edifício, o que adulterou a posição registada (problema conhecido dos sistemas GPS). No caso dos pontos inicial e final ambos apresentam um erro de precisão elevado que poderá ter a ver com a proximidade a edifícios de dimensão considerável e que provocam interferências que introduzem erros no sinal recebido.

5.4 - Envio, recepção e outras funcionalidades de mensagens

Este teste consiste na verificação da capacidade do sistema em enviar e receber mensagens. Para tal será necessário simular dois utilizadores a usufruir do sistema em simultâneo. Assim sendo, foi utilizado o *smartphone* em que fez autenticação o utilizador “Darth Vader” e foi configurado o emulador Android num portátil em que fez autenticação o utilizador “Luke Skywalker”. Os resultados são demonstrados com *screenshots* da aplicação Android no *smartphone* e emulador e ainda *screenshots* do que se passou na base de dados.

5.4.1 - Envio e recepção de mensagens

Neste teste o utilizador “Darth Vader” enviará uma mensagem ao utilizador “Luke Skywalker” com o conteúdo “Luke I am your father!”.

Através da figura 5.16 verifica-se no *screenshot* do *smartphone* (elipse vermelha) que o utilizador “Darth Vader” enviou a mensagem, no *screenshot* do emulador (elipse amarela) o utilizador “Luke Skywalker” recebeu a mensagem (podendo depois decidir se quer responder ou apagar).

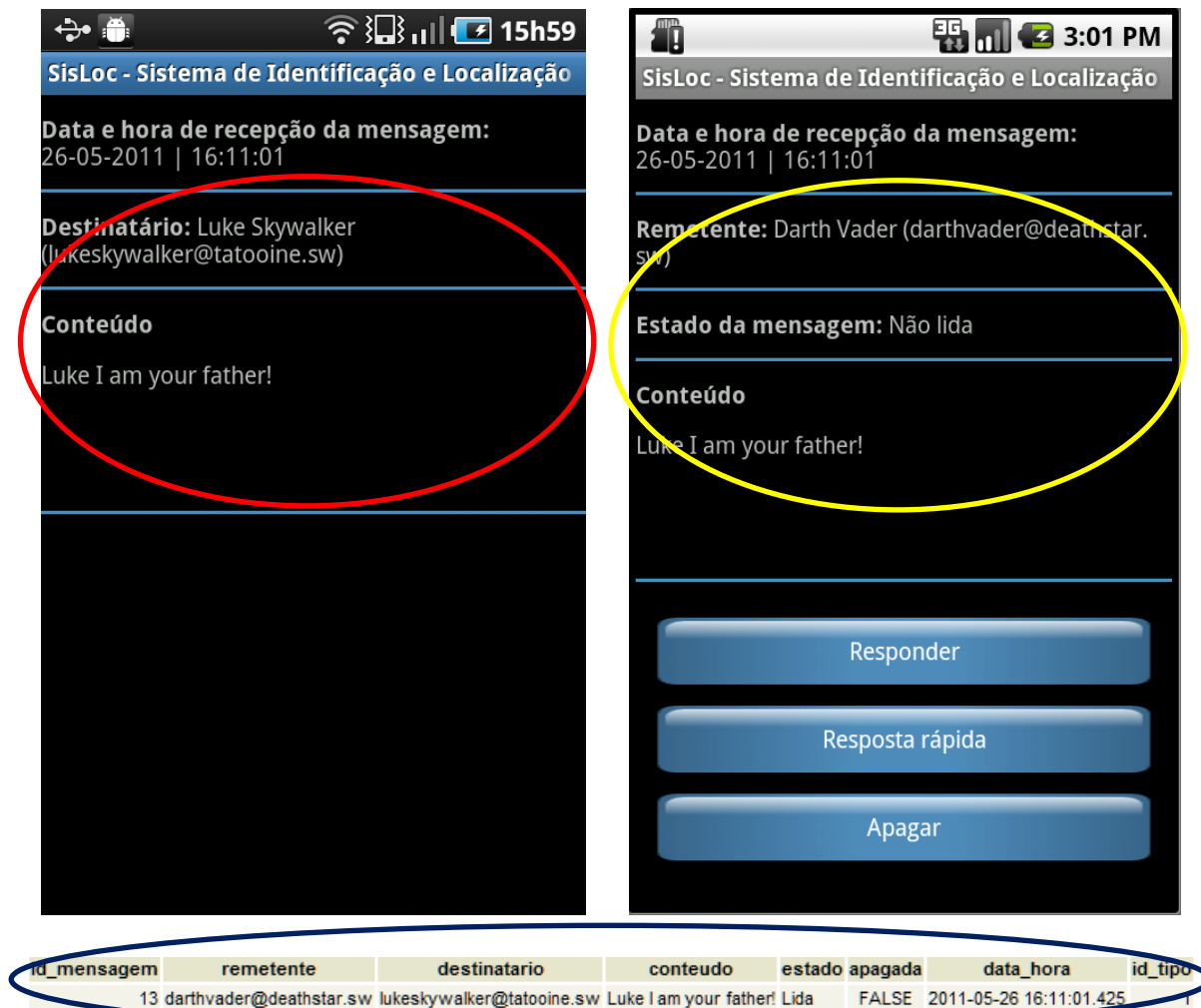


Figura 5.16 - Vista da mensagem enviada por Darth Vader e recebida por Luke Skywalker.

O registo destas mensagens pode ser consultado no *screenshot* da base de dados (elipse azul), onde se demonstra quem foi o remetente e o destinatário da mensagem, qual o conteúdo, o estado da mensagem e a data e hora de envio.

5.4.2 - Notificações de recepção de mensagens

Sempre que o perfil activo for “Notifications Only” ou “All On”, o utilizador é alertado para a chegada de novas mensagens através de uma mensagem que aparece na barra de estado (elipse vermelha) do *smartphone* e, se activos, através de vibração ou toque sonoro.

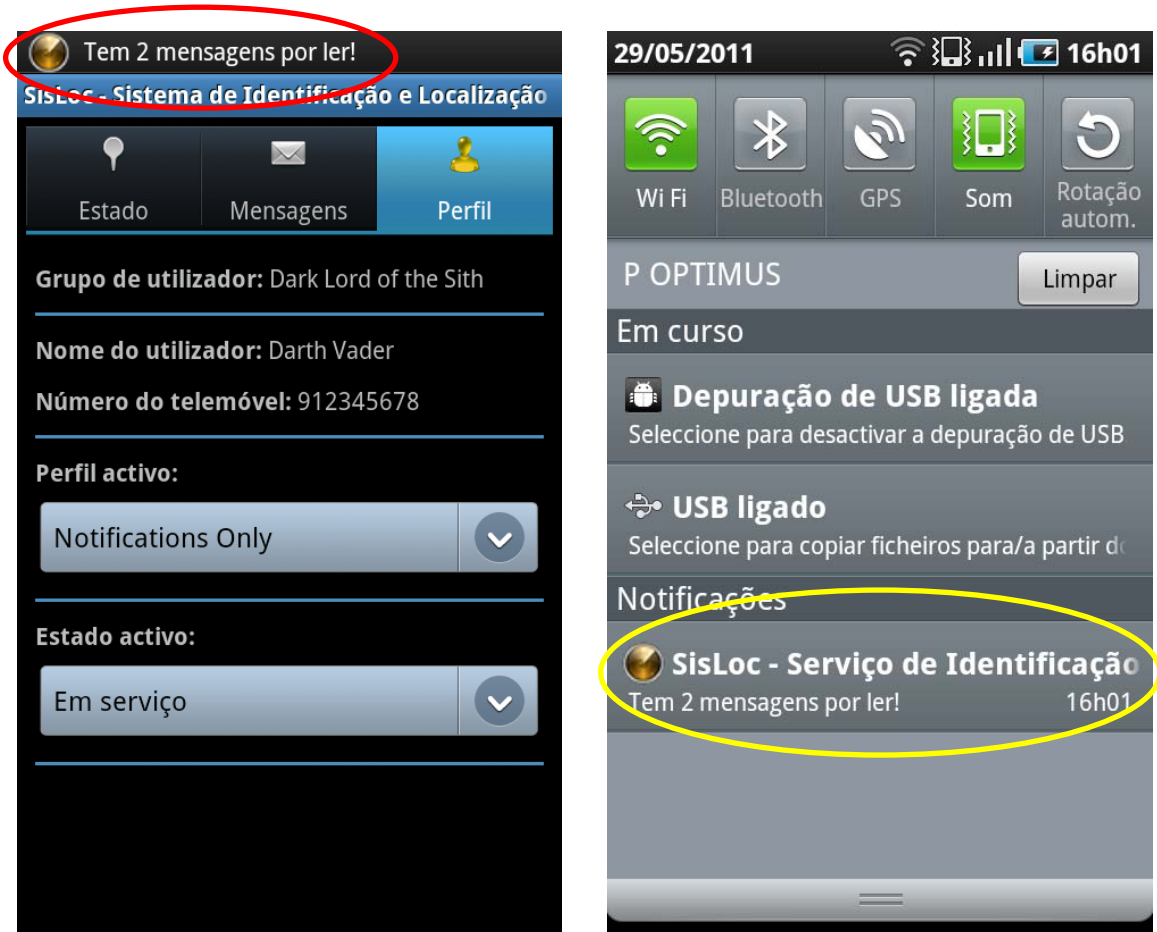


Figura 5.17 - Notificação de mensagens.

Caso o utilizador não se aperceba da notificação inicialmente, um ícone do programa aparecerá na barra de estado e quando o utilizador carrega nele é apresentada a informação relevante que neste caso seria o número de mensagens por ler, e a hora a que a notificação foi lançada (elipse amarela).

5.4.3 - Resposta e “resposta rápida” a mensagens

Após recepção de uma mensagem o utilizador pode optar por responder ao destinatário. Na vista da mensagem recebida existem dois botões: i) “Responder” e ii) “Resposta rápida” (figura 5.18 a)).

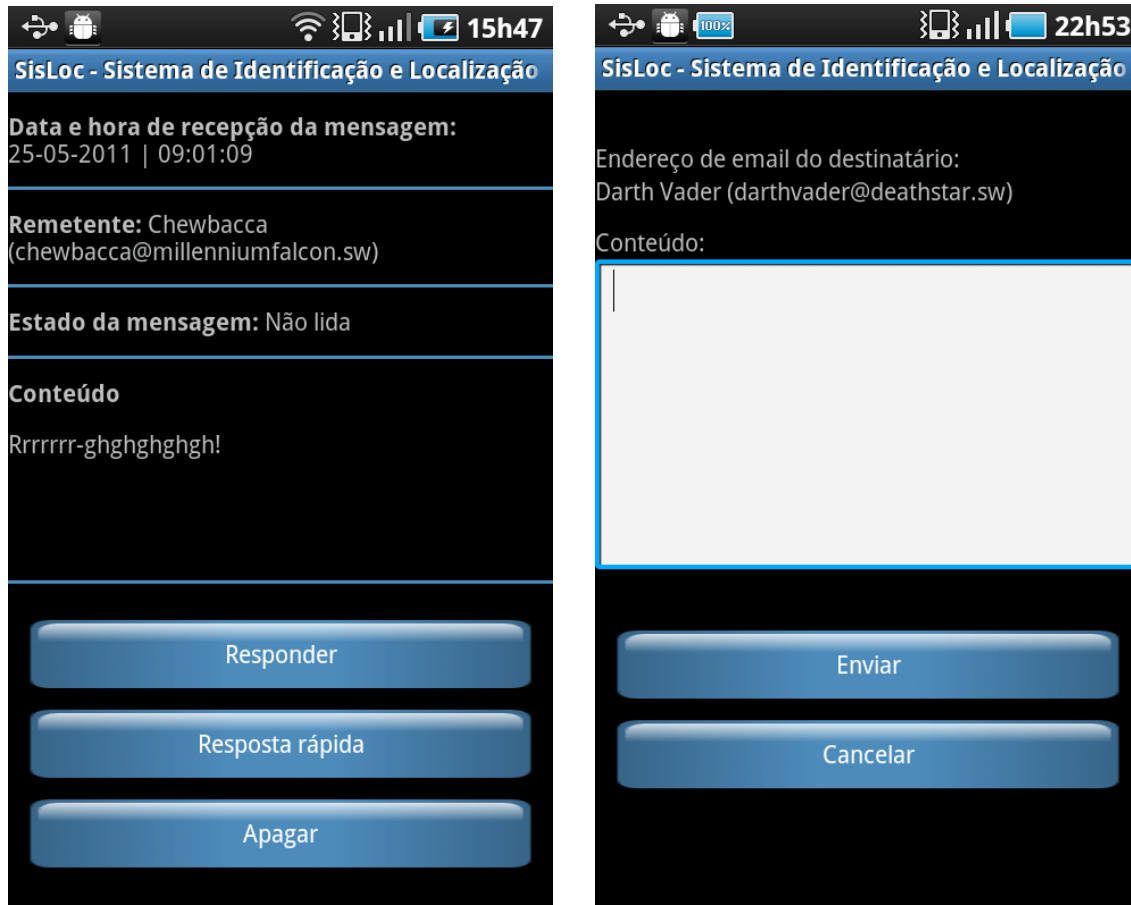


Figura 5.18 - Demonstração do mecanismo de resposta.

a) Vista de mensagem recebida. b) Vista de resposta.

Quando o utilizador pressiona i) é levado para o ecrã “Criar Mensagem”, só que o campo endereço do destinatário já aparece preenchido com o endereço do remetente da mensagem original (figura 5.18 b)).

Quando o utilizador pressiona ii) a aplicação envia de forma automática uma mensagem predefinida ao remetente da mensagem original em que dá conta de que a mensagem enviada anteriormente foi lida (figura 5.19).



Figura 5.19 - Mensagem pré-definida enviada através da resposta “rápida”.

Este tipo de resposta é ideal para situações em que o utilizador não tem disponibilidade para responder à mensagem, mas não quer deixar o remetente sem nenhum tipo de resposta.

5.4.4 - Remoção de mensagens da caixa de entrada

O utilizador tem também a opção de remover as mensagens da sua caixa de correio. Para tal basta seleccionar a mensagem que pretende remover, e depois na vista da mensagem pressionar o botão apagar. Nessa altura surgirá um *popup* de confirmação de remoção da mensagem; se o utilizador responder positivamente, a mensagem será apagada como pode ser visto na figura 5.20.

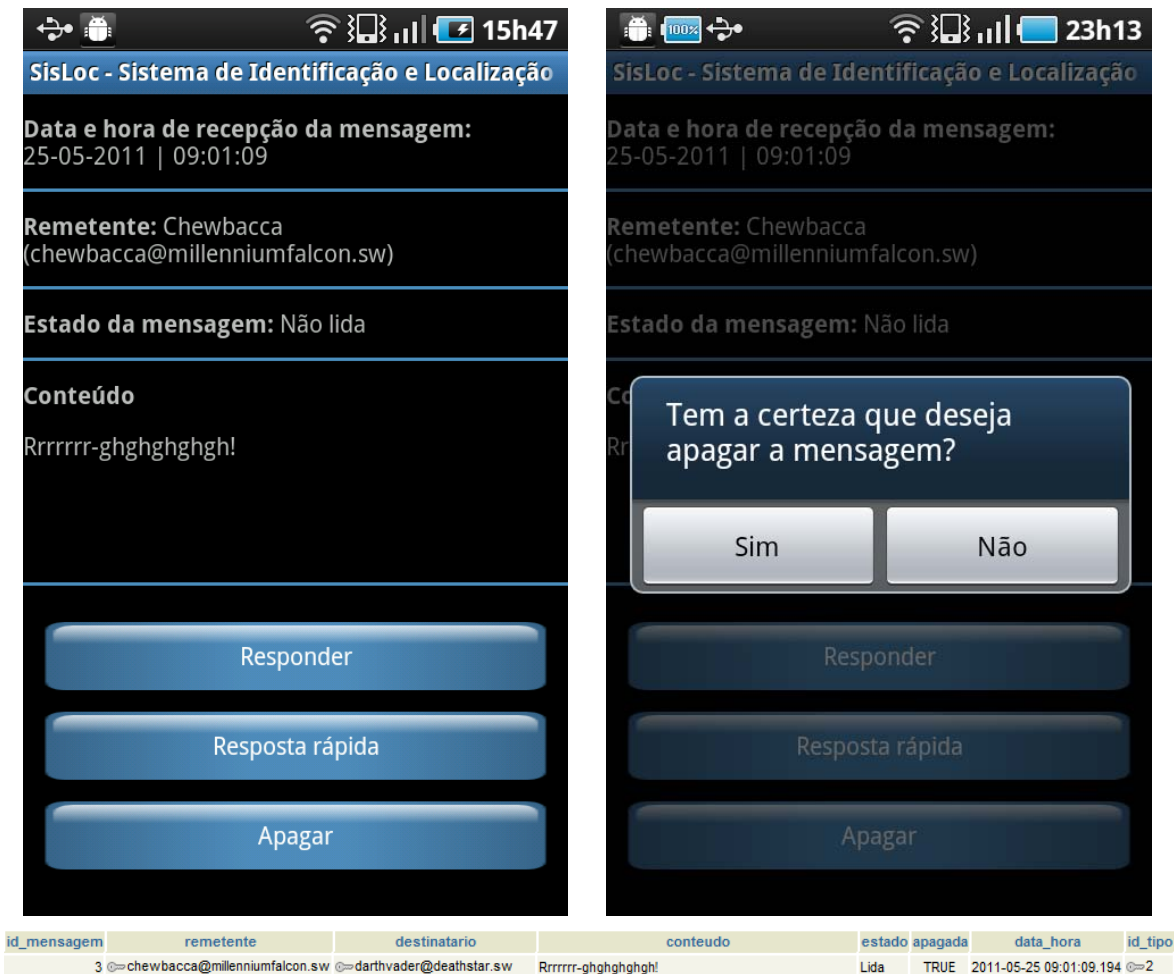


Figura 5.20 - Mecanismo de remoção de mensagens.

No entanto, ao nível da base de dados a mensagem não é verdadeiramente apagada, é mantida apenas invisível para o utilizador que a apagou. O motivo pelo qual a mensagem não é apagada prende-se com as boas políticas de programação em bases de dados, referentes à integridade dos dados. Os dados introduzidos não devem ser eliminados pois podem estar referenciados em várias tabelas, podendo a sua eliminação provocar consequências inesperadas. Para além disso poderá haver interesse em guardar um histórico de mensagens por motivos de segurança. Em condições normais o parâmetro apagado encontra-se a FALSE; quando o utilizador apaga a mensagem, o mesmo parâmetro passa a ter o valor TRUE e a aplicação deixa de mostrar essa mensagem como estando na caixa de correio do utilizador.

Capítulo 6

Conclusões e trabalho futuro

Revendo o trabalho efectuado é possível afirmar que os objectivos essenciais propostos para o desenvolvimento do projecto foram cumpridos com sucesso. O sistema implementado permite identificar e localizar utilizadores em ambientes interiores e exteriores, sendo ainda capaz de oferecer interactividade e personalização aos utilizadores. A precisão da solução revelou-se adequada, de acordo com os requisitos inicialmente definidos, tendo apenas sido detectados erros nos testes interiores em que o utilizador percorreu os pontos de acesso sem nunca parar e nos testes exteriores em que utilizador se encontrava dentro (ou muito próximo) de edifícios.

Numa perspectiva de mercado o sistema necessita ainda de alguns aperfeiçoamentos, pois apesar de ser a única solução conhecida que contempla localização interior e exterior num só sistema com suporte à interacção entre utilizadores recorrendo a mensagens de texto, falta-lhe ainda a implementação de algumas funcionalidades como uma interface Web que permita a consulta e gestão dos utilizadores da base de dados de uma forma simplificada e *user friendly*, bem como a cifragem de dados sensíveis na base de dados. Um outro pormenor a ter em conta são as áreas de aplicação recomendadas. Esta solução baseia-se na tecnologia WiFi que, das várias estudadas, era a que tinha menor precisão; para além disso, a técnica utilizada para localização (baseada no AP a que o telemóvel se encontra ligado) não é das mais precisas para esta tecnologia. Devido a estas razões, esta implementação é pouco recomendada para áreas de segurança crítica como controlo de pacientes, prisioneiros ou de visitantes com acesso não autorizado a certas zonas. Por outro lado revela-se uma importante ferramenta em ambientes empresariais onde pode ser utilizada para registo de presenças e horário laboral ou ainda, por exemplo, para controlo de frotas automóveis fazendo uso da capacidade de localização exterior.

Apesar de o sistema implementado se encontrar funcional e poder ser utilizado em diversas situações, deverá sofrer alterações de forma a torná-lo o mais completo possível; nomeadamente, deverão ser acrescentadas novas funcionalidades e optimizados alguns dos mecanismos existentes.

Ao nível da precisão de localização interior deverá ser utilizado uma técnica de localização mais avançada. Poder-se-á por exemplo efectuar o mapeamento das potências de

signal de cada piso dividido em vários sectores, utilizando para isso triangulação de três ou mais pontos de acesso (RSSI com Fingerprinting). Outro aspecto a ter em conta são as interferências existentes em cada piso, causadas por mobílias e dispositivos sem fios que em determinados horários poderão ser superiores ao normal. As mesmas devem ser tidas em conta na elaboração de um algoritmo dinâmico que seja capaz de reduzir os erros introduzidos por essas interferências.

Uma outra alteração possível será a passagem do serviço de notificações de mensagens presente na aplicação para o servidor *Web*, através da criação de uma aplicação (em Java, C++, Python, etc.), que faça *polling* à base de dados, enviando a notificação para o *smartphone* apenas quando se justificar. Dessa forma seria possível poupar nos recursos consumidos ao nível de processamento, memória e bateria por parte do *smartphone* e de largura de banda consumida na rede *WiFi*.

Relativamente às funcionalidades da aplicação deverá ser acrescentado um mecanismo que permita apresentar ao utilizador informação contextualizada de acordo com a localização do mesmo, como por exemplo horário de atendimento dos serviços de informática, visualização da planta do piso/edifício em que se encontra, onde estariam assinalados a posição do utilizador e pontos de interesse como casas de banho, salas, bares, etc.. Uma maior interacção com o ambiente que rodeia o utilizador, como possibilidade de controlo da iluminação ou temperatura seria também uma boa adição.

A introdução de um menu de configuração de *proxies* assim como a garantia de compatibilidade com o protocolo MS-CHAP são alterações relevantes que poderão vir a ser implementadas na aplicação por forma a ultrapassar a limitação inerente ao sistema operativo Android. No entanto, se se comprovar que tal não é possível e for justificável para a utilização pretendida do sistema, poderá ser considerado a escolha de um outro sistema operativo móvel.

Em termos de funcionalidades exteriores à aplicação Android, deverá ser desenvolvido uma nova interface para o servidor *Web*, interface essa acessível a partir de qualquer *browser* que possibilite do ponto de vista dos utilizadores do sistema enviar/consultar mensagens, configurar perfis e estados, adicionar um novo dispositivo ao sistema associando-o à sua conta etc., e do ponto de vista dos administradores adicionar/remover utilizadores e adicionar/remover pontos de acesso. Tudo isto deve ser possível de uma forma simples que permita a sua utilização por um leigo.

Relativamente à base de dados, os dados mais sensíveis, como as *passwords* armazenadas, deverão ser alvo de cifragem.

Referências

- [1] Kimaldi. (Acedido a 28 de Janeiro 2011). *Sistema de localização de pessoal hospitalar mediante RFID Activo*. Disponível em: http://www.kimaldi.com/kimaldi_por/sectores/geriatricos_y centros_sanitarios/sistema_de_localizacion_de_personal_hospitalario_mediante_rfid_activa
- [2] S. Networks, "Samsung Real Time Location System," 2008.
- [3] V. Hahanov, I. Filipenko, and L. Lavrova, "Contemporary RFID Systems and Identification Problems," em *CAD Systems in Microelectronics, 2007. CADSM '07. 9th International Conference - The Experience of Designing and Applications of*, 2007, pp. 343-344.
- [4] Bitkom, "RFID White Paper Technology, Systems, and Applications " 2005.
- [5] S. A. W. Sanjay E. Sarma, and Daniel W. Engels, "RFID Systems and Security and Privacy Implications," 2003.
- [6] Y. Huanjia and Y. Shuang-Hua, "Connectionless indoor inventory tracking in Zigbee RFID sensor network," em *Industrial Electronics, 2009. IECON '09. 35th Annual Conference of IEEE*, 2009, pp. 2618-2623.
- [7] A. Team. (Acedido a 7 de Março de 2011). *Android vs iOS vs Windows Phone 7 - A Brief Comparison*. Disponível em: <http://www.androidmeup.com/articles/android-vs-ios-vs-windows-phone-7-a-brief-comparison>
- [8] Z. Alliance. (Acedido a 23 de Junho de 2011). *ZigBee Alliance Standards*. Disponível em: <http://zigbee.org/Standards/Overview.aspx>
- [9] P. Kinney, "ZigBee Technology: Wireless Control that Simply Works," 2003.
- [10] S. Onoabagbe, "Zigbee versus Radio Frequency Identification (RFID) " 2008.
- [11] I. S. Association. (Acedido a 7 de Fevereiro de 20011). *IEEE 802.11™: WIRELESS LOCAL AREA NETWORKS (LANs)*. Disponível em: <http://standards.ieee.org/about/get/802/802.11.html>
- [12] J. Ruela, "Wireless LANs - IEEE 802.11 e 802.11e," em *Acetatos de Redes de Banda Larga*, ed. FEUP, 2009/10.
- [13] M. Gauthier, "Wireless Networking in the Developing World - 2.4 GHz Wi-Fi channels," ed, 2009.
- [14] P. Mahasukhon, M. Hempel, C. Song, and H. Sharif, "Comparison of Throughput Performance for the IEEE 802.11a and 802.11g Networks," em *Advanced Information Networking and Applications, 2007. AINA '07. 21st International Conference on*, 2007, pp. 792-799.
- [15] T. Selvam and S. Srikanth, "Performance study of IEEE 802.11n WLANs," em *Communication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International*, 2009, pp. 1-6.
- [16] Y. Chun Yeow, "Experimental study of 802.11n network," em *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on*, 2010, pp. 1067-1072.
- [17] D. Haider. (Acedido a 29 de Janeiro de 2011). *802.11n and Short Guard Interval*. Disponível em: <http://wifijedi.com/category/80211n/short-guard-interval/>
- [18] D. Dyi-Rong, L. Tsung-Chi, T. Chi-Ho, and C. Shin-Jie, "An Implementation of AES Algorithm with the Multiple Spaces Random Key Pre-Distribution Scheme on MOTE-KIT 5040," em *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, 2006, pp. 64-71.
- [19] C. Fine, "The Evolution of RFID Networks: The Potential for Disruptive Innovation " *Center for eBusiness* vol. VIII, March 2006.

- [20] M. Ricardo, "IEEE 802.11 Basic Connectivity," em *Acetatos de Comunicações Móveis*, ed. FEUP, 2009/10.
- [21] C. Consultants, "Zonal Location and Asset Tracking with ZigBee Technology (using RSSI)," 2006.
- [22] T. K. Paul and T. Ogunfunmi, "Wireless LAN Comes of Age: Understanding the IEEE 802.11n Amendment," *Circuits and Systems Magazine, IEEE*, vol. 8, pp. 28-54, 2008.
- [23] P. Zhongmin, D. Zhidong, Y. Bo, and C. Xiaoliang, "Application-oriented wireless sensor network communication protocols and hardware platforms: A survey," em *Industrial Technology, 2008. ICIT 2008. IEEE International Conference on*, 2008, pp. 1-6.
- [24] A. Papapostolou and H. Chaouchi, "Exploiting multi-modality and diversity for localization enhancement: WiFi & RFID usecase," em *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, 2009, pp. 1903-1907.
- [25] S. Jing and Z. Xiaofen, "Study of ZigBee Wireless Mesh Networks," em *Hybrid Intelligent Systems, 2009. HIS '09. Ninth International Conference on*, 2009, pp. 264-267.
- [26] A. Hyo-Sung and Y. Wonpil, "Wireless Localization Networks for Indoor Service Robots," em *Mechronic and Embedded Systems and Applications, 2008. MESA 2008. IEEE/ASME International Conference on*, 2008, pp. 65-70.
- [27] C. Benavente-Peces, V. M. Moracho-Oliva, A. Dominguez-Garcia, and M. Lugilde-Rodriguez, "Global System for Location and Guidance of Disabled People: Indoor and Outdoor Technologies Integration," em *Networking and Services, 2009. ICNS '09. Fifth International Conference on*, 2009, pp. 370-375.
- [28] E. Coca, V. Popa, and G. Buta, "An indoor location system performance evaluation and electromagnetic measurements," em *Design and Technology in Electronic Packaging (SIITME), 2010 IEEE 16th International Symposium for*, 2010, pp. 69-72.
- [29] B. Lewter, "Inexpensive Real Time Location Systems (RTLS) for Event Tracking using Existing WiFi Infrastructures," 2006.
- [30] T. Denis, "Real Time Location System using WiFi," 2006.
- [31] LogicPulse. (Acedido a 28 de Janeiro de 2011). *BlueTag*. Disponível em: <http://www.logicpulse.pt/05produtos/BlueTag/tabid/467/Default.aspx>
- [32] Kimaldi. (Acedido a 28 de Janeiro de 2011). *Controlo de vageantes baseado na tecnologia RFID Activa*. Disponível em: http://www.kimaldi.com/kimaldi_por/aplicaciones/control_de_errantes/control_de_errantes_basado_en_tecnologia_rfid_activa
- [33] Kimaldi. (Acedido a 28 de Janeiro de 2011). *Controlo de presença, acesso e recursos com RFID activos*. Disponível em: http://www.kimaldi.com/kimaldi_por/aplicaciones/control_de_acceso/control_de_presencia_acceso_y_recursos_con_rfid_activos
- [34] Kimaldi. (Acedido a 28 de Janeiro de 2011). *Controlo de presença e traçabilidade logística*. Disponível em: http://www.kimaldi.com/kimaldi_por/aplicaciones/trazabilidad_y_rfid_activa/control_de_presencia_y_trazabilidad_logistica
- [35] R. Centre. (Acedido a 28 de Janeiro de 2011). *Indoor RFID Tracking*. Disponível em: http://www.rfidc.com/docs/indoor_rfid_tracking.htm
- [36] Cleode. (Acedido a 28 de Janeiro de 2011). *LifeNurse*. Disponível em: <http://www.cleosys.fr/en/applications.php?page=lifenurse>
- [37] Ekahau. (Acedido a 28 de Janeiro de 2011). *Ekahau Real-Time Location System (RTLS)*. Disponível em: <http://www.ekahau.com/products/real-time-location-system/overview.html>
- [38] D. Ionescu. (Acedido a 7 de Março de 2011). *Mobile OS Smackdown: Windows Phone 7 vs. iOS vs. Android*. Disponível em: http://www.pcworld.com/article/208491/mobile_os_smackdown_windows_phone_7_vs_ios_vs_android.html
- [39] Christy Pettey and B. Tudor. (Acedido a 6 de Março de 2011). *Gartner Says Android to Become No. 2 Worldwide Mobile Operating System in 2010 and Challenge Symbian for No. 1 Position by 2014*. Disponível em: <http://www.gartner.com/it/page.jsp?id=1434613>
- [40] T. A. S. Foundation. (Acedido a 2 de Junho de 2011). *Welcome to the Apache Software Foundation*. Disponível em: <http://www.apache.org/>

- [41] T. P. Group. (Acedido a 2 de Junho de 2011). *PHP: Hypertext Preprocessor*. Disponível em: <http://www.php.net/>
- [42] P. G. D. Group. (Acedido a 2 de Junho de 2011). *PostgreSQL: The world's most advanced open source database*. Disponível em: <http://www.postgresql.org/>
- [43] p. Project. (Acedido a 2 de Junho de 2011). *phpPgAdmin*. Disponível em: <http://phppgadmin.sourceforge.net/doku.php?id=start>
- [44] Farproc. (Acedido a 23 de Junho de 2011). *WiFi analyzer*. Disponível em: <https://sites.google.com/site/farproc/wifi-analyzer>
- [45] Daveba. (Acedido a 23 de Junho de 2011). *Transparent Proxy*. Disponível em: <http://forum.xda-developers.com/showthread.php?t=766569>
- [46] Samsung. (Acedido a 23 de Maio de 2011). *Samsung Galaxy S Specification*. Disponível em: <http://www.samsung.com/global/microsite/galaxys/specification/spec.html?ver=high>

Anexos

A - Modelo relacional

GrupoUtilizador	id_grupo PK	nome_tipo NN	
PerfilUtilizador	id_perfil PK	nome_perfil UK,NN	notificacao NN
	tracker NN		
EstadoUtilizador	id_estado PK	nome_estado NN	
Utilizador	id_utilizador PK	email UK,NN	password NN
	nome NN	numero_telemovel UK,NN	imei UK,NN
	#id_perfil → PerfilUtilizador(id_perfil)	#id_grupo → GrupoUtilizador(id_grupo)	#id_estado → EstadoUtilizador(id_estado)
TipoMensagem	id_tipo PK	nome_tipo UK,NN	
Mensagem	id_mensagem PK	conteudo NN	data_hora NN
	apagada NN	estado NN	#remetente → Utilizador(email)

#destinatario → Utilizador(email)	#id_tipo → TipoMensagem(id_tipo)
--------------------------------------	-------------------------------------

Edificio	id_edificio PK	nome_edificio UK,NN
-----------------	----------------	---------------------

Piso	id_piso PK	nome_piso UK,NN
-------------	------------	-----------------

Sala	id_sala PK	nome_sala UK,NN
-------------	------------	-----------------

PontoAcesso	id_ponto PK	ssid UK,NN	bssid UK,NN
--------------------	-------------	------------	-------------

#id_sala → Sala(id_sala)

Externa	id_externa PK	nome_localizacao UK	bssid UK
	ssid	endereco_ip	endereco_mac
	coordenadas_gps		

Encontra_se	#imei → Utilizador(imei)	#id_ponto → PontoAcesso (id_ponto)	#id_externa → Externa (id_externa)
--------------------	--------------------------	---------------------------------------	---------------------------------------

data_hora NN

Legenda

PK - Primary Key

UK - Unique Key

- Foreign Key

NN - Not Null

B - Modelo entidade associação

