



Dissertação

Mestrado em Engenharia Informática – Computação Móvel

Arquitetura para aquisição de bens, pagamentos, faturação eletrónica e análise inteligente dos dados envolvidos.

Heitor Emanuel Órfão Simões

*Esta página foi intencionalmente deixada em branco*



Leiria, novembro 2016

Dissertação

Mestrado em Engenharia Informática – Computação Móvel

Arquitetura para aquisição de bens, pagamentos, faturação eletrónica e análise inteligente dos dados envolvidos.

Heitor Emanuel Órfão Simões

Dissertação de Mestrado realizada sob a orientação do Doutor António Pereira, Professor da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

Leiria, Novembro 2016



## **Dedicatória**

*“Determinação, coragem e autoconfiança são fatores decisivos para o sucesso. Não importa quais sejam os obstáculos e as dificuldades. Se estamos possuídos de uma inabalável determinação, conseguiremos superá-los. Independentemente das circunstâncias, devemos ser sempre humildes, recatados e despidos de orgulho.”*

*“Determination, courage and self-confidence are decisive factors for success. No matter what the obstacles and difficulties. If we are possessed of an unshakable determination, we will overcome them. Regardless of the circumstances, we must always be humble, modest and stripped of pride.”*

*Dalai Lama*

*Esta página foi intencionalmente deixada em branco*

## **Agradecimentos**

---

A realização desta dissertação de mestrado contou com importantes apoios e incentivos sem os quais não teria sido possível a sua realização assim, gostaria de expressar os meus agradecimentos a todos os que direta ou indiretamente contribuíram para a realização deste trabalho.

Em primeiro lugar, gostaria de agradecer ao meu orientador, o Professor Doutor António Manuel de Jesus Pereira, pela compreensão, auxílio e disponibilidade que sempre demonstrou para me apoiar, orientar e elucidar ao longo de todo o desenvolvimento deste trabalho e sem o qual seria impossível concluí-lo com sucesso.

Aos meus colegas de trabalho ao longo do Mestrado em Eng. Informática ramo Computação Móvel, o Jorge Mendes e o Patrício Rosa, formamos uma tripla de sucesso.

Gostaria ainda de agradecer às várias pessoas que de algum modo contribuíram para a realização do meu trabalho, nomeadamente.

- Ao Instituto Politécnico de Leiria (IPL), pelos meios e condições que colocou ao meu dispor para a realização deste trabalho.
- Aos professores, Catarina Silva, Luís Marcelino, José Ribeiro e Nuno Costa, pelos momentos em que me ajudaram a remover obstáculos que foram aparecendo.

Por fim, gostaria de agradecer à minha família, à Sónia ao Pedro (Puto Maravilha) e ao Miguel (O meu Fixola), pelos sacrifícios que fizeram por mim ao longo destes últimos anos. Aos meus pais sem os quais não teria sido possível fazer o mestrado em **Engenharia Informática – Computação Móvel**.

O meu muito obrigado a todos.

*Esta página foi intencionalmente deixada em branco*

O autor desta Dissertação, foi coautor na seguinte publicação:

- Heitor Simões, Jorge Mendes, Patrício Rosa, Nuno Costa, Carlos Rabadão, António Pereira, “Secure Low-cost Solution for Elder's eCardio Surveillance”, in Procedia Computer Science, Volume 27, 2014, Páginas 46-56, ISSN 1877-0509.

*Esta página foi intencionalmente deixada em branco*

## **Resumo**

No presente e no futuro, os computadores irão habitar nos mais triviais objetos: etiquetas de roupas, chávenas de café, interruptores de luz, canetas, etc, de forma invisível para o utilizador; assim, devemos aprender a conviver com os computadores e não apenas a interagir com eles. De facto, num futuro, esta interação será feita sem a necessidade da intervenção humana.

Mas para que os equipamentos interajam entre si, ter-se-á de recorrer a serviços baseados em localização, aplicados ao contexto das redes sem fios, uma vez que estes abrem perspectivas para novas aplicações e agregam valor a estas redes. Neste tipo de aplicação, podem ser oferecidos serviços ao utilizador diretamente influenciados pela sua posição física. Esta é uma área de atuação muito abrangente, onde os problemas relacionados com a localização e posicionamento podem ser abordados de diferentes formas, dependendo da aplicação, precisão desejada e ambiente onde o serviço seja implementado.

Atualmente uma grande percentagem de utilizadores transportam os seus Smartphones para todo lado por onde se deslocam; assim, pretende-se desenvolver um sistema que através dos Smartphones que contenham dados básicos de um utilizador/comprador, nomeadamente, o seu número de identificação fiscal, o possam transmitir de forma transparente a outros dispositivos tais como (POS, Máquinas de Vending, Portagens de auto estrada etc...) de forma a que os utilizadores fiquem automaticamente identificados sem necessidade de intervenção humana. O ponto chave para a resolução deste problema é a criação de uma arquitetura com capacidade de inferir a posição de dispositivos sem fios utilizando uma simples solução por software e uma pequena solução de baixo custo em termos de hardware.

Foi, então, implementado e testado um protótipo que, recorrendo à tecnologia Bluetooth Low Energy(BLE) e num ambiente real, transfere os dados de um Smartphone para um outro equipamento através de uma Personal Area Network (PAN) sem necessidade de intervenção humana. Deste modo foram desenvolvidos os módulos, Identify\_IT(aplicação móvel), PoScan(aplicação POS) e MLBS(Midleware que vai ligar as duas soluções).

Palavras-chave: Localização, Wireless, Bluetooth Low Energy, PAN, Smartphone, Mobile.

*Esta página foi intencionalmente deixada em branco*

## ***Abstract***

---

Nowadays and in the future, computers will be part of our most common objects: clothing labels, coffee cups, light switches, pens, etc., invisibly to the user; So we must learn to live with computers and not just interact with them. In fact, in the future, this interaction will be done without the need of human intervention.

But in order the equipment may interact with each other, location-based services will have to be applied to the context of wireless networks, since they open perspectives for new applications and add value to these networks. In this type of application, user services can be offered directly influenced by their physical position. This is a very broad area of action, where problems related to location and positioning can be approached in different ways, depending on the application, desired accuracy and environment where the service is implemented.

Currently a large percentage of users carry their Smartphones everywhere they go; Thus, it is intended to develop a system that through Smartphones which contain basic data of a user / buyer, in particular, its tax identification number, can transmit it transparently to other devices such as (POS, Vending Machines, Tolls Of highway etc ...) So that users are automatically identified without the need of human intervention. The key to solving this problem is the creation of an architecture capable of inferring the position of wireless devices using a simple software solution and a small, low-cost solution in terms of hardware.

A prototype was then implemented and tested using Bluetooth Low Energy (BLE) technology and in a real-world environment, that transfer data from a Smartphone to another device through a Personal Area Network (PAN) without the need of human intervention. This way the modules Identify\_IT (mobile application), PoScan (POS application) and MLBS (Middleware that will connect the two solutions) were developed.

Key-Words: Location, Wireless, Bluetooth Low Energy, PAN, Smartphone, Mobile.

*Esta página foi intencionalmente deixada em branco*

## Índice de Figuras

---

FIGURA 1 - PICONET .....	16
FIGURA 2 - ESTADOS DO BLE .....	21
FIGURA 3 - PILHA PROTOCOLAR BLE .....	22
FIGURA 4 - ESTADOS DO BLE .....	24
FIGURA 5 - ARQUITETURA DA SOLUÇÃO .....	31
FIGURA 6 - DIAGRAMA DE CASOS DE USO .....	33
FIGURA 7 - CASO DE USO 1 - INTRODUÇÃO DE NIF .....	34
FIGURA 8 - CASO DE USO 2 - GRAVAR NIF .....	34
FIGURA 9 - CASO DE USO 4 - INICIAR A VENDA .....	35
FIGURA 10 - CASO DE USO 5 - DESCOBERTA AUTOMÁTICA DO NIF .....	36
FIGURA 11 - CASO DE USO 6 - PREENCHIMENTO DO DOCUMENTO DE VENDA .....	36
FIGURA 12 - CASO DE USO 7 - GRAVAR A VENDA .....	37
FIGURA 13 - IDENTIFY_IT ÍCONE .....	40
FIGURA 14 - APLICAÇÃO IDENTIFY_IT .....	41
FIGURA 15 - POSCAN ÍCONE .....	41
FIGURA 16 - APLICAÇÃO POSCAN .....	42
FIGURA 17 - PILHA PROTOCOLAR DO BLE ADAPTADO [32] .....	44
FIGURA 18 - COEXISTÊNCIA DE CANAIS BLE E WI-FI ADAPTADO [21] .....	45
FIGURA 19 - MAPA DE ESTADOS BLE ADAPTADO [21] .....	46
FIGURA 20 - ESQUEMA DO BLE- ADAPTADO [35] .....	48
FIGURA 21 - ESQUEMA DE FUNCIONAMENTO DA SOLUÇÃO .....	49
FIGURA 22 - PROCESSO DE ESTABELECIMENTO DE CONEXÃO .....	49
FIGURA 23- CONFIGURAÇÃO DA SALA ANECOICA .....	52
FIGURA 24 - DADOS RECOLHIDOS COM SMARTPHONE NA CÂMARA ANECOICA .....	53
FIGURA 25 - DADOS RECOLHIDOS COM TABLET NA CÂMARA ANECOICA .....	53
FIGURA 26 - ESQUEMA DE LOCALIZAÇÃO DE PESSOAS .....	54
FIGURA 27 - MEDIÇÃO DE CONSUMO DE ENERGIA INICIAL .....	55
FIGURA 28 - MEDIDOR DE CONSUMO DE ENERGIA FINAL .....	56

*Esta página foi intencionalmente deixada em branco*

## ***Índice de Tabelas***

---

TABELA 1 - COMPARAÇÃO BLUETOOTH, BLE, WIFI E NFC - FONTE SSR ANALYSIS .....	25
TABELA 2 - ESTUDO COMPARATIVO BLUETOOTH VS BLUETOOTH LOW ENERGY.....	25
TABELA 3 - COMPARAÇÃO BLE, NFC.....	26
TABELA 4 - REQUISITOS FUNCIONAIS.....	30
TABELA 5 - REQUISITOS NÃO-FUNCIONAIS.....	30
TABELA 6 - RESUMO DOS TESTES À UTILIZAÇÃO DA SOLUÇÃO .....	51

*Esta página foi intencionalmente deixada em branco*

## ***Lista de Siglas***

AES	Advanced Encryption Standard
API	Application Programming Interface
ATT	Attribute Protocol
BLE	Bluetooth Low Energy
BR	Basic Rate
cm	Centímetro
dBm	Decibel miliwatt
DEP_REQ	Data Exchange Protocol Request
DID	Device Identification
DSL_RES	Deselect Response
DSL_REQ	Deselect Request
DSSS	Direct-Sequency Spread Spectrum
EDR	Enhanced Data Rate
GAP	Generic Access Profile
GATT	Generic Attribute Profile
GFSK	Gaussian Frequency-Shift Keying
GHz	GigaHertz
GPS	Global Positioning System
HCI	Host-Controller Interface
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
JSON	JavaScript Object Notation

L2CAP	Logical Link Control Protocol
LAN	Local Area Network
LL	Link Layer
LMP	Link Manager Protocol
Mbps	Megabit por segundo
MC	Mobile Computing
MHz	MegaHertz
MIMO	Multiple-Input and Multiple-Output
NFC	Near Field Comunication
NIF	Número de Identificação Fiscal
OFDM	Orthogonal Frequency-Division Multiplexing
PAN	Personal Area Network
PC	Personal Computer
PHY	Physical Layer
PoS	Point of Sale
PSL_REQ	Parameter Selection Request
Qos	Quality of Service
REST	Representational State Transfer
RF	Radio Frequency
RFID	Radio-Frequency Identification
RLS_REQ	Release Request
RLS_RES	Release Response
RSSI	Received Signal Strength Indicator
SBL	Sistemas Baseados em Localização
SDD	Single Device Discovery
SE	Secure Element
SIG	Special Interest Group
SMP	Security Manager Protocol
SPI	Serial Peripheral Interface
TKIP	Temporal Key Integrity Protocol

UART	Universal Asynchronous Receiver/Transmitter
ULP	Ultra Low Power
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy
WLAN	Wireless Area Network
WPA	Wired Protected Access
WUP_REQ	Wake Up Request
WUP_RES	Wake Up Response

*Esta página foi intencionalmente deixada em branco*

---

<b>DEDICATÓRIA</b> .....	<b>I</b>
<b>AGRADECIMENTOS</b> .....	<b>III</b>
<b>NOTA PRÉVIA</b> .....	<b>V</b>
<b>RESUMO</b> .....	<b>VII</b>
<b>ABSTRACT</b> .....	<b>IX</b>
<b>ÍNDICE DE FIGURAS</b> .....	<b>XI</b>
<b>ÍNDICE DE TABELAS</b> .....	<b>XIII</b>
<b>LISTA DE SIGLAS</b> .....	<b>XV</b>
<b>ÍNDICE</b> .....	<b>XIX</b>
<b>1. INTRODUÇÃO</b> .....	<b>1</b>
1.1. ENQUADRAMENTO .....	1
1.2. DEFINIÇÃO DO PROBLEMA .....	1
1.3. ESTRUTURA DO DOCUMENTO .....	3
<b>2. REVISÃO DA LITERATURA</b> .....	<b>5</b>
2.1. A ENVOLVENTE SOCIAL .....	5
2.2. SOLUÇÕES DE IDENTIFICAÇÃO DE UTILIZADORES USANDO O SEU POSICIONAMENTO. ....	6
2.3. SOLUÇÕES MÓVEIS PARA TRANSAÇÕES ELETRÓNICAS. ....	7
2.4. SÍNTESE .....	7
<b>3. TECNOLOGIAS ANALISADAS</b> .....	<b>9</b>
3.1. Wi-Fi .....	9
3.1.1. <i>Wi-fi e a precisão de localização/identificação dos utilizadores</i> .....	10
3.2. NFC .....	11
3.2.1. <i>Comportamento Ativo e Passivo</i> .....	13
3.2.1.1. Fluxo de ativação do modo ativo de comunicação .....	13
3.2.1.2. Fluxo de ativação do modo passivo de comunicação .....	14
3.3. BLUETOOTH .....	16
3.3.1. <i>BLE</i> .....	18
3.3.1.1. Evolução Histórica .....	19
3.3.1.2. Pilha Protocolar .....	21
3.3.1.3. Esquema de Comunicação .....	23
3.4. ESTUDO COMPARATIVO DAS DIVERSAS TECNOLOGIAS .....	24
.....	25
3.5. SÍNTESE .....	26
<b>4. SOLUÇÃO PROPOSTA</b> .....	<b>28</b>
4.1 LEVANTAMENTO DE REQUISITOS .....	28

4.1.1. <i>Requisitos Funcionais e Não Funcionais</i> .....	29
4.1.1.1. <i>Requisitos Funcionais</i> .....	30
4.1.1.2. <i>Requisitos Não Funcionais</i> .....	30
4.2. <b>ARQUITETURA DA SOLUÇÃO</b> .....	31
4.3. <b>CASOS DE USO E PROTOTIPAGEM</b> .....	32
4.3.1. <i>Diagrama de casos de uso</i> .....	32
4.3.2. <i>Prototipagem</i> .....	33
4.4. <b>CENÁRIOS DE UTILIZAÇÃO</b> .....	37
4.5. <b>ANÁLISE DA SOLUÇÃO</b> .....	38
4.6. <b>SÍNTESE</b> .....	38
<b>5. IMPLEMENTAÇÃO DA SOLUÇÃO</b> .....	<b>40</b>
5.1. <b>MÓDULOS DA SOLUÇÃO</b> .....	40
5.1.1. <i>Aplicação Smartphone(Identify_IT)</i> .....	40
5.1.2. <i>Aplicação POS (PoScan)</i> .....	41
5.1.3. <i>Midleware MLBS</i> .....	42
5.1.3.1. <i>BLE – Esquema de Comunicação</i> .....	43
5.1.3.2. <i>Midleware MLBS</i> .....	48
5.2. <b>SÍNTESE</b> .....	50
<b>6. TESTES</b> .....	<b>51</b>
6.1. <b>TESTES AO SOFTWARE DESENVOLVIDO</b> .....	51
6.2. <b>TESTES À MEDIÇÃO DE SINAL</b> .....	52
6.3. <b>TESTES AO CONSUMO ENERGÉTICO DA APLICAÇÃO IDENTIFY_IT</b> .....	55
6.4. <b>TESTES DE ACEITAÇÃO DA SOLUÇÃO DESENHADA.</b> .....	56
6.5. <b>SÍNTESE</b> .....	57
<b>7. CONCLUSÕES E TRABALHO FUTURO</b> .....	<b>58</b>
7.1. <b>CONCLUSÕES</b> .....	58
7.2. <b>TRABALHO FUTURO</b> .....	59
<b>BIBLIOGRAFIA</b> .....	<b>60</b>

*Esta página foi intencionalmente deixada em branca*



# 1. Introdução

---

## 1.1. Enquadramento

No presente e no futuro, os computadores irão habitar nos mais triviais objetos: etiquetas de roupas, chávenas de café, interruptores de luz, canetas, etc, de forma invisível para o utilizador. Devemos aprender a conviver com os computadores, e não apenas interagir com eles [1].

*“Centenas de minúsculos computadores interagem e integram-se no ambiente de um modo tão natural que deixamos de ter a perceção da sua existência”*

MARK WEISER

Este conceito de computação ubíqua está atualmente presente no nosso quotidiano, o que faz com que os componentes se integrem sem necessidade de intervenção humana. No entanto, para que este conceito faça sentido é necessário que os equipamentos interajam entre si e isso apenas é possível recorrendo a serviços baseados em localização geográfica indoor, aplicados ao contexto das redes sem fios, uma vez que abrem perspetivas para novas aplicações e agregam valor a estas redes. Neste tipo de aplicação, podem ser oferecidos serviços ao utilizador para que os parâmetros de entrada e/ou a saída sejam diretamente influenciados pela sua posição física. Esta é uma área de atuação muito abrangente, onde os problemas relacionados com a localização e posicionamento podem ser abordados de diferentes formas, dependendo da aplicação, precisão desejada e ambiente onde o serviço vá ser implementado.

## 1.2. Definição do Problema

Atualmente uma grande percentagem de utilizadores transportam os seus Smartphones para todo lado onde se deslocam; assim, pretende-se desenvolver um sistema que através de

Smartphones que contenham dados básicos do utilizador Número de Identificação Fiscal(NIF) os possam transmitir a outros dispositivos tais como (Point of Sale(PoS), Máquinas de Vending, Portagens de auto estrada, etc...) de forma a que os utilizadores fiquem automaticamente identificados sem grande necessidade de intervenção de utilizadores externos.

Atualmente sempre que um utilizador faz a compra de um produto ou serviço e deseje fazer a sua identificação tem que dar ao vendedor o seu Número de identificação fiscal (NIF), processo que se torna moroso uma vez que nem sempre um comprador sabe os seus dados fiscais e tem de recorrer à abertura de carteiras para poder satisfazer o pedido. Além disso, viola a privacidade do comprador pois tem de estar a transmitir em voz alta os seus dados pessoais.

Acresce ainda o facto de que em determinadas compras de valor pequeno este procedimento é bastante complicado uma vez que nem sempre temos à mão os nossos documentos de identificação! Por exemplo, na aquisição de um jornal ou até na compra de um simples bolo numa pastelaria, procedermos à nossa identificação é um processo moroso; este facto leva a que muitos compradores não se identifiquem ao fazerem as suas compras.

No caso de compras realizadas através de máquinas de Vending ou pagamento de parques de estacionamento automóvel, o processo de identificação do comprador pode até nem conseguir ser feito devido à não existência de interação humana uma vez que o vendedor é apenas uma “máquina”.

Não devemos deixar de olhar também para o facto de que, atualmente, todos os consumidores ao solicitarem documentos de venda com a sua identificação (NIF) obtêm benefícios fiscais o que torna importante a identificação do comprador.

Nesta perspetiva o ponto-chave para a resolução deste problema é a localização de pessoas, normalmente em ambientes interiores(lojas) e por vezes em espaços físicos reduzidos. Este sistema de localização tem a capacidade de inferir a posição de dispositivos sem fios utilizando uma simples solução por software e uma pequena solução de baixo custo em termos de hardware. Assim, procura-se, através de uma arquitetura baseada na tecnologia Bluetooth Low Energy(BLE) a construção de um modelo de localização cujos parâmetros são calculados dinamicamente e em tempo real.

Parece, então, pertinente a realização deste trabalho de dissertação, que se afigura complexo, mas ao mesmo tempo ambicioso e que pode trazer alguma evolução nesta área de trabalho. As envolventes deste trabalho abarcam duas áreas: por um lado, a Gestão de Empresas uma vez que facilita imenso na identificação de contribuintes; por outro, a Engenharia nomeadamente no que diz respeito à micro localização e à transferência de dados via BLE.

Neste documento será descrita a arquitetura sua implementação e teste de um protótipo que num ambiente real transfira os dados de um Smartphone para um outro equipamento através de uma Personal Area Network (PAN) sem necessidade de intervenção humana.

### ***1.3. Estrutura do documento***

Atendendo aos objetivos definidos anteriormente e para além deste capítulo introdutório, a presente dissertação começa por apresentar, no capítulo dois, uma análise e uma revisão da literatura. Em suma, o segundo capítulo exhibe o Estado da Arte.

No capítulo três é feito o estudo e análise das tecnologias que atualmente fazem parte de um Smartphone e que podem ajudar na resolução da problemática no que diz respeito ao envio de dados via wireless sem necessidade do utilizador.

No quarto capítulo é apresentada a solução proposta, sendo iniciado pela definição e levantamento dos requisitos a que esta deve responder, com base na revisão da literatura apresentada no capítulo dois. Após o levantamento dos requisitos é apresentada a arquitetura proposta para a solução, especificando-se com detalhe os diferentes módulos constituintes e seus componentes.

Seguidamente será analisada a forma como foi construída a implementação dos módulos com vista à resolução do problema.

Os testes e a implementação da aplicação móvel são exibidos no capítulo seis onde são explorados os resultados dos testes de forma a validar o desenvolvimento e funcionamento, de acordo com os requisitos definidos. É, ainda, analisada a usabilidade da aplicação por parte dos utilizadores e os cenários de utilização.

A conclusão é efetuada no capítulo sete onde são apresentadas as conclusões relativas ao projeto bem como algumas indicações para trabalho futuro.

## **2. Revisão da literatura**

---

Nos dias atuais, com a convergência das tecnologias de rádio, dos microprocessadores e dos dispositivos eletrônicos digitais de uso pessoal, tornou-se possível fazer com que os dispositivos com certo poder de processamento computacional, tanto móveis quanto fixos, cooperem entre si para fornecer ao utilizador acesso instantâneo a novos serviços de forma transparente. Essa característica levou ao surgimento do conceito de ubiquidade na computação [1].

A computação ubíqua abrange um modelo de computação no qual utilizadores móveis, serviços e recursos são capazes de descobrir outros utilizadores, serviços e recursos. Nesse paradigma computacional, as responsabilidades pela execução de determinado serviço necessário para o utilizador são distribuídas entre uma variedade de dispositivos, cada qual com as suas tarefas e funcionalidades específicas [2].

Mark Weiser, considerado o pai da computação ubíqua, chama a este tipo de computação a “*Tecnologia calma ou invisível*”; considera ainda que temos travado uma luta a tentar entender o design da tecnologia calma, e que os nossos pensamentos ainda estão incompletos e talvez até um pouco confusos. No entanto, acredita-se que a tecnologia calma pode ser o maior problema e o projeto mais importante do século XXI [3].

De seguida será feita uma análise da envolvente social nacional, para percebermos que os países e, nomeadamente o nosso, se encontram abertos e interessados neste tipo de trabalhos.

### **2.1. A envolvente social**

Atualmente as ligações entre os cidadãos e todas as entidades que os envolvem (estado, escolas, hospitais, comercio, etc...) têm tendência a serem complexas e a exigirem informação a todo momento. As relações entre o cidadão e o estado está cada vez mais exigente e torna-se imperioso simplificar a vida aos cidadãos em geral.

Os cidadãos vêm-se na obrigação de transportar inúmeros documentos não só deles mas também dos seus familiares.

As empresas criam sistemas no sentido de organizarem bases de dados com informação sobre os seus clientes, o estado sobre os contribuintes/utentes; no entanto essa interação é sempre feita com recurso a documentos e de forma manual, tornando-se demorada e pouco objetiva.

O estado português criou através do Simplex e pela Lei n.º 36/2011 de 21 de junho, uma norma que estabelece a adoção de normas abertas para a informação em suporte digital na Administração Pública, promovendo a liberdade tecnológica dos cidadãos e organizações e a interoperabilidade dos sistemas informáticos do Estado. Esta lei estabelece ainda: normas e protocolos de comunicação em redes informáticas; normas e protocolos de integração, troca de dados e orquestração de processos de negócio na integração entre organismos [4].

## ***2.2. Soluções de identificação de utilizadores usando o seu posicionamento.***

O tema da identificação de utilizadores através do seu posicionamento sofreu várias análises ao longo dos tempos. Em 1996 e à medida que os dispositivos eletrónicos se tornaram menos exigentes em termos de requisitos de energia e menos onerosos, começaram a aparecer os dispositivos que podem adicionar novos serviços, são apresentadas soluções onde o corpo humano pode trocar informações digitais por acoplamento capacitivo de correntes. Uma portadora de baixa frequência (menos de 1 megahertz) é usada para que não haja energia propagada, minimizando a escuta remota e interferência por redes vizinhas [5].

Em 1998 é descrito um aparelho e método para codificar e transferir dados de um transmissor para um preceptor, utilizando o corpo humano como um meio de transmissão. O transmissor inclui um gerador de campo elétrico, um codificador de dados que opera por modulação do campo elétrico e elétrodos para acoplar o campo elétrico através do corpo humano, registado pela patente, US5796827 A [6].

Em 2011 foi registada por David Creemer a patente US20110171976 A1, que regista um método para direcionamento de conteúdo (por exemplo, um serviço ou um anúncio) de acordo com informações baseadas em localização derivadas de um dispositivo transmissor-recetor sem fios móvel. A informação de posição em função do tempo é utilizada para calcular uma taxa de deslocação e uma direção de deslocação [7].

Em Portugal, realizou-se uma tentativa de criar uma Framework, “Auto configuration and Self-management of Personal Area Networks”, com o objetivo de permitir a operação automática e implantação dinâmica de uma Rede Área Pessoal no ambiente pessoal heterogéneo, ambientes previstos para a próxima geração, no entanto a solução estudada necessita de intervenção do utilizador [8].

### ***2.3. Soluções móveis para transações eletrónicas.***

Os dispositivos móveis (por exemplo, Smartphone, Tablet, etc) são cada vez mais uma parte essencial da vida do ser humano uma vez que são as ferramentas de comunicação mais eficazes e convenientes não estando limitadas pelo tempo e pelo lugar. Os utilizadores móveis acumulam uma rica experiência de vários serviços de aplicações móveis (por exemplo, aplicativos para iPhone, Google apps, etc), que são executados nos dispositivos e/ou em servidores remotos através das redes sem fios. A rápida evolução de computação móvel/Mobile Computing (MC) torna-se uma forte tendência no desenvolvimento da tecnologia da informação, bem como no comércio e indústria. No entanto, os dispositivos móveis enfrentam muitos desafios (a duração da bateria, armazenamento, segurança e largura de banda). Os recursos limitados travam de forma significativa a melhoria da qualidade de serviço.

Na realidade atualmente têm sido desenhadas algumas soluções móveis para transações eletrónicas e comerciais; no entanto, nenhuma permite que o consumidor/utilizador, seja identificado automaticamente perante um vendedor sem necessidade de interação humana.

### ***2.4. Síntese***

Todas as soluções que foram estudadas apresentam sempre lacunas para a solução do problema levantado por esta dissertação.

O tema das PANS associado a localização de indivíduos tem vindo a ser muito discutido ao longo dos tempos, no entanto, abre espaço a muitas soluções num futuro próximo. O tema carece da criação de soluções que sejam efetivamente uma mais-valia para a população em geral e para a área de Gestão de empresas em particular.

É neste contexto que surge a necessidade de uma proposta de solução de baixo custo, utilizando as tecnologias disponíveis atualmente num Smartphone. A análise e escolha de tecnologias disponíveis será abordada no próximo capítulo.

## 3. Tecnologias analisadas

---

Para a realização da presente dissertação foram analisadas todas as tecnologias que poderiam responder ao nosso problema e que estivessem atualmente disponíveis de forma nativa num Smartphone, nomeadamente, Wi-Fi, Near Field Communication (NFC), Bluetooth, BLE.

### 3.1. Wi-Fi

O Wi-Fi é uma marca registada da Wi-Fi Alliance, que é utilizada por produtos certificados que pertencem à classe dos dispositivos de Rede Local Sem Fios/Wireless Área Network(WLAN) baseados no padrão IEEE 802.11. As principais normas da família IEEE 802.11 são:

- IEEE 802.11a: norma Wi-Fi para a frequência 5 GHz com capacidade teórica de 54 Mbps;
- IEEE 802.11b: norma Wi-Fi para a frequência 2,4 GHz e com uma capacidade teórica de 11 Mbps. Esta norma utiliza Direct-Sequence Spread Spectrum(DSSS) para diminuição das interferências;
- IEEE 802.11g: norma Wi-Fi para a frequência 2,4 GHz e com uma capacidade teórica de 54 Mbps;
- IEEE 802.11n: norma Wi-Fi para a frequência 2,4 GHz e/ou 5 GHz e com uma capacidade de 65 a 600 Mbps. Esta norma utiliza como método de transmissão MIMO-OFDM;
- 802.11ac: iniciado em 1998, o padrão irá operar em faixa de 5GHz (menos interferência). IEEE 802.11ac opera com taxas nominais maiores que utilizam velocidade de até 1 Gbps, padronizando em 1300Mbps trabalhando na faixa de 5GHz, como ocorreu com o padrão 802.11n. O 802.11ac ainda não foi padronizado, mas isso não impede que os fabricantes criem aparelhos para trabalhar nesse novo padrão, nessa nova especificação ela utiliza múltiplas conexões de alta velocidade para transferir conteúdo em vez de propagar as ondas de modo uniforme para todas as direções; os roteadores Wi-Fi reforçam o sinal para os locais onde há computadores conectados. Outra vantagem que padrão "AC" ou "AD" traz é a possibilidade de conversar simultaneamente com diversos aparelhos conectados ao roteador sem qualquer interrupção. Por mais rápido que fosse o padrão "N" só permitia que essa conversa fosse feita com um dispositivo por vez. Com essa tecnologia, há uma potencial economia de energia nos dispositivos móveis, a expectativa da indústria é que o padrão 802.11ac esteja efetivamente disseminado em massa até 2016.

Um ponto de acesso sem fios liga um grupo de dispositivos sem fios a uma LAN com fios. Um ponto de acesso é semelhante a um HUB de rede, retransmitindo dados entre dispositivos sem fios ligados e (normalmente) a um único dispositivo com fios ligado, geralmente um Hub Ethernet ou Switch, permitindo aos dispositivos sem fios comunicarem com outros dispositivos com fios. Como o raio de alcance é grande torna-se, por isso, necessário impor limitações, uma vez que, sem segurança, qualquer dispositivo se poderia ligar à Internet desde que esteja ao alcance do sinal, e é por essa razão que há diferentes mecanismos de segurança para a proteção das redes, o que evita a utilização de dispositivos não autorizados, sendo os principais mecanismos os seguintes:

- **Wired Equivalent Privacy (WEP):** existe desde a norma IEEE 802.11 original, consistindo num mecanismo de autenticação básica e que funciona de forma fechada ou aberta através do uso de chaves. Esse sistema pode funcionar com chaves de 64 bits e de 128 bits (podem existir também com 256 bits), tendo assim, diferentes níveis de segurança, sendo a última a mais segura, todavia, não se indica a utilização do WEP devido as suas potenciais falhas de segurança;
- **Wired Protected Access (WPA):** com os problemas com segurança existentes no WEP, a Wi-Fi Alliance criou o formato (WPA), que é mais seguro que o WEP por se basear num protocolo chamado Temporal Key Integrity Protocol (TKIP) e que ficou conhecido, também, como WEP2, e de forma contrária ao WEP, a chave é trocada periodicamente, sendo a sequência definida na configuração da rede (passphrase), recomendando-se a utilização do WPA ao invés do WEP;
- **WPA2(AES):** o WPA2 é uma variante do WPA que se baseia no protocolo Advanced Encryption Standard (AES), fazendo parte da norma IEEE 802.11i. Este mecanismo oferece um alto grau de segurança, no entanto, tem como ponto negativo uma elevada necessidade de processamento, o que pode prejudicar o desempenho do equipamento onde está implementado, por esta razão, não é recomendável para utilizadores domésticos, além disso, não é compatível com equipamentos antigos.

### **3.1.1. Wi-fi e a precisão de localização/identificação dos utilizadores**

Desde o aparecimento da tecnologia Wi-Fi que têm vindo a ser desenvolvidos vários métodos para determinar a localização de dispositivos, mas parte destes revelaram-se impraticáveis devido às grandes condicionantes impostas pelos seus criadores, os quais fixavam em demasia a solução ao caso em estudo, não encontrando uma resposta genérica, capaz de ser aplicada a outras disposições de pontos de acesso (APs) ou a outros locais [9].

Grande parte dos sistemas de localização em redes Wi-Fi funcionam em duas fases: uma fase de treino (fase offline) e uma fase de determinação de localização (fase online). Na primeira fase, é feita a recolha de todas as potências de sinais Wi-Fi recebidas por um dispositivo móvel, sendo isto feito em várias posições do espaço de localização que servirão de pontos de referência. Em cada posição, o dispositivo móvel fica à escuta em toda a gama de frequências utilizadas pela norma Wi-Fi e regista as potências de sinais recebidos e o Service Station Identifier (SSID) do respetivo AP. As posições registadas formam normalmente uma grelha de posições, contudo há casos onde somente são feitos os registos dos sinais Wi-Fi em posições consideradas estratégicas para o sistema de localização. Para cada posição registada, é feita a média da potência de sinal para cada AP em alcance e é sobreposto ao mapa do espaço de localização, construindo assim o chamado mapa rádio. A este processo de criação de um mapa rádio é dado o nome de RF fingerprinting [10].

Com base nos diversos métodos focados acima a precisão de posicionamento e em vários estudos levados a cabo estima-se que o erro de posicionamento se situa na casa de 7,14 metros [11].

### **3.2. NFC**

A tecnologia NFC é uma tecnologia emergente focada na conectividade sem fios de curto alcance, apenas poucos centímetros. Trata-se de uma tecnologia que evoluiu da combinação de outras tecnologias de comunicação e identificação Contactless e que facilita a conectividade entre dispositivos eletrónicos. O NFC permite interações bidirecionais de uma forma simples e segura entre dispositivos eletrónicos permitindo, assim, aos consumidores efetuarem de forma segura transações Contactless, acederem a conteúdo digital e conectar dispositivos com um simples toque.

Esta tecnologia móvel vem, assim, aumentar o conforto, segurança e rapidez em inúmeros processos tais como pagamentos sem dinheiro físico, compra de bilhetes através do telemóvel a qualquer hora e em qualquer lugar, melhores esquemas de fidelização com cupões, vouchers, cartões, entre outros, sempre no seu telemóvel.

O NFC resultou de um esforço inicial da Royal Philips Electronics e da Sony Corporation. Em 2004 estas empresas formaram o NFC Forum para promover a implementação e definição como standard da tecnologia NFC para garantir a interoperabilidade entre dispositivos e serviços. O NFC Forum tem neste momento cerca de 130 membros e continua a ser a entidade de referência no universo em expansão do NFC. Baseando-se em Radio-Frequency Identification(RFID) de curto alcance, esta é uma tecnologia de Smart Card Contactless e opera a 13,56 MHz. O NFC apresenta retro compatibilidade com os atuais standards Contactless e suporta ainda dois protocolos próprios, o NFCIP-1 e o NFCIP-2. Outra característica é a flexibilidade desta tecnologia e o facto de um chip NFC poder funcionar não só como um cartão Contactless, mas também como um leitor Contactless. Este último modo de funcionamento torna o NFC muito apropriado para identificação de dispositivos e inicialização de comunicação.

A tecnologia NFC tem três modos de operação diferentes. Os diferentes modos de operação baseiam-se na norma ISO/IEC 18092 NFCIP-1 e na ISO/IEC 14443, dois standards de Smart Card Contactless:

- Modo Leitura/Escrita: o dispositivo NFC é capaz de ler etiquetas NFC. Este modo tem uma interface de radiofrequência que está em conformidade com a norma ISO 14443 e o FeliCa;
- Modo Peer-to-Peer: dois dispositivos NFC podem trocar dados. Por exemplo, pode partilhar os parâmetros de ligação Bluetooth ou Wi-Fi, ou trocar dados, como cartões-de-visita ou fotografias digitais. Este modo está em conformidade com a norma ISO/IEC 18092;
- Modo Emulação de Cartões: o próprio dispositivo NFC age como sendo uma etiqueta NFC, assemelhando-se a um Smart Card Contactless tradicional.

O telemóvel é o dispositivo móvel de eleição para a implementação desta tecnologia. Tal facto deve-se a este ser um dispositivo móvel e pessoal que praticamente toda a gente possui. Um telemóvel com a tecnologia NFC é composto pelos seguintes 3 elementos:

- Antena: permite a criação do campo magnético utilizado para transmitir os dados;
- Chip NFC: gere as comunicações entre o processador das aplicações do telemóvel, o meio de transmissão de dados (antena) e o local onde se encontram armazenadas as aplicações (Elemento Seguro);
- Elemento Seguro: local onde são armazenadas, de forma segura, as aplicações.

O Elemento Seguro/Secure Element (SE) pode ser visto como um local de armazenamento seguro presente no telemóvel, para além do chip NFC e da antena. No SE podem ser armazenadas várias aplicações, que podem estar a ser executadas de forma independente entre elas próprias e do próprio telemóvel.

### **3.2.1. Comportamento Ativo e Passivo**

Nos modos de operação referidos atrás, os dispositivos NFC podem assumir dois tipos de comportamento:

- Modo Ativo: no modo ativo as informações são codificadas usando código Miller com 100% de modulação, atingindo uma taxa de transmissão de 106Kbps. Nesse modo, iniciador e alvo se comunicam gerando alternadamente seus campos magnéticos;
- Modo Passivo: com codificação Manchester à taxa de modulação de 10%, transmite a até 424Kbps. O iniciador provê um campo magnético portador, o qual induz corrente na antena do alvo, energizando-o, e este por sua vez responde modulando esse campo [12].

Torna-se necessário perceber as diferenças entre os dois modos de ativação da comunicação.

#### **3.2.1.1. Fluxo de ativação do modo ativo de comunicação**

No modo ativo de comunicação (também chamado de NFC ativo), o fluxo inicia-se com um passo de prevenção de colisão. Uma vez que o meio esteja livre, o dispositivo iniciador entra no modo NFC ativo. O iniciador deve executar o algoritmo de deteção de colisão para verificar se há algum campo RF externo. Se nenhum for detetado, ativa o seu campo RF. Em seguida, envia um pedido de requisição de atributo (Attribute Request – ATR\_REQ) a uma taxa de transmissão que pode ser de 106Kbps, 212Kbps ou 424Kbps. O iniciador então desliga o seu rádio e aguarda uma resposta. Os parâmetros negociados nesse pedido são as taxas de transmissão de ida e de volta, e o limite máximo de dados para uma trama. O alvo que recebeu a trama ATR\_REQ executa o algoritmo de prevenção de colisão de resposta (vários alvos podem responder ao mesmo tempo, causando uma colisão). Se o meio estiver livre, o alvo envia a trama de resposta de atributo (Attribute Response – ATR\_RES) de volta, na mesma taxa de transmissão, e desliga seu rádio [12].

O iniciador faz uma deteção de colisão. Caso receba mais de uma resposta ao mesmo tempo (colisão), reenvia a trama ATR\_REQ. Caso contrário, recebe a trama de resposta contendo os

parâmetros propostos pelo alvo. Se não estiver satisfeito com algum parâmetro, envia uma trama Parameter Selection Request (PSL\_REQ) para mudar um parâmetro, e aguarda uma resposta PSL\_RES. Se estiver satisfeito, envia uma trama do tipo Data Exchange Protocol Request (DEP\_REQ) para iniciar o protocolo de troca de dados. Se der tudo certo, a essa altura o alvo terá um número de identificação (Device Identification - DID) ao qual o iniciador se referirá daí por diante [12].

Após terminar a sua troca de dados, o iniciador pode desativar o protocolo de troca de dados. Ao enviar uma trama Deselect Request (DSL\_REQ) a um alvo em particular, o alvo envia uma trama de resposta Deselect Response (DSL\_RES) e entra em modo sleep. Neste modo, a trama pára de responder ao protocolo de troca de dados. Para reativá-lo, o iniciador deve enviar uma trama Wake Up Request (WUP\_REQ) que contém a identificação (DID) do alvo. Em seguida o alvo responde com uma trama Wake Up Response (WUP\_RES) e volta a ativar-se. O iniciador pode liberar um alvo com o qual não deseja manter mais nenhum vínculo. Para isso, envia uma trama Release Request (RLS\_REQ) e aguarda uma trama de confirmação do alvo do tipo Release Response – RLS\_RES. Neste momento, o alvo perde o seu número de identificação (DID) e fica livre para passar por outro processo de inicialização [12].

### **3.2.1.2. Fluxo de ativação do modo passivo de comunicação**

No modo passivo de comunicação (também chamado de NFC passivo), o fluxo de inicia-se a prevenção de colisão. Uma vez que o meio esteja livre???, o dispositivo iniciador entra no modo NFC passivo. O próximo passo consiste num loop em que ocorrem a inicialização e a descoberta de único dispositivo (Single Device Discovery - SDD). Esta etapa utiliza protocolos de descoberta de dispositivo, de acordo com a taxa de transmissão escolhida pelo iniciador. A 106Kbps, usa-se o protocolo de detecção por colisão de bit. A 212 e 424Kbps, usa-se o protocolo de detecção por janela de tempo. Os dispositivos alvo possuem os seguintes estados de funcionamento:

- Estado Desligado (POWER OFF): o alvo não está a receber um campo magnético suficientemente forte para entrar em funcionamento;
- Estado Perceptivo (SENSE): o alvo está a ser alimentado por um campo magnético e encontra-se preparado para responder a iniciadores à procura de dispositivos alvo;

- Estado de Resolução (RESOLUTION): o alvo permanece neste estado enquanto é anunciado o protocolo de descoberta de dispositivo. Uma vez que é descoberto, entra no Estado Seleccionado;
- Estado Seleccionado (SELECTED): neste estado, o alvo é capaz de responder aos comandos de determinação de parâmetros e de transmissão de dados, emitidos pelo iniciador;
- Estado Adormecido (SLEEP): um alvo no Estado Seleccionado que recebe uma requisição de remoção entra no Estado Adormecido. Aqui o alvo só é capaz de responder à requisição para acordar (daí volta para o Estado de Resolução) [13].

A deteção por colisão de bit funciona da seguinte forma:

1) O iniciador faz uma requisição para que todos os alvos respondam, de forma síncrona, com seus números binários de identificação única. O iniciador recebe todos os identificadores de uma vez, sobrepostos (totalmente colididos);

2) O iniciador verifica a primeira posição de bit (a posição do bit mais significativo). Caso tenha havido colisão (um valor 0 de um alvo e um valor 1 de outro), prevalece o nível alto (no caso, o valor 1). Então o iniciador faz uma nova requisição, para que respondam todos os alvos cujos identificadores contêm o valor 1 na primeira posição de bit;

3) Desta vez, os alvos cujos identificadores começam com 0 não respondem, e por conseguinte menos colisões ocorrem. O iniciador repete a etapa 2, mas desta vez verificando também a próxima posição de bit;

4) Este processo repete-se até que o iniciador faça uma requisição com um identificador completo, à qual apenas um alvo irá responder (já que o identificador é único).

Com o NFC, o Smartphone ganha outras funcionalidades como a implementação de aplicações para pagamento e transporte com cartões de proximidade (RFID). De facto, existem três grandes vantagens em usar o NFC num Smartphone: a primeira é a sua disseminação em larga escala; a segunda está no poder de processamento/memória superiores ao de uma etiqueta RFID; e a terceira está no acesso que o Smartphone tem a redes de dados (redes móveis, redes locais ou Internet) [13].

### **3.3. Bluetooth**

Bluetooth é uma tecnologia de rede voltada para aplicações de curto alcance de baixa potência. Assim, foi inicialmente desenvolvida pela Ericsson, mas trata-se uma especificação aberta, gerida pelo Grupo de Interesse Bluetooth Special. [14]

Bluetooth é uma especificação de rede sem fios de âmbito pessoal (Wireless Personal Area Network – PAN) consideradas do tipo PAN ou mesmo WPAN. O Bluetooth estabelece uma maneira de conectar e trocar informações entre dispositivos como Smartphone, computadores, impressoras, etc. Esta comunicação é feita através de uma frequência de rádio de curto alcance globalmente licenciada e segura.

Quando dois ou mais dispositivos se comunicam por meio de uma conexão Bluetooth, eles formam uma rede denominada Piconet. Nesta comunicação, o dispositivo que iniciou a conexão assume o papel de Master (mestre), enquanto que os restantes dispositivos se tornam Slave (escravos). Cabe ao master a tarefa de regular a transmissão de dados na rede e o sincronismo entre os dispositivos.

Cada Piconet pode suportar até 8 dispositivos (um Master e 7 Slave); no entanto, é possível elevar este número a partir da sobreposição de Piconets. Em poucas palavras, este procedimento consiste em fazer com que uma Piconet se comunique com outra que esteja dentro do limite de alcance, esquema este denominado Scatternet. Note-se que um dispositivo Slave pode fazer parte de mais de uma Piconet ao mesmo tempo; no entanto, um master pode ocupar esta posição somente numa única Piconet.

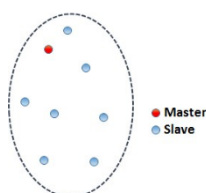


Figura 1 - Piconet

Assim como em qualquer tecnologia de comunicação, o Bluetooth precisa de uma série de protocolos para funcionar, cada um atendendo a um fim específico. Os mais importantes são chamados de protocolos núcleo ou protocolos de transporte e são divididos, basicamente, nas seguintes camadas:

- Radio Frequency(RF): como o nome indica, camada que lida com os aspetos relacionados ao uso de radiofrequência;
- Baseband: camada que determina como os dispositivos localizam e se comunicam com outros aparelhos via Bluetooth. É aqui, por exemplo, que se define como dispositivos master e Slave se conectam dentro de uma Piconet, sendo também onde os padrões SCO e ACL (mencionados anteriormente) atuam;
- Link Manager Protocol(LMP): esta camada responde por aspetos da comunicação em si, lidando com parâmetros de autenticação, taxas de transferência de dados, criptografia, níveis de potência, entre outros;
- Host Controller Interface(HCI): esta camada disponibiliza uma interface de comunicação com hardware Bluetooth, proporcionando interoperabilidade entre dispositivos distintos;
- Logical Link Control and Adaptation Protocol(L2CAP): esta camada serve de ligação com camadas superiores e inferiores, lida com parâmetros de Qualidade de Serviço/Quality of Service (Qos), entre outros.

Bluetooth tem o potencial para ser muito mais do que a substituição de um fio, o Bluetooth foi de facto elaborado com um objetivo mais ambicioso. O Bluetooth mantém a promessa de se tornar a tecnologia de escolha para as redes adhoc de futuro. Isto é em parte porque o seu baixo consumo de energia e baixo custo potencial tornam-no numa solução atraente para os dispositivos móveis típicos usados em redes adhoc. Bluetooth é uma maneira de conectar e trocar informações e dados entre Smartphones, laptops, câmaras digitais etc [16].

O consumo de energia varia consoante a classe de Bluetooth.

Seguidamente iremos analisar o BLE, que se afigura mais importante para o trabalho a desenvolver.

### **3.3.1. BLE**

O BLE é uma tecnologia criada como complemento ao Bluetooth clássico e que tem como principal objetivo tornar-se na tecnologia sem fios com o menor consumo energético. O BLE é uma tecnologia distinta do Bluetooth clássico. Apesar de herdar a marca Bluetooth® e grande parte da sua tecnologia, tem objetivos e segmentos de mercado bastante distintos.

O Bluetooth clássico foi criado para juntar os mundos da computação e da comunicação, ligando os telemóveis aos computadores. No entanto, rapidamente se percebeu que era prático utilizá-lo para estabelecer uma ligação áudio do telemóvel para um auricular. Com o crescimento da tecnologia foram adicionadas muitos mais casos de uso como o streaming de música e a transferência de ficheiros.

A tecnologia Bluetooth é uma tecnologia de curto alcance de comunicação cuja robustez, baixo consumo de energia e baixo custo, é ideal para uma ampla gama de dispositivos que vão desde telemóveis, Smartphones, computadores, dispositivos médicos até produtos de entretenimento doméstico.

A tecnologia de base é definida e mantida pelo Bluetooth SIG na "Especificação do núcleo", que serve uma estrutura uniforme para dispositivos de forma a operarem entre si.

O BLE é caracterizado por uma pilha de protocolos inteiramente nova, para uma rápida acumulação de ligações muito simples. Torna-se importante explorar as motivações que levaram à sua criação, bem como as suas principais características e implementações.

BLE é a resposta da Bluetooth SIG para a convergência de várias tendências-chave na conectividade sem fios, nomeadamente:

- **Wireless everywhere:** atualmente a conectividade está presente num número crescente de dispositivos, que têm sido tradicionalmente ligados através de cabos ou que simplesmente não possuem qualquer ligação;
- **Portabilidade:** enquanto todos os mercados sem fios têm crescido de forma constante nos últimos anos, o mercado dos dispositivos sem fios PAN tem crescido de forma

muito acentuada levando, inclusive, à necessidade de estes serem alimentados por uma bateria pequena, como uma moeda;

- Baixo custo: com esta tecnologia sem fios a generalizar-se, a concorrência e a necessidade de penetrar no mercado torna esta tecnologia de baixo custo.

A tecnologia BLE responde à necessidade de uma ligação de comunicação entre os dispositivos simples que devem operar com baixo consumo de energia e ter um custo muito baixo, sendo particularmente adequada para dispositivos que precisam de transferir uma quantidade muito pequena de dados em intervalos de tempo relativamente curtos.

### **3.3.1.1. Evolução Histórica**

Foi criado pela Nokia com o nome de Wibree, antes de ser adotado pelo Bluetooth Special Interest Group (SIG) com o nome BLE, ou Bluetooth Smart. O BLE tomou um caminho completamente diferente do Bluetooth clássico. Em vez de aumentar a largura de banda disponível, foi otimizado para consumos de energia muito baixos. Assim, os objetivos da criação desta nova tecnologia foram permitir uma utilização à escala mundial, baixo custo, robustez, curto alcance e baixo consumo energético. Para permitir uma utilização à escala mundial foram utilizadas frequências na gama dos 2,4GHz ISM (Industrial, Scientific and Medical), uma vez que é uma faixa disponível em todo o mundo e além disso é gratuita, não requerendo qualquer licenciamento, reforçando a ideia do baixo custo. A robustez é conseguida através da utilização de grande parte da especificação do Bluetooth clássico, mas otimizando-a para baixo consumo energético através de larguras de banda mais baixas e comunicações de curto alcance.

Em 2001 Investigadores da Nokia determinaram que havia vários cenários que as tecnologias sem fios ainda não tinham abordado. Para resolver o problema, a Nokia iniciou o desenvolvimento de uma tecnologia sem fios adaptada do padrão Bluetooth, o que iria resultar num baixo consumo de energia a um preço reduzido, minimizando a diferença entre a tecnologia Bluetooth e as novas tecnologias.

Os resultados foram publicados em 2004 e, após negociações com os membros da Bluetooth SIG, em junho de 2007, foi feito um acordo para incluir esta tecnologia na especificação Bluetooth como Bluetooth de baixa energia (BLE).

A especificação BLE está disponível para o público em geral como parte da especificação Bluetooth Core Version 4.0 que é o estado atual da especificação e que inclui alguns recursos opcionais.

Atualmente alguns dos parceiros que estão a licenciar a tecnologia e a colaborar na definição da especificação são Alwise, Broadcom Corporation, CSR, Epson, MindTree, Nordic Semiconductor e Texas Instruments [9].

Os primeiros chips BLE, a partir de RSE, Nordic Semiconductor, foram disponibilizados para o mercado de massa no final de 2010 e início de 2011. Os primeiros produtos de consumo, utilizando a tecnologia BLE apareceram no mercado no primeiro semestre de 2011.

O protocolo BLE não é compatível com o protocolo Bluetooth clássico. No entanto, a tecnologia BLE e a tecnologia Bluetooth utilizam o mesmo espectro e o hardware subjacente é semelhante. Um determinado dispositivo pode ser capaz de operar como uma tecnologia Bluetooth baixa energia (BLE) e Bluetooth clássico usando o mesmo chip e o mesmo hardware de rádio.

A partir desta especificação é possível assim construir três tipos de dispositivos: Single-Mode, Dual-Mode e Clássico. Os dispositivos Dual-Mode implementam a especificação Bluetooth por completo, fornecendo a possibilidade de utilização tanto de Bluetooth clássico como de BLE.

Os dispositivos Single-Mode apenas implementam a especificação do BLE, ao invés dos dispositivos Clássicos que apenas implementam a parte correspondente ao Bluetooth clássico. Na seguinte tabela podemos ver a compatibilidade em termos de comunicações e tecnologias rádio entre estes dispositivos.

	Single-Mode	Dual-Mode	Clássico
Single-Mode	BLE	BLE	ND
Dual-Mode	BLE	Bluetooth clássico	Bluetooth clássico
Clássico	ND	Bluetooth clássico	Bluetooth clássico

Figura 2 - estados do BLE

### 3.3.1.2. Pilha Protocolar

A arquitetura do Bluetooth Low Energy é muito semelhante à do Bluetooth Clássico. De acordo com, e como podemos ver na Figura 5, esta está dividida em três partes: Controlador, Host e Aplicações. O Controlador é tipicamente o dispositivo físico que transmite e recebe os sinais rádio e entende como é que esses sinais podem ser interpretados como pacotes com informação. O Host é uma camada de software que gere a forma como dois ou mais dispositivos comunicam com outro e quantos serviços diferentes podem ser disponibilizados pelo rádio. As Aplicações utilizam o Host, e conseqüentemente o Controlador, para implementar um caso de uso.

O modo de implementação desta tecnologia divide-se em dois estados de implementação:

- Single-mode: implementação voltada para o baixo consumo de energia e dispositivos de pequeno porte. Apenas implementa a especificação Bluetooth Low Energy;
- Dual-mode: esta implementação é uma extensão de um Bluetooth clássico, voltado para telemóveis e PC's. Implementa ambas as versões do Bluetooth: o clássico e o Low Energy.

A pilha protocolar do BLE divide-se em duas grandes áreas:

- Host;
- Controller.

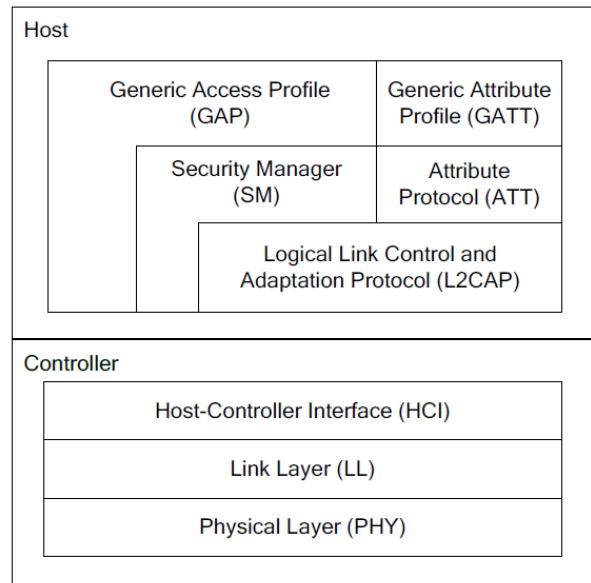


Figura 3 - Pilha protocolar BLE

A pilha do protocolo consiste em duas seções: o Controller e o Host. Esta separação entre Controller e Host é derivada dos dispositivos padrão Bluetooth BR/EDR, em que as duas partes são frequentemente implementadas separadamente. Os perfis e as aplicações que forem implementadas ficarão acima das camadas da pilha GAP e GATT.

A Physical Layer (PHY) implementa um canal de 1Mbps que utiliza o método de salto em frequência adaptativo, GFSK (Gaussian Frequency-Shift Keying) e opera na frequência de rádio não licenciada 2,4 GHz ISM (Industrial, Scientific, and Medical).

A Link Layer (LL) controla, essencialmente o estado de RF do dispositivo, podendo o dispositivo estar num dos cinco estados possíveis: standby, advertising, scanning, initiating, ou connected. Os advertisers transmitem dados sem necessitarem de estar numa ligação, enquanto scanners estão à escuta. O initiator é um dispositivo que responde a um advertiser com um pedido de ligação. Se o advertiser aceitar, ambos entram no estado connected. Quando um dispositivo está numa ligação, está connected numa de duas funções: master ou slave. O dispositivo que iniciou a conexão torna-se o master, e o dispositivo que aceitou o pedido torna-se slave.

A Host-Controller Interface (HCI) fornece um meio de comunicação entre o Host e o controller através duma interface normalizada. Esta camada pode ser implementada por meio de uma API de software, ou por uma interface de hardware, tais como UART, SPI, ou USB.

Acima do controller, a camada Host incorpora o Logical Link Control Protocol (L2CAP), que fornece uma camada básica de abstração baseada em aplicações e serviços. Realiza a fragmentação e desfragmentação dos dados das aplicações, a multiplexação e a desmultiplexação de vários canais através de um link compartilhado.

Além do L2CAP, a camada Host inclui o Security Manager Protocol (SMP) e o Attribute Protocol (ATT). O SMP usa um canal L2CAP fixo para implementar as funções de segurança nas ligações entre dispositivos. O ATT fornece um método para comunicar pequenas quantidades de dados através de um canal L2CAP fixo.

Os dispositivos que determinam os serviços e as características dos outros dispositivos também usam o Generic Attribute Protocol (GATT). O GATT especifica a forma como os dados de perfil são trocados. Esta estrutura define elementos básicos, tais como serviços e características, utilizados por um perfil. Finalmente, o Generic Access Profile (GAP) define quais são os requisitos básicos de um dispositivo Bluetooth.

### **3.3.1.3. Esquema de Comunicação**

O modo de funcionamento da tecnologia sem fios Bluetooth baixa energia tem que se adaptar à transmissão de dados a partir de sensores sem fios compactos (troca de dados a cada meio segundo) ou outros periféricos, como comandos remotos onde a comunicação totalmente assíncrona pode ser usada. Estes dispositivos que enviam baixos volumes de dados (ou seja, alguns bytes) poucas vezes (por exemplo, algumas vezes por segundo para uma vez a cada minuto, ou mais raramente).

O BLE utiliza dois tipos de chips Bluetooth - um de chips de baixa energia e um chip Bluetooth v4.0. O chip de baixo consumo de energia Bluetooth é novo para a especificação Bluetooth - é a parte da tecnologia otimizada para a operação ULP.

Os chips de BLE podem comunicar com outros chips de BLE e Bluetooth v4.0 quando este estiver a usar o Bluetooth de baixa energia parte da tecnologia sem fio de sua arquitetura para transmitir e receber. Os chips Bluetooth v4.0 também têm a capacidade de comunicação com tecnologia sem fio Bluetooth clássico utilizando sua arquitetura Bluetooth convencional.

Os dispositivos BLE podem ter mais do que um estado a cada momento, como mostra a figura abaixo.

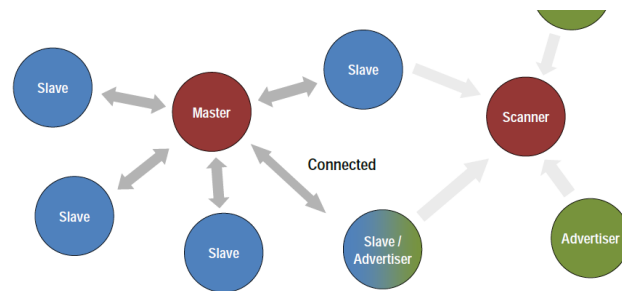


Figura 4 - Estados do BLE

O Master pode ter várias ligações enquanto o Slave apenas poderá ter uma ligação; após o início da comunicação o Master pode simultaneamente ocupar o papel de Master e de Scanner.

O Master e o Slave podem ambos funcionar como advertiser, mas apenas são permitidas conexões slave/advertiser em simultâneo.

Para a resolução do problema proposto escolheu-se esta tecnologia pois além de ser uma tecnologia emergente, o Bluetooth Low Energy tem a capacidade de efetuar ligações rápidas, ter relativamente curto alcance quando comparada com o Wi-Fi (cerca de 10m) e ter algoritmos de correção a falhas na leitura da força do sinal recebido (RSSI) o que permite que o erro cometido na comparação de vários dispositivos através deste parâmetro seja menor.

### ***3.4. Estudo comparativo das diversas tecnologias***

Para melhor compreendermos as diferenças entre as tecnologias fez-se um pequeno estudo comparativo entre as quatro tecnologias.

Deste estudo resulta numa primeira análise que a tecnologia Wi-Fi e Bluetooth têm consumos de energia muito elevados.

Tabela 1 - Comparação Bluetooth, BLE, Wifi e NFC - Fonte SSR Analysis

<b>Wireless Technology Specifications</b>				
	<b>Classic Bluetooth</b>	<b>Bluetooth LE</b>	<b>WiFi</b>	<b>NFC</b>
<b>Standards Body</b>	Bluetooth SIG	Bluetooth SIG	WiFi Alliance	ISO/IEC
<b>Network Standard</b>	IEEE 802.15.1	IEEE 802.15.1	IEEE 802.11n	ISO 13157
<b>Range</b>	100m (330ft)	<b>50m (160ft)</b>	70-250m (230-820ft)	<0.2m (7.8 inches)
<b>Frequency</b>	2.4-2.5GHz	<b>2.4-2.5GHz</b>	2.4-5GHz	13.56MHz
<b>Over the air data rate</b>	2.1 Mbps	<b>1Mbps</b>	Up to 600Mbps w 4x4 MIMO	424kbps
<b>App throughput</b>	0.7-2.1Mbps	<b>0.27 Mbps</b>	Varies	Up to 424 kbps
<b>Latency</b>	100ms	<b>6ms</b>	<1ms	1ms
<b>Peak current consumption</b>	<30mA (Varies)	<b>&lt;15mA (read and transmit)</b>	~50mA (Read) ~200mA (Transmit)	<15mA (read)

Source: SSR Analysis

No estudo comparativo entre o Bluetooth e o BLE saltam à vista aspectos como o consumo de energia e o nº de dispositivos ligados em simultâneo.

Tabela 2 - Estudo comparativo Bluetooth vs Bluetooth Low Energy

<b>Tecnologia/Características</b>	<b>Bluetooth</b>	<b>Bluetooth Low Energy (BLE)</b>
Aplicação	Conectividade entre Dispositivos	Aplicações desportivas, saúde, doméstica, eletrónica
Autonomia	1 – 7 Dias	191 Dias - Vários anos
Largura de banda	720 Kbps	1 Mbps
Alcance	Entre 10 e 100m	<50 m
Nº Dispositivos Ligados Simultâneo	8	Ilimitado
Vantagens	Versatilidade na ligação entre dispositivos	Baixo consumo de energia Compatibilidade versões anteriores
Complexidade	Alta	Baixa
Latência	100 ms	3 ms
Inserção de novo escravo	20 s	N/A
Mudança de estado do escravo (sleep /ativo)	3 s	N/A
Segurança	64 e 128 bits	AES, 128 bits
Topologia	Scatternet	Star, P2P
Capacidade de Voz	Sim	Não
Frequência	2.4 GHz	2.4 GHz
Estrutura do pacote	Access code – 68 or 72-bit  Header – 56-bit Data payload– 32-bit	Preamble - 8-bit Address – 32-bit Data payload – 32-bit CRC – 8-bit
Tamanho do pacote	160 bits	40 bits
Consumo de energia	12.5 mA	8.1 mA

Comparando o BLE e o NFC salta à vista a distancia de atuação nomeadamente porque no caso do NFC tem de ser feita quase em contacteless.

Tabela 3 - Comparação BLE, NFC – adaptado [18]

## What difference of BLE and NFC

BLE is faster and great security than NFC, BLE can use like an Wi-Fi

Aspect	NFC	BLE
RFID compatible	ISO 18000-3	No (but can using like it)
Security Mode	No	Disabled Mode, Passkey Mode
Network Standard	ISO 13157 etc.	IEEE 802.15.1
Network Type	<b>Point-to-point</b>	<b>WPAN (wireless personal area network)</b>
Cryptography	not with RFID tag	<b>available</b>
Range	< 0.2 m	<b>~50 m</b>
Bit rate	424 kbit/s	<b>~1.0 Mbit/s</b>
Set-up time	< 0.1 s	<b>&lt; 0.006 s</b>
Power consumption	<b>&lt; 15mA (read), Unpowered</b>	< 15 mA (read and transmit)
Track location device	No	<b>Yes</b>

- NFC operates time at slower speeds than BLE
- NFC works with an **unpowered device** (RFID Tag)
- NFC power consumption is **greater than that of BLE**
- NFC **doesn't require pairing** (COMFORTABLE, BUT NOT SECURE)
- NFC lower transfer data rate than Bluetooth low energy
- NFC Great for Peer-to-peer communication

Apesar do NFC se apresentar como uma tecnologia de troca de informação sem fios poderosa esta obriga a que os dispositivos estejam suficientemente próximos um do outro obrigando o utilizador a ter algum grau de intervenção (Touch and Run).

Deste estudo resulta ainda que, relativamente à tecnologia WiFi, esta torna difícil a identificação uma vez que precisa de triangulação de antenas. No que à tecnologia NFC diz respeito, esta apresenta sempre a necessidade de intervenção do utilizador pelo que foi também preterida.

Relativamente às restantes duas tecnologias, foi feita uma análise comparativa concluindo-se que a tecnologia Bluetooth Low Energy é a que melhor se adequa, pois é a que possui melhor relação entre latência e consumo energético.

## ***4. Solução proposta***

---

A identificação de forma automática de utilizadores/utentes/clientes num espaço físico (distância) reduzido torna-se vital num mundo em que cada vez mais a informação está centralizada e em que a informação fiscal se torna imperiosa. A permanente necessidade dos utilizadores terem de se identificarem torna o processo de identificação muito moroso e às vezes impossível. A simples compra de um jornal, de uma comida numa máquina de vending, tornam impossível a obtenção de um documento com identificação fiscal.

Analisando o mercado chega-se à conclusão que não existem soluções para fazer face a este problema. O utilizador tem sempre que se identificar e a elaboração de uma fatura passa irremediavelmente pelo preenchimento de um conjunto de campos nomeadamente, número de contribuinte.

Assim, é proposta uma solução que permite eliminar a necessidade de que a cada documento fiscal se tenha que preencher todos estes campos. Para tal iremos utilizar o Smartphone uma vez que atualmente faz parte integrante da vida de qualquer cidadão, resolvendo assim o problema da permanente identificação ao transacionarmos qualquer bem ou serviço.

Neste capítulo efetua-se o levantamento dos requisitos funcionais e não funcionais necessários.

Este levantamento é fundamental de forma a definir as funcionalidades e as especificidades a que cada módulo deve corresponder.

Analisar-se-á todos os módulos que constituem a arquitetura de forma a explicar as suas funções, responsabilidades e interações. É também feita a análise dos módulos constituintes da arquitetura proposta de forma a efetuar o levantamento dos casos de uso e consequente descrição e efetuar a prototipagem quando assim se justifique.

### ***4.1 Levantamento de Requisitos***

Os sistemas informáticos desempenham um papel cada vez mais importante no dia-a-dia das pessoas. Assim, é necessária a produção de sistemas confiáveis e seguros de forma económica e rápida. Contudo, a construção destes sistemas é complexa, pois tem de se lidar com requisitos intransigentes, restrições de integridade e a necessidade de um conhecimento aprofundado de forma a descrever as interações entre o sistema e o ambiente. Quando não existe um bom levantamento de requisitos isto traduz-se numa discrepância entre as funcionalidades reais e as esperadas do sistema.

O levantamento de requisitos é umas das partes mais importantes do processo que resultará no desenvolvimento de um sistema. Entender aquilo que o cliente deseja ou o que o cliente acredita que precisa e as regras do negócio ou processos do negócio. Isso é o fator determinante que move essa importante função que faz parte da Engenharia de Software (Engenharia de requisitos).

Aliado ao levantamento de requisitos, existe o mapeamento dos processos que é de vital importância para a melhoria dos resultados obtidos pelo levantamento de requisitos. Muitos sistemas são retardados em termos de prazo ou até mesmo morrem durante seu percurso, pois, a etapa de levantamento de requisitos é negligenciada [15].

#### **4.1.1. Requisitos Funcionais e Não Funcionais**

O software tem impacto em quase todos os aspetos da sociedade atual, o processo de desenvolvimento é um conjunto coerente de atividades, serviços, tarefas ou funções que o sistema deve executar.

A definição de requisitos numa primeira fase define de forma razoável os objetivos a serem alcançados, pelo que se torna importante não cometer erros nesta fase de desenvolvimento, estes erros levam a graves problemas na fase de construção do software, assim os objetivos da definição de requisitos são a definição dos propósitos da solução proposta sublinhando o seu comportamento externo [16].

O sucesso de um sistema é o nível de correspondência que este tem com os requisitos para os quais foi desenvolvido. Assim, é de extrema importância pois torna possível visualizar e modificar um sistema sem causar problemas ao mesmo. Além disso, o esforço necessário para

localizar uma modificação ou implementação torna-se aceitável. Existem dois tipos de requisitos: funcionais e não funcionais.

#### 4.1.1.1. Requisitos Funcionais

Os requisitos funcionais descrevem as diversas funções que queremos ver no software [17] e especificam os resultados particulares de um sistema. Assim, a próxima tabela irá fazer o resumo dos requisitos funcionais da solução proposta:

Tabela 4 - Requisitos Funcionais

ID	Descrição	Prioridade
F1	Cada utilizador terá que ter um Smartphone com tecnologia BLE.	Obrigatório
F2	O dado necessário será, o número de contribuinte(NIF).	Obrigatório
F3	A passagem de dados do Smartphone para o POS não deve interferir no dia a dia dos utilizadores.	Obrigatório
F4	Cada Smartphone apenas contem um registo.	Obrigatório
F5	O Smartphone permite guardar o número de contribuinte dados.	Obrigatório
F6	O Smartphone comunica através de Bluetooth com o POS.	Obrigatório
F7	O POS estabelece comunicação com o Smartphone e recebe os dados necessários à transação(NIF).	Obrigatório

#### 4.1.1.2. Requisitos Não Funcionais

Os requisitos não-funcionais não estão ligados diretamente às funções fornecidas pelo sistema.

Em geral preocupam-se com padrões de qualidade como confiabilidade, desempenho, robustez, segurança, usabilidade, portabilidade, legibilidade, qualidade, manutenção, entre outros. São muito importantes, pois definem se o sistema será eficiente para a tarefa que se propõe fazer.

Um sistema ineficiente certamente não será usado. Os requisitos não funcionais descrevem então as qualidades globais do software [18]. De seguida iremos fazer o levantamento dos requisitos não-funcionais da solução proposta:

Tabela 5 - Requisitos Não-Funcionais

ID	Descrição	Prioridade
NF1	A interface do sistema deve ser agradável, intuitiva e de fácil utilização	Obrigatório

	para qualquer tipo de utilizador.	
NF2	O sistema deve utilizar a tecnologia sem fios Bluetooth Low Energy para efetuar a comunicação entre o Smartphone e o POS de recolha de dados.	Obrigatório
NF3	O sistema deverá ser implementado com recurso a soluções de baixo custo.	Obrigatório
NF4	Os sensores devem respeitar as especificações definidas pelo Bluetooth SIG na implementação do protocolo.	Obrigatório

## 4.2. Arquitetura da solução

Assim foi desenhada a arquitetura da solução a que se chamou de MISTP

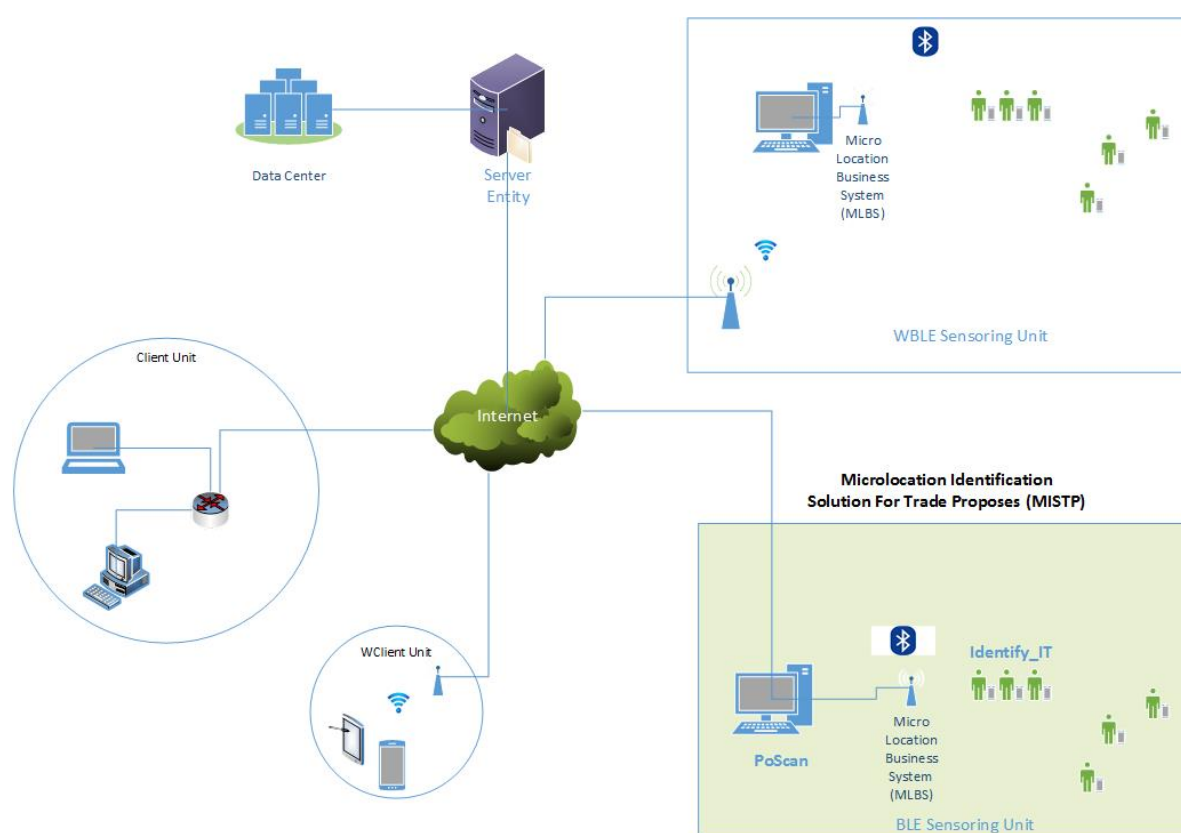


Figura 5 - Arquitetura da solução

A solução é composta por três blocos principais: Identify\_IT, PoScan e MLBS. Estes blocos interagem entre si de forma automática.

O módulo Identify\_IT é um módulo criado para correr num Smartphone e guarda os dados a serem enviados, após aberta a aplicação inicia o modo de anúncio, ou seja, inicia o processo de anúncio da sua presença.

O módulo PoScan é a aplicação onde vai ser registada a venda, neste caso vai ser introduzida a informação necessária à realização de uma venda, este módulo ao iniciar a venda inicia também um processo de varredura e descoberta de Smartphones, que obedeçam a determinados filtros.

Por fim o MLBS, é um Middleware que é responsável pela organização e gestão dos processos de anuncio e descoberta dos pacotes que contem a informação necessária, fazendo também o envio dos dados respetivos.

Um utilizador/comprador com o seu Smartphone no bolso e com a aplicação Identify\_IT instalada, dirige-se a uma loja para adquirir um produto, por exemplo um jornal. Após escolher o jornal dirige-se à caixa para efetuar o pagamento, ao chegar a caixa o cliente/comprador pretende documento de venda identificado com o NIF, no entanto, não tem interesse em perder tempo a abrir carteira para verificar o NIF, não simpatiza com a ideia de estar a dizer o NIF em voz alta e também não pretende estar a causar filas o que faz com que seja mais fácil que o NIF passe de forma automática do seu Smartphone para o PoS.

### ***4.3. Casos de uso e Prototipagem***

A atividade de identificação e especificação de requisitos do software é uma atividade bastante desafiadora. Identificar as reais necessidades do cliente; lidar com clientes; formalizar as necessidades do cliente através da especificação de requisitos, são algumas das tarefas necessárias para a definição dos casos de uso e prototipagem.

#### **4.3.1. Diagrama de casos de uso**

Pretende-se, de seguida, descrever os casos de uso e as funcionalidades que o utilizador espera do sistema. Estes casos de uso estão identificados no diagrama da figura que se segue com o objetivo de dar uma visão geral das funcionalidades de todo o sistema e como é que estas interagem entre si.

#### **Diagrama de casos de uso**



Figura 6 - Diagrama de casos de uso.

### 4.3.2. Prototipagem

#### Caso de Uso 1

Nome: introdução de NIF.

Descrição: efetuar a introdução do número de identificação fiscal.

Pré-Condições: nenhuma.

Caminho Principal:

1. O utilizador abre a aplicação;
2. O utilizador preenche o campo “NIF” com o seu número de contribuinte.



Figura 7 - Caso de uso 1 - Introdução de NIF

## Caso de Uso 2

Nome: introdução de NIF

Descrição: efetuar a introdução do número de identificação fiscal.

Pré-Condições: nenhuma.

Caminho Principal:

1. O utilizador abre a aplicação;
2. O utilizador preenche o campo “NIF” com o seu número de contribuinte.



Figura 8 - Caso de uso 2  
- Gravar NIF

## Caso de Uso 3

Nome: anúncio automático de NIF

Descrição: envio automático do número de identificação fiscal.

Pré-Condições: número de identificação fiscal estar gravado.

Caminho Principal:

1. Basta abrir a aplicação e o envio do número de identificação fiscal é feito de forma automática.

## Caso de Uso 4

Nome: iniciar a venda

Descrição: clicar no botão New Sale.

Pré-Condições: nenhuma.

Caminho Principal:

1. Basta abrir a aplicação e clicar no botão New Sale.

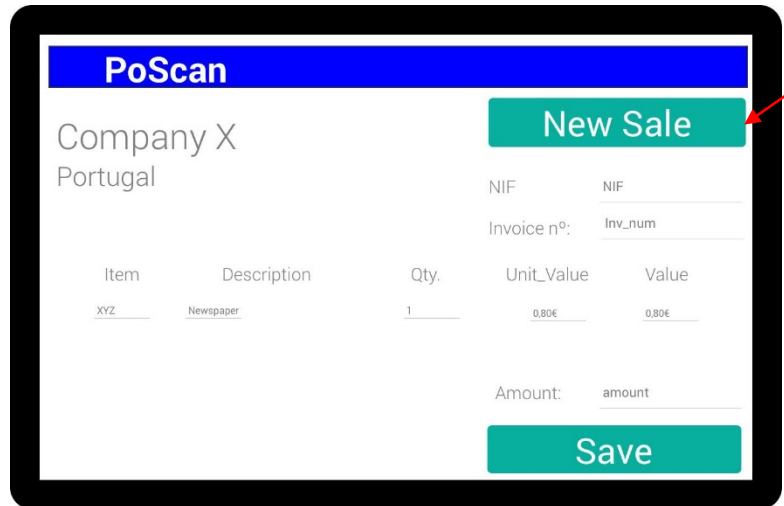


Figura 9 - Caso de uso 4 - Iniciar a Venda

## Caso de Uso 5

Nome: descoberta automático do NIF

Descrição: envio automático do número de identificação fiscal.

Pré-Condições: o botão New Sale ter sido ativado.

Caminho Principal:

1. O número de identificação fiscal é preenchido de forma automática.

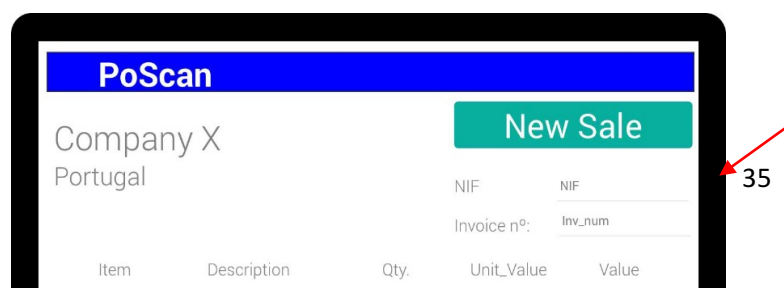


Figura 10 - Caso de uso 5 - Descoberta automática do NIF

### Caso de Uso 6

Nome: preenchimento do documento de venda

Descrição: preencher todos os campos.

Pré-Condições: nenhuma.

Caminho Principal:

1. Basta preencher todos os campos.

The screenshot shows the PoScan application interface. At the top, there is a blue header with the text "PoScan". Below the header, the company name "Company X" and "Portugal" are displayed. To the right, there is a green button labeled "New Sale". Below the company name, there are input fields for "NIF" and "Invoice nº:". A table with the following columns: "Item", "Description", "Qty.", "Unit\_Value", and "Value" is shown. The table contains one row with the following data: "XYZ", "Newspaper", "1", "0.80€", and "0.80€". A red arrow points to the "Value" column of this row. Below the table, there is an "Amount:" label and an input field for "amount". At the bottom right, there is a green button labeled "Save".

Figura 11 - Caso de uso 6 - Preenchimento do documento de venda

### Caso de Uso 7

Nome: gravar a venda.

Descrição: clicar no botão Save.

Pré-Condições: nenhuma.

Caminho Principal:

1. Basta clicar no botão Save.

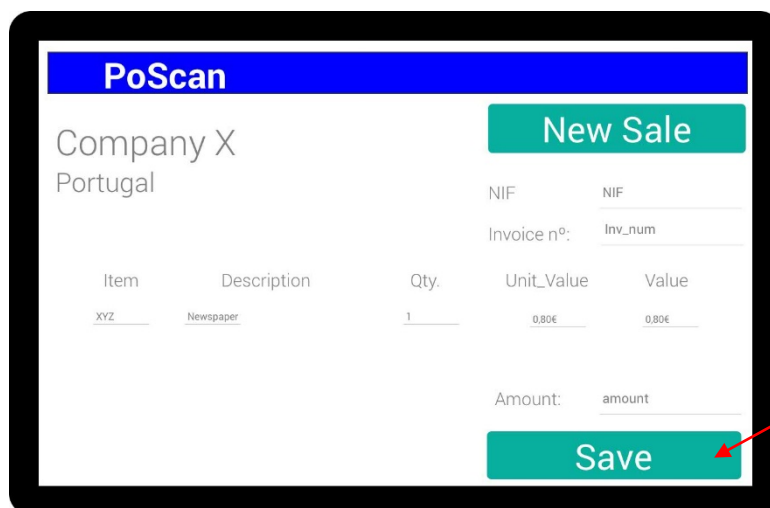


Figura 12 - Caso de uso 7 - Gravar a venda.

### **Caso de Uso 8**

Nome: libertar o NIF descoberto

Descrição: liberta o NIF descoberto e prepara nova venda

Pré-Condições: clicar no botão Save.

Caminho Principal:

1. Basta clicar no botão Save.

### **4.4. Cenários de utilização**

O objetivo da solução proposta é simples, o utilizador faz download de uma aplicação gratuita de nome Identify\_IT; após fazer o download o utilizador abre a aplicação e grava o seu número de identificação fiscal.

O vendedor terá de adquirir uma aplicação de POS de nome PoScan, que servirá para fazer as suas vendas.

Sempre que o utilizador quiser fazer compras com identificação, basta manter a aplicação aberta ou a correr em segundo plano no seu Smartphone; ao aproximar-se de um local de compra com o PoScan instalado, o utilizador não precisa de dizer nada pois automaticamente o seu NIF irá aparecer no PoScan do vendedor.

Este processo pode ser feito com um vendedor ou com uma máquina de Vending que tenha o PoScan instalado.

Desta forma, evitam-se filas no processo de transmissão verbal dos NIF e impede que pessoas estranhas saibam o NIF de qualquer comprador.

#### ***4.5. Análise da Solução***

Esta solução é de grande interesse para o utilizador/comprador, no entanto, apresenta algumas limitações atuais nomeadamente o facto de apenas Smartphones atuais utilizarem a tecnologia BLE Multi Advertisement, o que restringe um pouco o mercado alvo. Contudo, este problema não se afigura de grave resolução uma vez que com a evolução da tecnologia, em breve estará nativa em todos os Smartphones.

Acresce, também, o facto de que apesar da tecnologia BLE se encontrar em franca evolução verificam-se ainda, neste momento, algumas dificuldades de compatibilidade entre os diversos sistemas de BLE, nomeadamente a necessidade de sustentarem protocolos de Multi Advertisement.

Nesta dissertação foram menosprezados totalmente as informações que dizem respeito à segurança e privacidade dos dados.

#### ***4.6. Síntese***

Depois de terem sido levantados os requisitos funcionais e não funcionais da nossa solução, de terem sido desenhadas as arquiteturas do sistema e de todos os módulos constituintes, foram, ainda, elaborados os estudos dos casos de uso e a prototipagem, bem como a interação entre os diversos módulos.

Definiu-se, assim, uma arquitetura que respondesse às necessidades levantadas pelos requisitos funcionais.

Essa arquitetura envolve três partes essenciais: a componente de Smartphone utilizada pelo utilizador/comprador(Identify\_IT); a parte do POS Posto de venda (PoScan), que vai receber de forma automática os dados do utilizador, nomeadamente, o número de contribuinte; e o Middleware que vai funcionar como “anunciador” e “descobridor” do NIF do comprador.

No capítulo seguinte é abordada a implementação da solução proposta.

## **5. Implementação da solução**

O utilizador/cliente deverá ter um dispositivo com capacidades BLE Multi Advertisement e deverá ter a aplicação Identify\_IT instalada e configurada para que o seu dispositivo esteja com o BLE em modo de anúncio (Advertising) a anunciar o seu NIF. Desta forma, o PoScan ao detetar um pacote de (Advertising), uma vez que se encontra em modo escuta (Discover), vai identificar o cliente e vai analisar a força de sinal RSSI recebido no pacote de forma a identificar se quem está a realizar a compra é quem está mais próximo do PoScan. Caso esta condição se verifique, o PoScan, no ato da compra, associa o NIF do cliente à mesma.

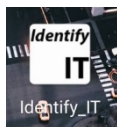
O PoScan é o terminal de venda que será o responsável por detetar os clientes e identificar aquele que se encontra a efetuar a compra. Esta verificação tem como objetivo associar o NIF do cliente à compra que o operador de caixa acaba de registar no PoScan sendo que, para isso, este irá estar sempre à descoberta de clientes e vai identificar o que tiver maior RSSI como sendo o que se encontra a efetuar a compra. Assim, o PoScan, irá estar com o BLE em modo de escuta (Discover) de forma a captar essas informações.

De seguida proceder-se à finalização da venda.

### **5.1. Módulos da Solução**

Genericamente a solução divide-se em três partes distintas: aplicação Smartphone (Identify\_IT), Aplicação PoS(PoScan) e Middleware MLBS.

#### **5.1.1. Aplicação Smartphone(Identify\_IT)**



*Figura 13 - Identify\_IT Ícone*

Como cliente da solução desenvolveu-se uma aplicação destinada a dispositivos baseados no sistema operativo Android da Google. A nossa escolha recaiu sobre esta plataforma uma vez

que a mesma funciona bem em relação à especificação da API BLE; estas não são proprietárias e de uso restrito aos equipamentos dos fabricantes que as criaram.

A aplicação cliente é responsável por anunciar através de pacotes Advertising da tecnologia BLE, o NIF do cliente que a possui.

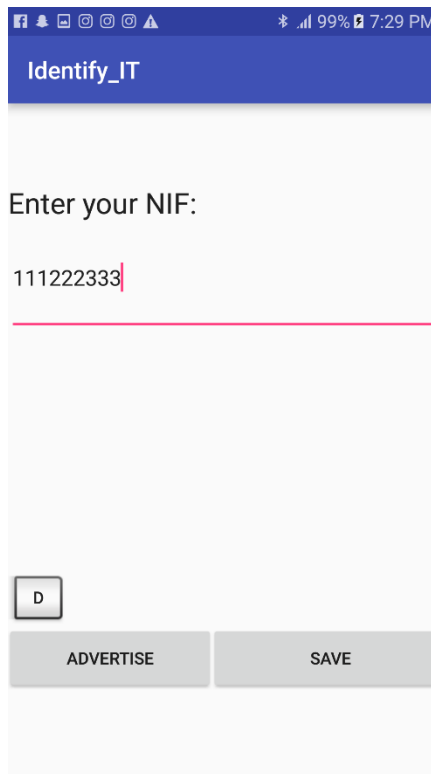


Figura 14 - Aplicação Identify\_IT

### 5.1.2. Aplicação POS (PoScan)

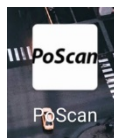


Figura 15 - PoScan Ícone

O módulo POS é o responsável por detetar e identificar o cliente que está a efetuar uma compra. Para que isso seja possível, o POS deverá possuir uma ligação Bluetooth BLE Multi Advertisement, utilizando um chip interno que atualmente está disponível na maior parte dos Smartphones e Tablets. Neste caso, utilizou-se para desenvolvimento o Bluetooth disponível num Tablet Android.

Utilizando POS com capacidade de comunicação BLE Multi Advertisement é, assim, possível que este possa detetar os clientes através desta tecnologia. Assim, o POS irá detetar os clientes e identificar o que estiver a realizar a compra, que será aquele que tiver maior RSSI, e irá associar o seu NIF aos dados da compra.

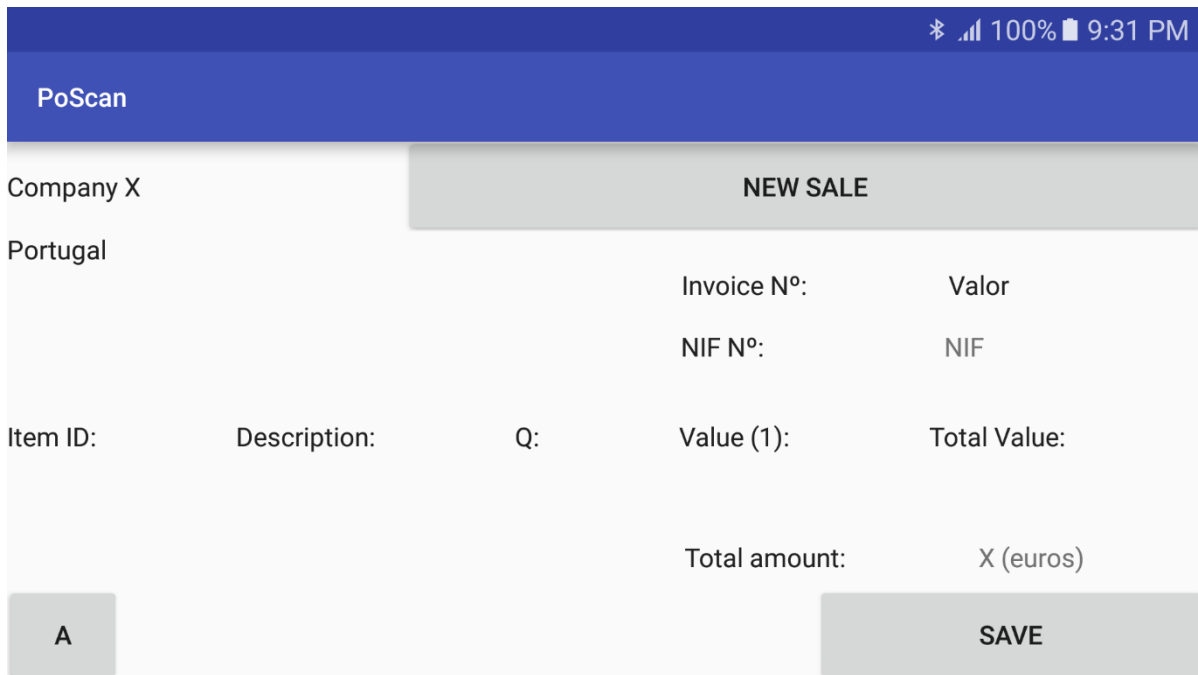


Figura 16 - Aplicação PoScan

### 5.1.3. Midleware MLBS

Para a realização do Midleware(MLBS) foi necessário um estudo bastante mais aprofundado da tecnologia escolhida o Bluetooth LE. A especificação da versão Bluetooth LE é definida como sendo uma tecnologia de comunicação sem fios de curto alcance, muito baixo consumo energético (ULP – Ultra Low Power), com uma pilha protocolar leve e que permite a integração com a tecnologia Bluetooth existente. No próximo subcapítulo irá ser dedicada uma atenção maior a esta tecnologia.

Irá ser dado maior enfase ao seguinte:

- Camada física;
- Camada de ligação;
- Interface Controlador;
- ATT (Attribute Protocol);
- GATT (Generic Attribute Profile);

- GAP (Generic Access Profile).

### 5.1.3.1. BLE – Esquema de Comunicação

Na versão do Bluetooth LE, pode-se verificar que a grande ênfase foi a introdução da componente de baixa energia (LE – Low Energy) acompanhada de novas funcionalidades como [21]:

- Camada física LE;
- Camada de ligação LE;
- Melhoramentos da camada HCI para LE;
- Modo teste direto LE;
- Encriptação AES;
- Melhoramentos da camada L2CAP para LE;
- Melhoramentos da camada GAP para LE;
- Camada ATT (Attribute Protocol);
- Camada GATT (Generic Attribute Profile);
- Camada de gestão de segurança (SM – Security Manager).

A pilha protocolar BLE, representada na figura seguinte, consiste em duas secções principais, que são o controlador (Controller) e o anfitrião (Host). A separação destas duas secções já é conhecida do padrão do Bluetooth BR/EDR. Quaisquer perfis ou aplicações usadas situam-se no topo da pilha protocolar.

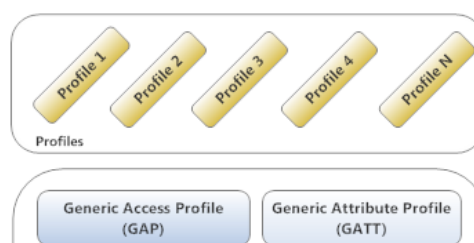
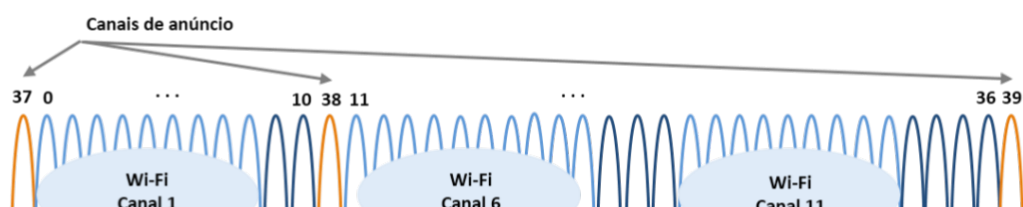


Figura 17 - Pilha protocolar do BLE adaptado [32]

**Camada Física** - O BLE opera na banda de frequências de 2,4 GHz e define 40 canais de rádio frequência (RF – Radio Frequency). Existem dois tipos de canais RF no BLE: canais de anúncios e canais de dados. Os canais de anúncio são três e são usados para descobrir dispositivos, estabelecer conexões e para transmissões broadcast, enquanto os 37 canais restantes de dados são usados para comunicação bidirecional entre os dispositivos conectados.

É usado o mecanismo de espalhamento espectral por saltos em frequência (FHSS – Frequency Hopping Spread Spectrum) nos canais de dados para evitar interferências e problemas de propagação no meio sem fios como desvanecimento (fading) e múltiplos caminhos (multipath).

Este mecanismo seleciona um dos 37 canais disponíveis para comunicação durante um dado intervalo de tempo [18]. O facto de existirem apenas três canais de anúncio torna mais provável a ocorrência da escolha do mesmo canal por parte de outra tecnologia de transmissão, resultando na degradação do sinal. Para combater esse facto, os canais de anúncio do BLE foram cuidadosamente escolhidos de modo a não coincidirem com os canais standard do Wi-Fi. A figura seguinte ilustra o mapeamento das frequências BLE para os canais de dados e de anúncio [22].



*Figura 18 - Coexistência de canais BLE e Wi-Fi adaptado [21].*

**Camada Ligação** - A operação da camada de ligação pode ser descrita em termos de uma máquina de estados que opera em 5 estados distintos, sendo eles: standby, anúncio (advertising), descoberta (scanning), iniciação (initiating) e conexão (connection). Apenas um destes estados está ativo num certo período de tempo. No estado de standby não são transmitidos ou recebidos quaisquer pacotes, e este estado pode ser acedido a partir de qualquer outro estado. No estado de anúncio é possível transmitir pacotes de anúncio para a rede, e há a possibilidade de ouvir e responder a respostas desencadeadas por esses canais de anúncio. Um dispositivo neste estado é chamado de anunciante (advertiser) e este estado pode ser acedido através do estado de standby. A camada de ligação a operar no estado de descoberta escuta os canais de anúncio procurando por pacotes de anúncio vindos de dispositivos anunciantes. Um dispositivo neste estado é chamado de “scanner”, e o estado anterior a este é sempre o de standby. No estado de iniciação ocorre a escuta por pacotes de anúncio vindos de dispositivos específicos, e ocorre a resposta a esses canais de forma a iniciar-se uma ligação com esse dispositivo. Um dispositivo que inicia uma conexão é chamado de iniciador, e transita para este estado vindo do estado de standby. Por fim, o estado de conexão pode ser acedido pelo estado de anúncio ou de iniciação, pois um dos dispositivos estava a anunciar e o outro é que descobriu e iniciou a ligação. Assim, aquando num estado de conexão, dois papéis são definidos ao nível da camada de ligação: mestre e escravo. A um dispositivo que chega ao estado de conexão vindo de um estado de iniciação, é-lhe atribuído o papel de mestre; já o dispositivo que transitou do estado de anúncio para o estado de conexão fica com o papel de escravo. A camada de ligação no papel de mestre comunica com um ou mais dispositivos escravos e define os tempos de transmissão dos dados. Já no papel de escravo, a camada de ligação, comunica apenas com um dispositivo mestre.

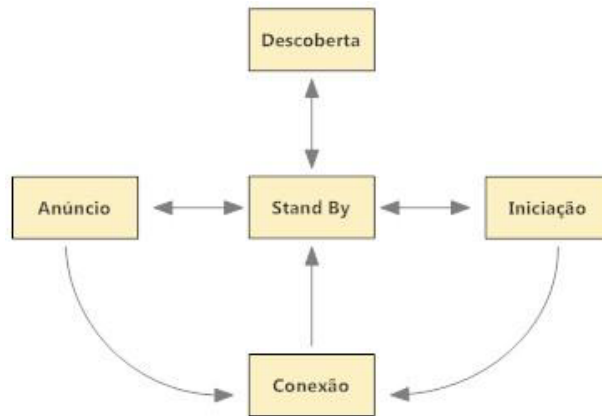


Figura 19 - Mapa de estados BLE adaptado [21]

**Interface Controlador - Anfitrião (HCI)** A camada HCI fornece os meios de comunicação entre a secção controladora (Controller) e a secção anfitriã (Host) através de interfaces padronizadas. Esta camada pode ser implementada quer através de uma API, quer por interfaces de hardware como UART (Universal Asynchronous Receiver/Transmitter), SPI (Serial Peripheral Interface) ou USB (Universal Serial Bus).

**ATT (Attribute Protocol)** - Este protocolo permite expor a outros dispositivos certos componentes dos seus dados, chamados de atributos. Os atributos são estruturas de dados que armazenam informações fornecidas pela camada GATT, que será abordada mais à frente. Um atributo é composto por 4 elementos: 16 bits para a handle que define unicamente um atributo; um UUID (Universal Unique Identifier) de 16 ou 32 bits que define o tipo de atributo; a sua descrição e por fim o seu valor de tamanho variável. No contexto do ATT, um dispositivo que expõe os seus atributos é referido como o servidor e o dispositivo vizinho é o cliente. Os papéis de mestre/escravo atribuído na camada de ligação são independentes dos papéis de cliente/servidor definidos neste protocolo. Por exemplo, um dispositivo mestre tanto pode ser um cliente ou um servidor, e o mesmo acontece com o dispositivo que toma o papel de escravo.

É também possível um dispositivo ser cliente e servidor em simultâneo. O cliente pode aceder aos atributos do servidor através do envio de pedidos, e o servidor, de modo a garantir eficiência, pode enviar ao cliente dois tipos de mensagens não solicitadas contendo os atributos, que são: notificações, onde o servidor envia dados ao cliente e este não confirma a sua receção; ou indicações, que requerem uma confirmação por parte do cliente.

**GATT (Generic Attribute Profile)** - A camada GATT define uma framework para usar os procedimentos da camada ATT para descoberta de serviços e especifica a estrutura dos perfis. Todas as comunicações de dados que ocorrem entre dispositivos numa conexão BLE são processadas através de procedimentos desta camada. No BLE, todos os dados que estão a ser usados para um serviço são chamados de “características”. Uma característica é por sua vez um conjunto de dados que inclui um valor e certas propriedades. Os dados relativos ao serviço e às suas características são guardados em atributos. De forma hierárquica podemos dizer que um perfil pode ter vários serviços e cada serviço pode ter várias características. A definição dos serviços e características está organizada sob a forma de atributos, mapeados numa tabela chamada de tabela de atributos. Como já foi referido, toda esta informação está definida na camada GATT, mais propriamente no dispositivo servidor (GATT Server) pois é neste que estão definidos vários serviços, que como foi já dito são nada mais nada menos que uma coleção de dados para executar uma determinada função, como por exemplo informação obtida de um sensor de temperatura. O dispositivo cliente (GATT Client) tem a hipótese de aceder a estes atributos através de operações de leitura e escrita, consoante as permissões implementadas. Segundo as normas definidas pelo Bluetooth SIG, a definição de um serviço tem como UUID o valor 0x2800 [16]. Todos os atributos seguintes pertencem a este serviço até ser encontrado novamente o mesmo UUID, significando assim o início de um novo serviço. Além disso, o valor deste atributo é outro UUID, mas que neste caso especifica o tipo de serviço que é, ou seja, o primeiro UUID referido diz respeito ao tipo de atributo e serve para delimitar o serviço, já o segundo refere-se ao tipo de serviço (ex. sensor de temperatura, alarme de proximidade

**GAP (Generic Access Profile)** - No nível mais alto da pilha protocolar do BLE situa-se a camada GAP. Esta camada é a interface direta com as aplicações e/ou perfis, sendo também responsável pela especificação dos papéis dos dispositivos, modos para a descoberta de dispositivos e serviços, gestão do estabelecimento e término de ligação e, por fim, a iniciação do processo de segurança. Esta camada opera sempre num destes 4 papéis: broadcaster, observador, periférico ou central. Um dispositivo no papel de broadcaster apenas difunde informação através dos canais de anúncio e não suporta conexões com outros dispositivos. Um dispositivo que é observador é o complemento do broadcaster, ou seja, escuta os anúncios, não tendo também a capacidade de se conectar. Um dispositivo central procura por anúncios e inicia conexões, opera como mestre e pode gerir múltiplas conexões. Por fim, um dispositivo periférico é um anunciador que tem a competência de se conectar e opera como escravo numa conexão simples, ou seja, está ligado a apenas um mestre.

Num sistema BLE típico, o dispositivo periférico anuncia que é um dispositivo pronto a estabelecer uma ligação, para dar conhecimento aos dispositivos centrais. Estes anúncios contêm o endereço único do dispositivo e podem conter dados adicionais como o nome do dispositivo. O dispositivo central, após receber o anúncio, envia ao dispositivo periférico um “Scan request” ao qual este lhe responde com um “Scan response”. Este é o processo de descoberta de dispositivos, na medida em que o dispositivo central passa a saber que o dispositivo com quem comunicou é uma estação periférica e pode assim estabelecer uma ligação. O dispositivo central envia então um pedido de estabelecimento de conexão (Link Request) ao dispositivo periférico, e este responde com um “Link Response”.

### 5.1.3.2. Midleware MLBS

Normalmente numa solução BLE existe um Advertiser que normalmente é um acessório como por exemplo um auricular ou um sensor de pulsação cardíaca e um Discover que normalmente é um Smartphone.



Figura 20 - Esquema do BLE- adaptado [35]

O Discover está permanentemente a enviar pacotes vulgarmente chamado de envio de varreduras, este procedimento faz com que o consumo de bateria seja enorme o que origina uma insatisfação por parte do utilizador. No entanto atualmente estas varreduras são feitas apenas em aplicações proprietárias e destinadas a determinados fins como por exemplo

aplicações para fazer exercício físico. Assim o consumo de energia é atenuado pelo facto de a aplicação apenas ser aberta em determinados momentos.

Para o desenvolvimento do MLBS a primeira preocupação é o consumo de energia, nenhum utilizador utiliza uma aplicação se esta lhe consumir em demasia a bateria do telemóvel. Assim os papéis foram invertidos. Na nossa aplicação o PoS é o Discover ou seja o que consome mais energia, o que não se afigura como sendo um problema grave uma vez que este está ligado à corrente elétrica e o Smartphone é o Advertiser que claramente consome menos energia.

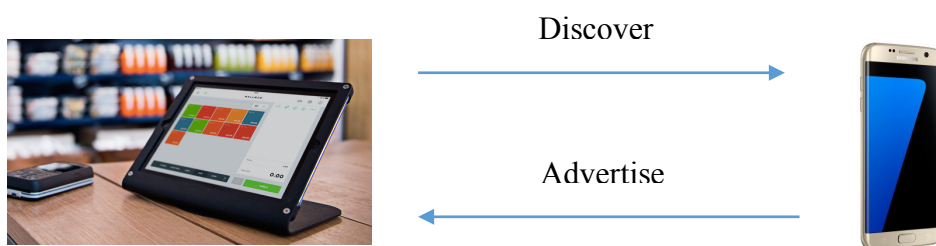


Figura 21 - Esquema de funcionamento da solução

Na figura acima verifica-se então que fizemos uma inversão de papéis e o Smartphone vai funcionar como periférico.

O Middleware MLBS está construído para satisfazer os seguintes requisitos, o Smartphone com a aplicação Identify\_IT funciona como “Advertiser” e vai fazer o seu anuncio e obter as suas respostas. O Tablet com a aplicação PoScan irá funcionar como “Discover” e, portanto, irá estar à escuta. Neste caso então o Smartphone funciona como um periférico(Peripheral).

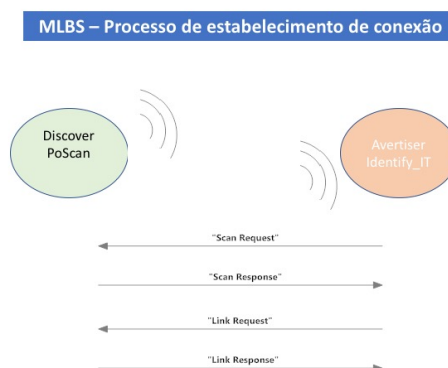


Figura 22 - Processo de estabelecimento de conexão

O Midleware desenvolvido para funcionar em Android, deverá fazer o seu processo de comunicação através de BLE e deverá comunicar fazendo uso das bibliotecas de comunicação através de Bluetooth para Android, na implementação foram definidas as funcionalidades de descoberta(BluetoothLeScanner) e de anúncio(BluetoothLeAdvertiser).

Com o objetivo de aliviar e reduzir o consumo de energia foram utilizadas bibliotecas que permitem o uso de um ScanFilter no processo de Discover, assim podemos seleccionar exactamente que tipo de varreduras estamos a enviar, estes filtros podem ser utilizados no Service UUID, Advertise data e Manufacturer data.

A funcionalidade de anúncio(BluetoothLeAdvertiser) em primeiro lugar adquire o pacote BLE Advertiser do adaptador físico de Bluetooth, de seguida foram definidas as características do modo de Advertiser, nomeadamente (TX\_POWER, LATENCY e Advertise). De seguida foi criado o UUID que identifica os pacotes e O PraceUUID que é convertido num array de Bytes e é aqui que é enviado o NIF.

A funcionalidade de descoberta(BluetoothLeScanner) utiliza um ScanFilter desta forma a aplicação apenas vai responder aos pacotes que interessam.

## ***5.2. Síntese***

Após o levantamento dos requisitos e da especificação da solução no capítulo 4 foram, assim, implementados os módulos: Identify\_IT(Aplicação para Smartphone), PoScan(Aplicação de POS) e MLBS Midleware responsável pelas comunicações.

Analisada a quota de mercado e as necessidades levantadas, nomeadamente, a de compatibilidade de sistemas BLE, optou-se pela utilização do sistema operativo Android.

Desta forma, foi apresentada a implementação da solução proposta: Identify\_IT(Aplicação para Smartphone), PoScan(Aplicação de POS) e a Framework, totalmente desenvolvidas em suporte Android.

Após o desenvolvimento da solução passou-se então à bateria de testes necessários ao funcionamento da implementação proposta.

## 6. Testes

Para o correto funcionamento de uma solução os testes são uma componente fundamental, validando as funcionalidades e capacidades para as quais a solução foi concebida. Iremos então, neste capítulo descrever os testes realizados à solução proposta.

Abordaremos essencialmente os testes ao software constituinte da aplicação de forma a validar o seu correto desenvolvimento e funcionamento, os testes à força de sinal e os testes ao consumo energético da aplicação uma vez que são vitais. A preocupação com a usabilidade da solução efetuada está também presente pelo que são também efetuados testes de usabilidade de forma a comprovar a facilidade de utilização das aplicações, bem como o levantamento de potenciais dificuldades de utilização.

Por fim, foram feitos testes de forma a validar a aceitação junto dos utilizadores relativamente ao conceito desenvolvido pela aplicação desenhada.

### 6.1. Testes ao software desenvolvido

Os testes realizados à utilização do software foram desenvolvidos tendo por base um público-alvo de diversas faixas etárias e de diferentes experiências de utilização de dispositivos móveis. O resultado dos testes efetuados foi recolhido através de observação direta.

Assim num total de 40 utilizadores que experimentaram a solução resumiu-se na tabela seguinte os resultados obtidos:

Tabela 6 - Resumo dos testes à utilização da solução

Faixa etária	Nº utilizadores		Dificuldades Inglês	Identify IT			PoScan			
	M	F		Abrir Aplicação	Preencher NIF	Gravar NIF	Abrir Aplicação	Iniciar Venda	Preencher Campos	Grava Venda
Até 25 anos	6	4	1	10	10	10	10	10	10	10
>25 e >40	8	6	2	14	14	14	14	14	14	14
>40 e >60	4	4	4	7	8	8	7	8	8	8
>60 anos	4	4	7	6	8	8	5	8	8	8

De uma forma geral os utilizadores conseguiram trabalhar com a solução desenvolvida de forma muito satisfatória, verificaram-se alguns entraves com alguns utilizadores por dois motivos essenciais: por um lado as dificuldades com a língua Inglesa e nas faixas etárias mais altas foi notória alguma dificuldade a trabalhar com dispositivos móveis. Estas dificuldades foram ainda mais notórias nas camadas etárias mais elevadas no que diz respeito à motricidade fina.

Nas camadas mais jovens não foi notada qualquer tipo de necessidade de ajuda nem qualquer dificuldade quer a operar com dispositivos móveis ou mesmo com a língua inglesa.

Não foram notadas diferenças substanciais entre o sexo masculino e feminino.

## 6.2. Testes à medição de Sinal

Os testes levados a cabo para a implementação da solução foram, numa primeira fase, realizados na câmara anecoica, propriedade do Departamento de Engenharia Eletrotécnica da Escola Superior de Tecnologia e Gestão de Leiria. A medição de valores de RSSI nesta câmara permitiu verificar, sem interferências, a potência recebida em vários pontos, utilizando dispositivos da marca Samsung com o sistema operativo Android. A figura seguinte mostra a configuração da sala.

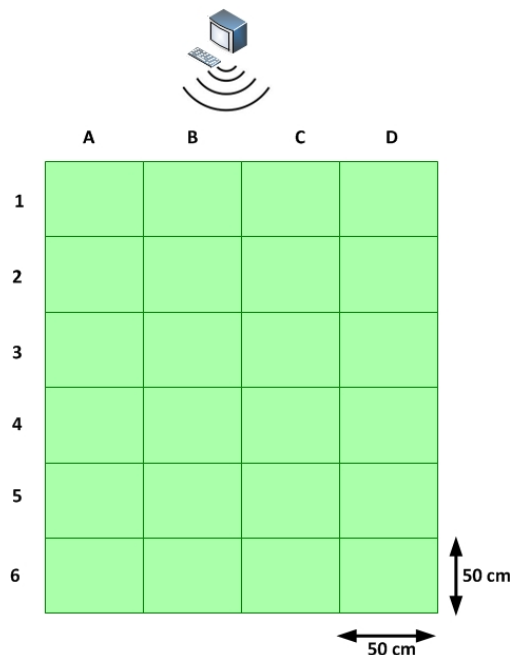


Figura 23- Configuração da sala anecoica

Após a instalação e configuração deste cenário obteve-se uma média da potência recebida em cada ponto da matriz desenhada no chão. Com esses pontos conseguimos constatar uma

referência para as medições em ambiente real, onde vamos estar sujeitos a diversas interferências. As figuras seguintes dizem respeito aos dados recolhidos na amostra sob a forma de gráfico.

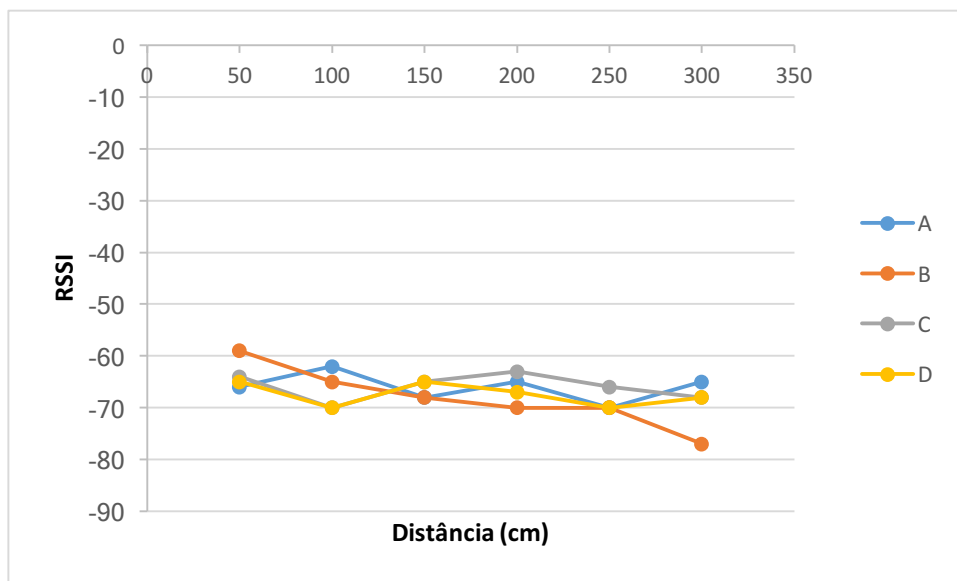


Figura 24 - Dados recolhidos com Smartphone na câmara anecoica

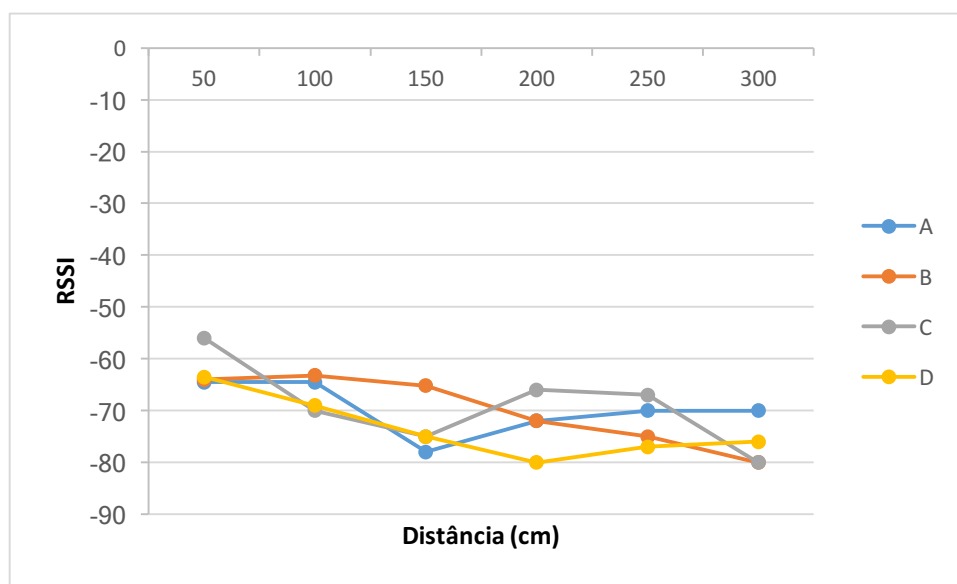


Figura 25 - Dados recolhidos com Tablet na câmara anecoica

Após estas medições de referência podemos observar que, mesmo num cenário onde as interferências do sinal devido a fatores externos eram mínimas, houve uma dispersão de valores. Isto pode ter-se devido ao facto de se terem retirado alguns absorventes do chão da câmara anecoica e, como o chão é de metal, o sinal poderia ter sido refletido e o que estávamos a apanhar na medição não era o sinal direto, mas sim uma refração.

Apesar destes erros, decidiu-se fazer medições em ambiente real. Para isso montou-se o cenário e foram feitas mais medições. Não foram precisas medições no mesmo número das anteriores pois logo no início foi despoletado um facto que levaria à solução do problema. A diferença entre o ponto mais próximo do Discover BLE situa-se próximo dos -45dBm e o ponto conseguinte, em qualquer das direções, próximo dos -58dBm. Esta diferença no RSSI de quase 15dBm é significativa o suficiente para que consigamos com sucesso reconhecer qual o cliente que se encontra mais próximo do terminal de venda.

Assim, definiu-se que conseguimos detetar, no máximo, uma pessoa que se encontra numa área de 60x50cm, o que corresponde sensivelmente à largura dos ombros de uma pessoa média por um comprimento de 50cm. Desta forma, e em conjunto com os resultados dos testes num ambiente mais próximo do real construiu-se o seguinte esquema.

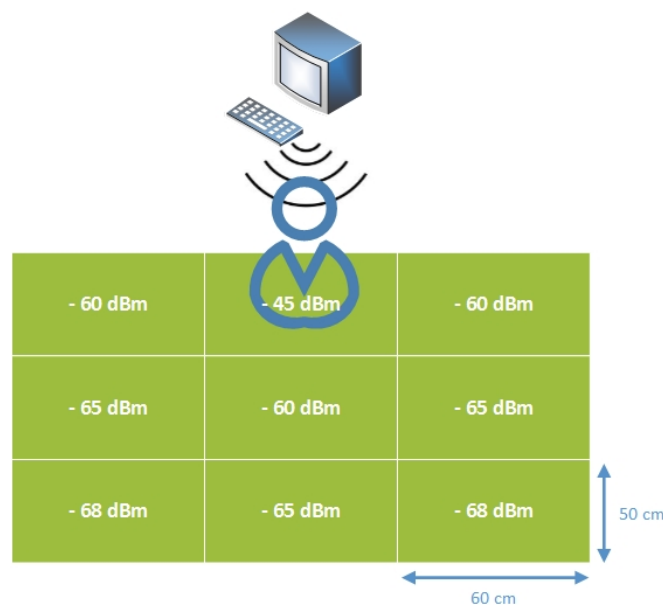


Figura 26 - Esquema de localização de pessoas

No esquema podemos ver de forma clara que se consegue diferenciar um cliente que esteja à frente do PoScan de um outro que esteja ao lado deste pois, em média, a diferença entre o RSSI recebido pelos dois é superior a 15dBm.

No caso de ocorrer um erro na medição o sistema deverá optar sempre pelo cliente com maior RSSI. Estes erros podem ocorrer devido à presença de uma quantidade considerável de obstáculos entre o PoScan e o dispositivo cliente ou devido à presença de objetos metálicos próximo de um deles, o que leva a que ocorram fenómenos de difração e refração nas ondas rádio BLE. Assim, considerando estes fatores, a quantidade de erro que poderá existir no sistema será mínima, uma vez que a diferença média do sinal recebido entre o cliente mais próximo do PoScan e o seguinte da fila é consideravelmente grande, situando-se próximo dos 0,5% o que se traduz num erro na emissão de uma fatura a cada duzentas.

### **6.3. Testes ao consumo energético da aplicação Identify\_IT**

Um dos testes considerados como mais importantes para uma aplicação de Smartphone que deve permanecer sempre aberta ou a funcionar em segundo plano é o teste de consumo de energia.

Para melhor compreendermos o consumo energético da aplicação utilizamos uma aplicação de nome “Ampere” que mede o consumo energético do Smartphone.

Mantendo o Smartphone com a aplicação Identify\_IT ligada e a aplicação “Ampere” em funcionamento verificou-se que ao fim de 5 horas o consumo energético foi de 2% o que se afigura como completamente irrelevante para a solução proposta.

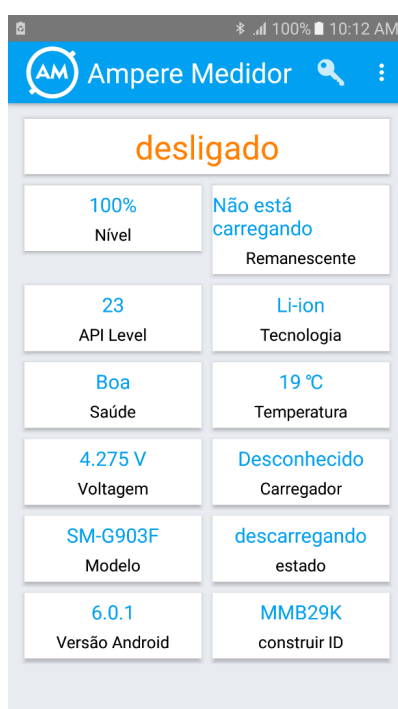


Figura 27 - Medição de consumo de energia inicial



Figura 28 - Medidor de consumo de energia final.

Conforme pode ser confirmado pelas figuras 19,20 o consumo ao fim de sensivelmente 5 horas é realmente reduzido. O que transforma um teste vital para a solução proposta como um teste bem-sucedido.

#### ***6.4. Testes de aceitação da solução desenhada.***

Por fim, com o objetivo de percebermos a utilidade da aplicação junto dos utilizadores foi feita uma entrevista verbal aos 40 utilizadores que participaram nos testes. Houve unanimidade relativamente ao interesse e à pertinência da solução proposta, no entanto cerca de 20% dos utilizadores não se mostraram preocupados ou necessitados de se identificarem no momento da realização da compra de um jornal, ou café, ou o pagamento de um estacionamento.

De facto este aspeto foi de certo modo inesperado não por questões de privacidade uma vez que não foram tratadas nesta dissertação, mas sim pelo desinteresse em fazer algumas compras sem identificação. Não obstante, o trabalho mantém-se inabalável pela sua pertinência e pelo valor acrescentado que pode trazer às áreas de engenharia e de gestão de empresas.

## **6.5. Síntese**

Após efetuada o conjunto de testes descrito neste capítulo, observa-se que relativamente à utilização do software desenvolvido, esta afigura-se simples mesmo estando o software desenvolvido em inglês. Os utilizadores não apresentaram dificuldades e quando surgiram dúvidas rapidamente as superaram.

No caso dos testes à força de sinal apesar de estes parecerem conclusivos não nos podemos esquecer que foram feitos com apenas um modelo de Smartphone e Tablet, o que significa que a força de sinal pode mudar dependendo do aparelho usado e do chip de Bluetooth incorporado.

Os testes ao consumo de energia são, no entanto mais conclusivos e neste caso apresentam valores de consumo que podem ser considerados mínimos.

Quanto à aceitação da solução claramente que verificamos que dependia do utilizador/comprador e do seu perfil enquanto cidadão e enquanto comprador.

No próximo capítulo iram ser retiradas as conclusões do trabalho desenvolvido e feita uma análise ao trabalho futuro.

## **7. Conclusões e Trabalho Futuro**

---

### **7.1. Conclusões**

O objetivo final deste projeto era definir uma solução que permitisse a transmissão dos dados (NIF) que identificassem um utilizador/comprador de forma automática e sem necessidade de intervenção do próprio no ato da realização de uma transação comercial. Esta transmissão de dados teria de ser feita com recurso a tecnologias sem fios.

Tornou-se ainda objetivo do trabalho simplificar as tarefas a realizar por parte do vendedor e permitir que essas tarefas fossem realizadas sem necessidade da presença do vendedor por exemplo através de uma máquina de Vending, desta forma resolve-se o problema de um utilizador/comprador obter um documento de venda destas máquinas de venda com identificação fiscal.

Para atingir os objetivos propostos, foi elaborada uma pesquisa às soluções existentes na área, bem como uma pesquisa conceptual às tecnologias inerentes, apresentadas no capítulo 2 e 3 respetivamente do presente documento. Foram ainda levantados requisitos funcionais e não funcionais para a arquitetura proposta; os mesmos foram validados através do recurso a entrevistas, dando posteriormente azo à elaboração de uma arquitetura modular de alto nível apresentada no capítulo.

A arquitetura especificada consiste, de forma sumária, num conjunto de aparelhos móveis wireless que se vão anunciar entre si e fazer a troca de informações necessárias para a realização de uma troca comercial. As vantagens desta abordagem prendem-se com o facto de por um lado reduzir de forma significativa o tempo de espera para a identificação de um cliente e a realização de uma venda e por outro lado permitir que em locais onde não exista intervenção humana se possam obter documentos de venda com identificação fiscal.

Dos testes realizados, conclui-se que a solução desenvolvida é viável uma vez que estes obtiveram resultados satisfatórios abrindo assim uma nova janela de investigação e a possibilidade de desenvolvimento de trabalho futuro.

Da realização deste projeto resulta uma clara vantagem para o cliente uma vez que cada vez mais os benefícios fiscais são concedidos aos clientes que façam as suas transações comerciais e que identifiquem o seu número de identificação fiscal. De salientar ainda que não só a área da engenharia beneficia com este projeto, mas também a área da gestão de empresas/fiscalidade saem beneficiadas com a realização deste projeto.

## **7.2. Trabalho Futuro**

Olhando um pouco para o trabalho desenvolvido e o futuro, está claramente identificado um primeiro passo, assim a continuidade deste trabalho passará pelo levantamento de requisitos com base ao desenvolvimento de uma solução mais poderosa em termos de comunicação, nomeadamente a criação de um Custom Profile BLE que permita o desenvolvimento de comunicação mais poderoso e com mais capacidade de envio de dados.

Dever-se-á ainda olhar com especial atenção para o hardware de suporte nomeadamente à compatibilidade de soluções de descoberta de pacotes Bluetooth BLE. Não esquecendo ainda o desenvolvimento de soluções para outras plataformas, iOS, Windows Phone etc.

A problemática da força de sinal merece também uma melhoria bem como uma bateria de testes baseada num conjunto mais vasto de equipamentos móveis.

Também de ser efetuado um estudo de envio das informações para servidores WEB e ou Servidores de entidades Fiscais Por fim a criação de uma aplicação móvel que permita ao utilizador/comprador aceder aos seus documentos de compra online.

## Bibliografia

- [1] V. C. Jürgen Bohn, M. Langheinrich, F. Mattern e M. Rohs, “Disappearing Computers Everywhere – Living in a World of Smart Everyday Objects,” *Institute for Pervasive Computing, ETH Zurich, Switzerland*.
- [2] R. B. d. Araujo, “Computação Ubíqua: Princípios, Tecnologias e Desafios,” em *XXI Simpósio Brasileiro de Redes de Computadores*.
- [3] C. E. Cirilo, “Computação Ubíqua: definição, princípios e tecnologias”.
- [4] M. Weiser e J. S. Brown, “Designing Calm Technology,” 1995.
- [5] A. D. R. Portuguesa, “Lei n.º 36/2011”.
- [6] T. G. Zimmerman, “Personal Area Networks: Near-field intrabody communication,” *IBM Systems Journal*, vol. 35, 1996.
- [7] P. R. T. G. Z. Don Coppersmith, “System and method for near-field human-body coupling for encrypted communication with identification cards”. Patente US5796827 A, 18 Ago 1998.
- [8] D. Z. Creemer, “Identifying client patterns using online location-based derivative analysis”. USA Patente US20110171976 A1, 14 Jul 2011.
- [9] R. Campos e M. Ricardo, “Autoconfiguration and Self-management of Personal Area Networks: a New Framework,” *Wireless World*, 2004.
- [10] J. F. M. Carvalho, “Localização de Dispositivos Móveis em Redes Wi-Fi,” 2007.
- [11] J. Letchner, D. Fox e A. LaMarca, “Large-Scale Localization from Wireless Signal Strength,” *National Conference on Artificial Intelligence (AAAI)*, 2005.
- [12] G. Jekabsons, V. Kairish e V. Zuravlyov, “An Analysis of Wi-Fi Based Indoor Positioning Accuracy,” *Scientific Journal of Riga Technical University Computer Science. Applied Computer Systems*, vol. 47, 20011.
- [13] V. Coskun, B. Ozdenizci e K. Ok, “A Survey on Near Field Communication (NFC) Technology,” *Sensors Journal*.
- [14] S. Burkard, “Near Field Communication in Smartphones”.
- [15] B. Dodson, H. Bojinov e M. S. Lam, “Touch and Run with Near Field Communication (NFC),” *Computer Science Department*.

- [16] M. D. S. S. A. Mrs. Pratibha Singh, "A Modern Study of Bluetooth Wireless Technology," *International Journal of Computer Science, Engineering and Information Technology (IJCEIT)*, vol. Vol.1, August 2011.
- [17] P. Singh, D. Sharma e S. Agrawal, "A Modern Study of Bluetooth Wireless Technology," *Dept. of Computer sci. & Eng. Raipur, (Chhattisgarh)*.
- [18] Paypal. [Online]. Available: <http://www.slideshare.net/few/pay-pal-beacon-and-apple-ibeacon>.
- [19] D. a. Rezende, *Engenharia de Software e Sistemas de Informação*, 3ª ed., Brassport Multimédia Ltda., 2003.
- [20] J. Y. Zhou, "Functional Requirements and Non-Functional Requirements: A Survey," Montreal - Canada, 2004.
- [21] A. F. P. Barbosa, "Design Thinking na Especificação de Requisitos," 2016.
- [22] S. P. DEZERBELLES, "A IMPORTÂNCIA DA ANÁLISE DE REQUISITOS NODESENVOLVIMENTO DE SOFTWARES," Cabo Frio, 2008.
- [23] B. SIG, "Bluetooth Core Specification 4.2," July 2015. [Online]. Available: <https://www.bluetooth.com/specifications/adopted-specifications>.
- [24] J. Decuir, ""Bluetooth 4.0 : Low Energy",".
- [25] F. Marteli, "BLUETOOTH LOW ENERGY," 2011.
- [26] M. Habbal, "Bluetooth Low Energy – Assessment within a Competing Wireless World," 2011.
- [27] N. Semiconductor, "nRF8001 single chip Bluetooth low energy solution," 2008.
- [28] J. Leonard, "Nordic Semiconductor technical article".
- [29] A. H. V. F. J. G. ROY WANT, "The Active Badge Location System," 1992.
- [30] A. J. A. H. Andy Ward, "A New Location Technique for the Active Office," 1997.
- [31] A. K. L. M. H. B. S. T. Nissanka B. Priyantha, "The Cricket Compass for Context-Aware Mobile," MIT Laboratory for Computer Science, 2000.
- [32] SnapTrack, "Location Technologies for GSM, GPRS and UMTS Networks," 2003.
- [33] P. Bahl, "RADAR: an in-building RF-based user location and tracking system," *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, 2000.

- [34] P. Krishnan, "A system for LEASE: location estimation assisted by stationary emitters for indoor RF wireless networks," *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, 2004.
- [35] T. Instruments, "Texas Instruments," 2015.
- [36] W. Integrated, "Wireless Integrated," [Online]. Available:  
<http://www.wirelessintegrated.com/wp-content/uploads/2013/04/bluetooth-low-energy-sticker1.png>.