Faculdade de Engenharia da Universidade do Porto

Tecnologias de apoio à monitorização de fluxos de pessoas e controlo de acessos

João Augusto Pinho da Costa das Neves Viana

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

Major Telecomunicações

Orientador: Prof. Dr. José António Ruela Simões Fernandes

Co-orientador: Eng. Filipe Sousa

Fevereiro de 2009

Resumo

A presente tese incide sobre o trabalho realizado no âmbito da dissertação do Mestrado Integrado em Engenharia Electrotécnica e de Computadores, subordinada ao tema “Tecnologias de apoio à monitorização de fluxos pessoas e controlo de acessos”.

Trata-se de uma solução de controlo de acessos a áreas extensas onde possa haver necessidade de segmentação das mesmas. A solução tem uma apetência natural para a utilização de tecnologias sem fios mas, apesar disso, não se restringe às mesmas.

Podem ser encontradas neste trabalho descrições das mais recentes tecnologias e soluções na área de monitorização e controlo de acessos, assim como detalhes sobre tecnologias de telecomunicações que serviram de base para o trabalho.

Após esta introdução ao estado da arte é caracterizado e detalhado o modelo de forma a fazer face aos requisitos inicialmente propostos. Os algoritmos utilizados, conceitos de funcionamento e módulos constituintes do modelo são abordados nessa fase do trabalho.

Posteriormente, e devido à sua dimensão, foi escolhido um segmento fulcral do modelo, detecção de fluxos de pessoas, para implementação com o intuito de validar o conceito.

Finalmente apresenta-se um conjunto de testes que permitiram avaliar a eficácia do algoritmo implementado.

Abstract

The present thesis entitled “Support technologies for monitoring the flow of people and access control” describes the work carried out to obtain the Master of Science degree in Electrical and Computer Engineering.

The proposed access control solution is designed for controlling wide areas where there might be a need for segmentation. The use of wireless technologies is a natural choice for this environment, but the solution is not constrained by this choice.

The description of the most recent technologies and solutions in access control and monitoring can be found in this text, as well as details about the main telecommunications’ technologies that were used as a basis for the work.

After the introduction to the state o the art, the model is characterized and detailed taking into account the initially proposed requirements. At this stage, the algorithms used, the operational concepts and the operating modules are presented.

For the purpose of concept validation, the core part of the model (access monitoring) was selected for implementation.

Finally, a set of tests used to assess the performance of the implemented algorithm is presented, and is followed by a discussion of the results.

Agradecimentos

Em primeiro lugar a minha palavra de apreço aos orientadores do trabalho, Professor José Ruela e Eng. Filipe Sousa pela disponibilidade e apoio, contribuindo para um melhor nível de qualidade deste trabalho.

Gostaria também de agradecer ao meu pai, Marinho João, à minha mãe, Maria Arminda ao meu irmão, António Rui, e à minha esposa, Tami Itabashi, pelo apoio incondicional e constante incentivo, tornando este trabalho possível.

Obrigado a todos os meus amigos, em especial ao Amílcar Correia, Marc Antunes, Miguel Caetano e Daniel Sousa, que sempre me encorajaram e apoiaram, principalmente nas alturas de maior desânimo.

A todos, muito obrigado…

Aos meus pais, ao meu irmão e à Tami.

Conteúdos

Lista de figuras

Lista de tabelas

Abreviaturas e Símbolos

AP Access Point

ASCII American Standard Code for Information Interchange, norma universal para a representação de caracteres alfanuméricos, pontuação e caracteres de controlo.

CRC Cyclic Redundancy Check. Código detector de erros amplamente usado em comunicações digitais para verificar integridade de uma mensagem.

DS Distribution System

EAS Electronic Article Surveillance

ERP Effective Radiated Power

GPS Global Positioning System

IEC International Electrotechnical Commission, organização internacional, não governamental e sem fins lucrativos, que prepara e publica normas internacionais referentes a tecnologia eléctrica, electrónica e relacionadas.

ISM Industrial Scientific Medical

ISO International Organization for Standardization, organização não governamental constituída por representantes de institutos nacionais de normalização de 158 países.

MAC Medium Access Control

NRZ Non Return to Zero. Código de linha.

PCB Printed circuit board

RFID Radio Frequency IDentification, refere-se a uma tecnologia rádio que envolve emissores chamados *tags* que emitem informação, captada por dispositivos designados leitores.

RSSI Received Signal Strength Indicatior

RTLS Real Time Location System. Sistema de localização em tempo real.

RZ Return to Zero. Código de linha.

SRD Short Range Devices

WDS Wireless Distribution System

WLAN Wireless Local Area Network

XML eXtensible Markup Language, linguagem usada para descrever uma estrutura de dados.

Glossário

Checksum	valor usado para testar a integridade dos dados recebidos. Esse valor é calculado com base no valor dos dados enviados.
Datacarrier	termo genérico, frequentemente usado pela empresa SKIDATA, que designa um “portador de dados” que dependendo da tecnologia é aplicado a códigos de barras, bandas magnéticas e *tags* RFID, activas, passivas ou semi-passivas.
Ethernet	nome por que é conhecida a norma IEEE 802.3, para LANs com fios. Uma nova versão surgiu depois, a Ethernet II ou DIX, mas a designação é usada indistintamente para ambas.
Handshake	Do inglês “aperto de mão”, designa a transmissão que ocorre no início da sessão. O “aperto de mão” assegura que os dois processos, tipicamente executados em máquinas diferentes, concordam com o modo como a transmissão se irá desenrolar.
Manchester	Codificação de sequências binárias em símbolos. Código de linha bifásico.
Mesh	rede emalhada; os nós de uma rede estão ligados entre si de maneira a que exista redundância nas ligações.
Miller	Codificação de sequências binárias em símbolos. Também conhecida como codificação em atraso.
RS232	é uma especificação da interface física para transmissão em série da *Electronic Industries Association* (EIA).
Socket	Objecto de software que permite ligar uma aplicação a dispositivo físico ou lógico.
Wi-Fi	marca licenciada originalmente pela Wi-Fi Alliance para descrever a tecnologia de redes sem fio (WLAN) baseadas na norma IEEE 802.11. Opera em faixas de frequências que não necessitam de licença para instalação e/ou operação.

Capítulo 1

1. Introdução

Actualmente utilizamos controlo de acessos ou simplesmente monitorização de fluxos diariamente, normalmente sem nos apercebermos. Cada vez que entramos em transportes públicos, eventos desportivos ou culturais, estacionamos o nosso veículo num parque ou até ao entrarmos no nosso local de trabalho, estamos na presença de sistemas de controlo de fluxo e/ou de acessos. A evolução da tecnologia tem sido a grande responsável pela automatização dos processos nesta área, primeiro com código de barras e agora recorrendo a tecnologias sem fios.

A automatização na área de controlo de acessos e a sua interligação com Sistemas de Informação acarreta várias vantagens não só para o utilizador, simplificando e tornando transparentes os processos, mas também para quem implementa baixando os custos em pessoal e minimizando a fraude. A “Via Verde” é um exemplo ilustrativo de como o controlo de acessos a uma rede de auto-estradas pode ser simplificado, tornando o processo completamente transparente para o utilizador. A interligação entre Sistemas de Informação e controlo de acessos é de suma importância no combate à fraude no acesso a recintos desportivo, retirando o factor humano e obrigando o utilizador a identificar-se perante o sistema. Por último, os dados recolhidos pelo sistema de controlo de acessos são extremamente valiosos para a empresa que o implemente. Tomando como exemplo, o sistema de transportes público, é possível optimizar o número de veículos e cadência dos mesmos, partindo de uma análise de afluência de utilizadores.

Por outro lado, sistemas de localização em tempo real têm tido grandes desenvolvimentos com a tecnologia GPS. No entanto no campo de controlo de acessos tem vindo a ser pouco utilizada devido à impossibilidade do seu uso dentro de edifícios. Para colmatar estas lacunas têm vindo a ser desenvolvidas soluções baseadas em tecnologias sem fios, mas sem aplicação generalizada.

1.1 Motivação

A motivação deste trabalho advém da tentativa de criar um sistema de controlo de acessos ou monitorização de fluxos, versátil, simples, configurável e aberto. Estão previstas duas formas de implementação, implementar uma qualquer parte da estrutura do sistema, de forma a interagir com software de terceiros, ou implementar os sistemas integralmente.

O sistema pretende ser um híbrido entre um sistema de controlo de acessos e um sistema de localização em tempo real. Devido aos avanços da tecnologia de redes de computadores, esta solução pretende afastar o processamento de dados dos equipamentos terminais (pontos de acessos) e transferi-lo para montante.

1.2 Objectivos e especificação do problema

Com este trabalho pretende-se desenvolver um modelo de contabilização do fluxo de acessos de pessoas e veículos e, quando aplicável, de accionamento de barreiras físicas de forma a impedir o acesso.

A proposta impõe também os seguintes pré requisitos:

- Pontos de acessos que detectem a direcção do acesso e pelo menos nove *datacarriers* em simultâneo.
- Os locais de instalação de pontos de acesso com um máximo de dez metros de largura.
- O sistema tem de ser configurável, modular e adaptável. A versatilidade e a abertura do sistema também devem ser tidas em conta, podendo o modelo interagir com software de terceiros.
- Os pontos de acesso podem estar distanciados das unidades de processamento de acessos até 10 km.
- A área a controlar pode exceder os 5 km, podendo conter túneis.
- A solução deverá estar preparada para funcionar em ambientes hostis, por exemplo estaleiros de construção civil, estaleiros navais ou minas.
- Em caso de emergência deve ser gerado um alarme e haver informação da última localização.

1.3 Estratégia adoptada

Depois do estudo das tecnologias sem fios mais disseminadas e avaliação do seu estado de desenvolvimento foi possível optar por uma tecnologia. A escolha foi baseada em critérios como custo, disponibilidade e vocação inerente da tecnologia para o propósito em causa. O estudo incidiu sobre tecnologias como Wi-Fi (IEEE 802.11), Bluetooth, ou ZigBee (operando sobre IEEE 802.14.5) e RFID.

Dados os requisitos acima, a solução tende a ser vocacionada para a utilização de tecnologia RFID activa mas não limitada por esta.

A solução desenvolvida não se deve restringir ao controlo de acessos tradicional a um recinto, mas deve optar por uma aproximação mais granular, dividindo o recinto a controlar em zonas, separadas por *bottlenecks* com pontos de acesso.

O modelo desenvolvido é de natureza modular, criando camadas de abstracção de forma a tornar a implementação, a partir de um certo nível, independente do hardware utilizado e tornando possível a substituição de elementos com o mínimo de desenvolvimento adicional.

1.4 Estrutura da tese

Esta tese encontra-se dividida em 6 capítulos, cada um dos quais dividido em secções que abordam diferentes tópicos relativos ao título de cada um dos capítulos.

Neste primeiro capítulo, introdutório ao presente trabalho, faz-se menção aos objectivos propostos e é delineada uma estratégia para os atingir.

O segundo capítulo é dedicado ao estado da arte e incide principalmente nas tecnologias sem fios utilizadas em controlo de acessos, é dado particular ênfase à tecnologia RFID. Também neste capítulo são descritas outras tecnologias de telecomunicações que servem de base ao trabalho desenvolvido. É nesta fase que a escolha de tecnologia é fundamentada.

O terceiro capítulo debruça-se sobre soluções de controlo de acessos e soluções de localização já existentes no mercado. Na descrição das soluções é dado especial realce aos princípios de funcionamento e tecnologias utilizadas.

O quarto capítulo incide directamente na especificação do modelo a desenvolver. São apresentados os conceitos que servem de base aos algoritmos, os constituintes lógicos do modelo e definem-se interfaces entre módulos. Apresenta também propostas de *hardware* para implementação do modelo.

O quinto capítulo é dedicado à implementação e testes de uma peça fulcral do modelo, a monitorização de fluxo de pessoas. É criado um cenário de testes de forma a validar o conceito e avaliar a robustez do algoritmo e análise crítica dos resultados obtidos.

O sexto e último capítulo é dedicado às conclusões finais. É feita uma análise do trabalho realizado face aos objectivos propostos e são sugeridos possíveis melhoramentos futuros.

Capítulo 2

2. Estado da arte

Neste capítulo apresentar-se-á uma descrição das características de algumas tecnologias usadas em controlo de acessos, focando a atenção nos pormenores mais pragmáticos das tecnologias.

2.1 RFID

RFID é um acrónimo para *Radio Frequency IDentification*, isto é, identificação por radiofrequência. Foi inspirada inicialmente no conceito de reflexão da tecnologia de radar e dinamizada por várias patentes no início dos anos 50 do século XX.

Inicialmente pensado para substituir códigos de barras no rastreio de itens em cadeias de produção, a utilização da tecnologia tem vindo a expandir-se, sendo agora aplicada nos mais variados contextos, principalmente devido ao aumento do alcance e capacidade de memória.

Um sistema RFID é constituído tipicamente por *tag* (*transponder*), leitor (interrogador), estando uma antena (dispositivo de acoplamento) associada a cada um dos equipamentos. O leitor tipicamente está ligado a equipamentos com maior capacidade de processamento, de forma a processar os dados e executar os procedimentos necessários.

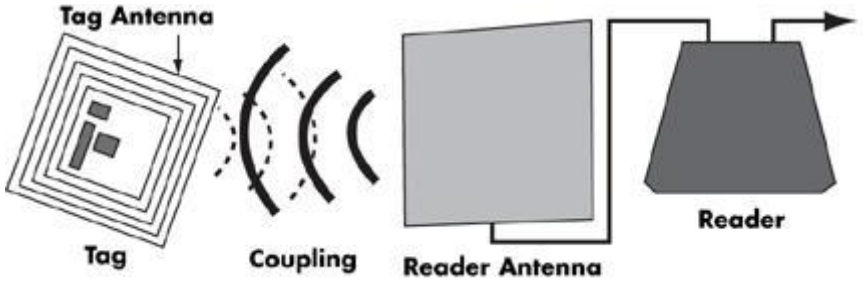

Figura 2-1 – Ligação típica entre leitor, *tag* e antenas(1)

2.1.1 Tags

As *tags* tipicamente são categorizadas pela forma como obtêm a potência para funcionar. As *tags* inicialmente desenvolvidas foram as *tags* passivas, que obtêm a energia para o funcionamento integralmente da energia radiada pelo leitor. Esta potência é utilizada para o processamento dos dados recebidos, escrita em memória (se aplicável), modulação e retorno de dados para o leitor. Pode ser visto na Figura 2-2 um modelo simplificado do funcionamento deste tipo de *tags*.

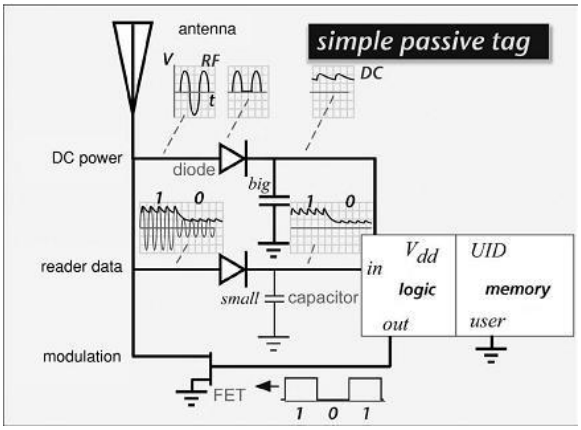

Figura 2-2 – Representação esquemática de uma *tag* passiva(2)

Ao contrário das anteriores, nas *tags* semi-passivas, todo o circuito de processamento é alimentado por uma bateria interna, sendo a energia recebida do leitor utilizada pela interface rádio no processo de transmissão. Esta configuração apresenta duas vantagens importantes. A primeira reside no aumento do alcance, visto que não é utilizada a potência recebida no processamento de dados e a segunda na possibilidade de incorporar sensores na *tag*, podendo esta recolher dados mesmo não estando na presença de um leitor. Esta última característica pode ser de extrema mais-valia se, por exemplo, o item a ser rastreado for um bem alimentar degradável.

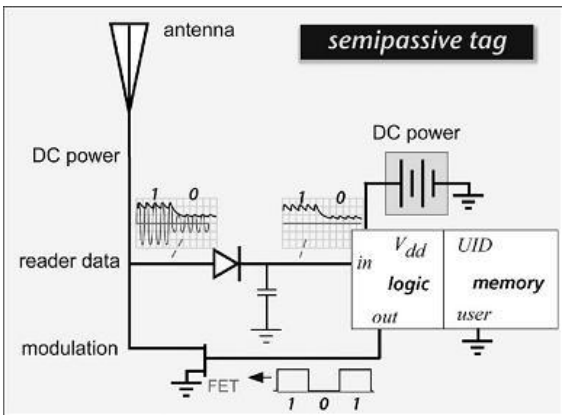

Figura 2-3 – Representação esquemática de uma *tag* semi-passiva(2)

As *tags* activas destacam-se por possuírem a bateria interna que alimenta tanto a interface rádio como o circuito de processamento, não dependendo da energia radiada pelo leitor. Ao contrário dos dois tipos de *tags* anteriores, cujo alcance tipicamente se situa na ordem dos centímetros ou poucos metros, as *tags* activas têm alcances que chegam aos 100 metros; a capacidade de recolher dados por intermédio de sensores das *tags* semi-passivas é mantida. Devido ao acréscimo de potência na interface rádio também são capazes de implementar protocolos de comunicação mais complexos. Embora esteja especificado que pode existir

comunicação entre *tags* (EPC *Class* 4), esta funcionalidade não é consensual na literatura e raramente implementada; neste caso deixaríamos de estar a falar de *tags* e entraríamos no âmbito das redes de sensores.

Torna-se importante ressalvar aqui a existência de dois tipos de *tags* activas; *transponders* e *beacons*. Nas primeiras a comunicação é sempre iniciada pelo leitor e a *tag* apenas responde quando interrogada. No segundo caso a *tag* está sempre a transmitir, com uma cadência predefinida pelo fabricante ou programada (se a *tag* o permitir).

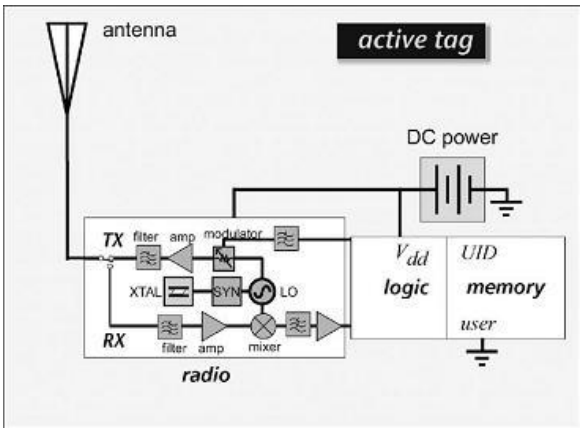

Figura 2-4 – Representação esquemática de uma *tag* activa(2)

2.1.2 Leitores

Os leitores RFID podem incorporar a antena ou utilizar antenas externas como exemplificado na Figura 2-5 e na Figura 2-6. A informação recolhida da *tag* é encapsulada e fornecida para montante no sistema RFID das mais variadas formas. Os leitores mas banais oferecem interfaces seguindo as normas RS232, RS485 ou *Wiegand*.

Figura 2-5 – Leitor RFID com antena incorporada

Figura 2-6 - Leitor RFID com antena externa

2.1.3 Frequências utilizadas

As frequências de operação em RFID são as disponibilizadas para aplicações ISM (*Industrial Scientific Medical),* ou então para SRD (*Short Range Devices)*. Ambas as gamas de frequências têm associadas limitações de potência de forma a mitigar interferências.

A escolha das frequências utilizadas está intrinsecamente ligada à utilização prevista para o sistema. Por exemplo, frequências baixas têm maior poder de penetração em água e objectos, enquanto frequências mais altas transportam mais informação e tipicamente têm maior alcance.

A tabela abaixo ilustra as gamas de frequências utilizadas em RFID e a respectiva potência de transmissão admitida.

Tabela 2-1 – Tabela das frequências usadas por sistemas RFID (Agosto 2006)(3)

Frequency ranges for RFID-Systems		
frequency range	comment	allowed fieldstrength / transmission power
< 135 kHz	low frequency, inductive coupling	72 dBµA/m max
3.155 ... 3.400 MHz	EAS	13.5 dBµA/m
6.765 .. 6.795 MHz	medium frequency (ISM), inductive coupling	42 dBµA/m
7.400 .. 8.800 MHz	medium frequency, used for EAS (electronic article surveilance) only	9 dBµA/m
13.553 .. 13.567 MHz	medium frequency (13.56 MHz, ISM), inductive coupling, wide spread usage for contactless smartcards (ISO 14443, MIFARE, LEGIC, ...), smartlabels (ISO 15693, Tag-It, I-Code, ...) and item management (ISO 18000-3).	60(!) dBµA/m
26.957 .. 27.283 MHz	medium frequency (ISM), inductive coupling, special applications only	42 dBµA/m
433 MHz	UHF (ISM), backscatter coupling, rarely used for RFID	10 .. 100 mW
865 .. 868 MHz	UHF (RFID only), Listen before talk	100 mW ERP Europe only
865.6 .. 867.6 MHz	UHF (RFID only), Listen before talk	2W ERP (=3.8W EIRP) Europe only
865.6 .. 868 MHz	UHF (SRD), backscatter coupling, new frequency, systems under developement	500 mW ERP, Europe only
902 .. 928 MHz	UHF (SRD), backscatter coupling, several systems	4 W EIRP - spread spectrum, USA/Canada only
2.400 .. 2.483 GHz	SHF (ISM), backscatter coupling, several systems,	4 W - spread spectrum, USA/Canada only
2.446 .. 2.454 GHz	SHF (RFID and AVI (automatic vehicle identification))	0.5 W EIRP outdoor 4 W EIRP, indoor
5.725 .. 5.875 GHz	SHF (ISM), backscatter coupling, rarely used for RFID	4 W USA/Canada, 500 mW Europe

2.1.4 Modelação e codificação

De forma análoga a outros sistemas de comunicação, a comunicação entre *tag* e leitor pode ser *full-duplex*, em que ambos os equipamentos transmitem simultaneamente, ou *half-duplex*, em que os equipamentos ocupam o meio alternadamente. A utilização de uma ou outra forma está inerente ao tipo de modulação e tecnologia usada.

Quanto ao acesso ao meio e modulação da onda electromagnética, existem várias abordagens, consonante a tecnologia utilizada, capacidade de processamento e energia disponível. As modulações digitais utilizadas variam entre OOK (On-off keying), ASK (Amplitude-shift keying), FSK (Frequency-shift keying), PSK (Phase-shift keying) ou QAM (Quadrature Amplitude Modulation). Consoante a escolha podemos obter mais ou menos imunidade ao ruído,

largura de banda, propensão à distorção ou robustez com diferentes condições de propagação. É de ressalvar que devido ao facto de conterem uma bateria, as *tags* activas têm mais energia disponível, logo são capazes de implementar modulações mais complexas.

Da mesma forma, as codificações utilizadas, que especificam a forma como os bits são representados por sinais a transmitir, incluem tipicamente RZ, NRZ , Manchester e Miller.

2.1.5 Acoplamento

Existem dois tipos principais de acoplamento, reflectivo (*backscatter*) e indutivo. O acoplamento indutivo baseia-se na geração de um campo magnético através de uma bobine para fornecer energia e passar informação à *tag*. A *tag* responde recorrendo a uma alteração de frequência ou em alguns casos armazenando energia num condensador interno e respondendo na mesma frequência depois de o leitor deixar de emitir. De notar que este tipo de acoplamento é usado em *tags* passivas e o seu alcance encontra-se tipicamente na ordem dos centímetros. A Figura 2-7 ilustra este processo.

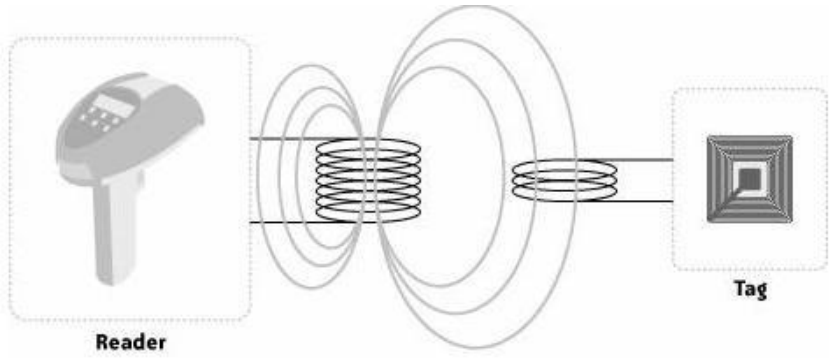

Figura 2-7 – Exemplo de um acoplamento indutivo

O acoplamento radiativo como o próprio nome indica baseia-se na reflexão da onda electromagnética. O leitor emite a onda magnética e a *tag* reflecte onda fazendo variar as suas características físicas. Segue-se na Figura 2-8 um exemplo figurativo do processo usando um espelho e uma lanterna.(4)

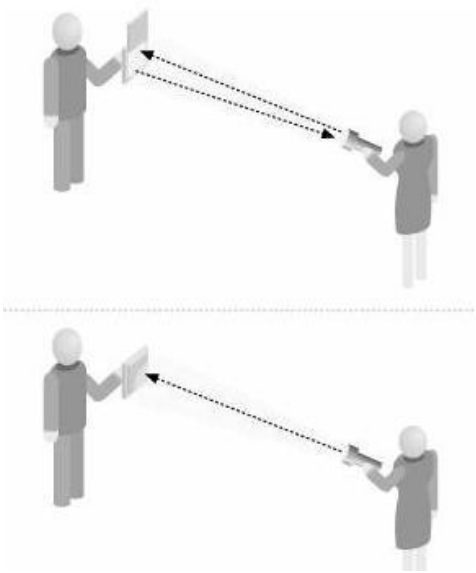

Figura 2-8 – Exemplo figurativo de um acoplamento radiativo

2.1.6 Memória e capacidade de processamento

Quanto à capacidade de processamento e memória, existe uma variedade de tecnologias aplicadas. Tipicamente as *tags* contêm um processador e blocos de memória, podendo a memória conter apenas um identificador ou ser capaz de guardar informação adicional.

Quanto à escrita e leitura, existem três tipos de *tags*: RO (*read only*), WORM (*write once read many*), WR (*read write*).

Nas primeiras, a informação é escrita apenas uma vez, no processo de fabrico, não podendo ser escritas novamente no seu tempo de vida. Destas destacam-se as *tags* SAW (*surface acustic wave*) e *wiegand*, não só pela tecnologia utilizada mas também pela inexistência de processador.

As *tags* SAW recebem do leitor, através da antena, um impulso de microondas que é conduzido a um transdutor que contém um cristal piezoeléctrico que vibra criando uma onda acústica. Essa onda acústica viaja através da *tag*, encontrando fitas reflectoras que reflectem parte da energia da onda. Essa energia reflectida é devolvida para o cristal que vibra novamente criando a reflexão para o leitor. O número e espaçamento de tiras determinam o número e o intervalo de tempo dos impulsos retornados para o leitor.

A construção de *tags wiegand* é baseada no efeito *wiegand*. O fio de *wiegand* é produzido trabalhado a frio um fio de uma liga metálica, Vicalloy. Este processo faz com que o fio apresente um núcleo magnético e uma periferia de mais alta coersividade. Quando exposto a um campo magnético de intensidade apropriada, o núcleo reverte a polaridade e posteriormente retorna à polaridade original. Este efeito é conhecido como “Salto de Barkhausen” ou “efeito de Barkhausen”. Ao espalhar estas descontinuidades pelo fio de *wiegand* é possível prever a ocorrência dos saltos de Barkhausen obtendo assim um identificador da *tag* (não confundir com protocolo Wiegand utilizado para comunicações cabeladas).

O tipo de *tags* WORM difere do primeiro, devido ao facto que a escrita de dados ou programação da *tag* geralmente não é efectuada pelo fabricante. Estas *tags* tipicamente contêm

microprocessadores, máquinas de estado simples, responsáveis pela interpretação de comandos recebidos pela interface rádio e operações de escrita e leitura na memória.

Por último temos *tags* WR, que podem ser lidas e escritas várias vezes, podendo transportar informação relevante. Este tipo de *tag* já é utilizado em transportes públicos, sendo utilizado apenas um título de acesso "recarregável"; isto significa que a *tag* é reescrita com nova informação.

Ainda temos um tipo de *tags* que geralmente não são consideradas RFID, devido ao facto de apenas transmitirem um bit. As *tags* EAS (*Electronic Article Surveillance*) são as mais disseminadas neste momento. Existem várias tecnologias aplicadas, variando desde utilização de campos magnéticos, ondas electromagnéticas ou até micro-ondas.

2.1.7 Normas

Ao contrário de outras tecnologias sem fios que convergiram para uma só norma, como por exemplo Wi-Fi e Bluetooth, no caso de RFID só agora se está a caminhar nesse sentido. Existe uma mescla de normas, muitas delas proprietárias. A Tabela 2-2 é ilustrativa disso mesmo, relacionando as frequências de operação com as normas utilizadas e o tipo de fonte de energia.

Tabela 2-2 – Tabelas de normas do interface rádio(2)

	Frequency					
Tag type:	125/134 kHz	5–7 MHz	13.56 MHz	303/433 MHz	860–960 MHz	2.45 GHz
Passive	ISO 11784/5, 14223 ISO18000-2 HiTag	ISO10536 iPico DF/iPX	MIFARE ISO14443 Tag-IT ISO15693 ISO18000-3 TIRIS Icode		ISO18000-6A,B,C EPC class 0 EPC class 1 Intellitag Title 21 AAR S918 Ucode	ISO18000-4 Intellitag µ-chip
Semipassive					AAR S918 Title 21 EZPass Intelleflex Maxim	ISO18000-4 Alien BAP
Active				ANSI 371,2 ISO18000-7 RFCode		ISO18000-4 ANSI 371,1

Destas convém salientar as normas ISO14443 (*proximity cards*), ISO15693 (*vicinity cards*), ISO18000-x e as classes 1,2,3,4 e classe 1 Geração 2 da EPC Global (5) pela sua disseminação.

É comum associar a tecnologia Mifare (6) (7)com a norma ISO 14443. Embora algumas variantes da tecnologia sigam a norma, o protocolo de criptografia é proprietário da empresa NXP Semiconductors. É de salientar também os esforços por parte da ISO e EPCGlobal para aprovar Class1 Gen2 da EPCGlobal como norma ISO 18000-6, de forma a fazer convergir estas duas normas.

2.2 Outras tecnologias.

No decorrer do estudo das tecnologias a utilizar foram analisadas tecnologias como NFC, Bluetooth e Zigbee.

Inicialmente desenvolvida como opção sem fios para a norma RS232, a tecnologia Bluetooth é actualmente usada nos mais variados contextos para transferência de dados a curta distância. Tem como mais-valias a robustez, segurança e baixo consumo de energia.

A tecnologia NFC é uma extensão da Norma ISO14443A, funcionando também com NFCIP (Near Field Communications Interface Protocol). É uma tecnologia proprietária da NXP Semiconductors, que se pretende colocar entre as tecnologias RFID e Bluetooth.(8)

No caso de Zigbee, especificação de uma pilha protocolar sobre a norma IEEE802.14.5, o ambiente natural são as redes de sensores sem fios, em que a conservação de energia e não a largura de banda é o factor fundamental. É de frisar, para o contexto em causa, que a especificação prevê um módulo de localização já com algumas implementações comerciais.(9)

2.3 Norma 802.11

A norma 802.11, desenvolvida pelo IEEE, define um conjunto de especificações ao nível das camadas protocolares de controlo de acesso ao meio (MAC) e física, de forma a permitir conectividade sem fios entre estações fixas, portáteis ou móveis numa rede local sem fios (WLAN). Em particular, descreve a operação de dispositivos em conformidade com a norma em redes infra-estruturadas e *ad-hoc*; serviços MAC assíncronos; técnicas de sinalização na camada física e funções da interface controladas pela camada MAC; operação numa WLAN que coexiste sobreposta com outras.

Na verdade, foram feitos melhoramentos à norma original, pelo que existem na realidade várias especificações e não uma só. Porém, essas especificações são apenas extensões à norma original. Entre as de maior destaque incluem-se o 802.11b, 802.11g e 802.11n, esta última ainda em desenvolvimento, que especificam extensões para suportar maiores débitos, até 11 Mbps, 54 Mbps e 278 Mbps, respectivamente, melhorando substancialmente a norma original (que previa débitos de 1 Mbps e 2 Mbps). No caso do 802.11b foram introduzidas rectificações permitindo uma operação comparável à da Ethernet. O 802.11n prevê ainda um aumento da área de cobertura para cerca do dobro das anteriores extensões. (10)

Em redes infra-estruturadas existe a necessidade de um DS, Distribution System, que interliga os elementos terminais da infra-estrutura, os Acess Points. Na revisão da norma em 2003 está ainda prevista a existência de um WDS, Wireless Distribution System, de forma que os APs sejam interligados sem a necessidade de uma infra-estrutura cablada.

Existem também soluções de localização baseadas na norma 802.11, usualmente tirando partido do indicador de potência recebida, RSSI (Received Signal Strength Indicatior), fornecido pelo interface Wi-Fi. Normalmente, neste tipo de soluções, é necessário fazer um mapeamento prévio das condições de propagação.

2.4 Conversores de meio

Actualmente no mercado existe uma variedade muito extensa de conversores de meio. Os mais interessantes neste contexto são os conversores RS232/RS485 para Ethernet ou Wi-Fi e os conversores Ethernet para fibra óptica. Os primeiros permitem por de parte a limitação do alcance de 9 metros do RS232 ou da natureza Half-Duplex do RS485, atribuindo um porto TCP e um

endereço IP a cada porta RS232/RS485, permitindo uma grande flexibilidade no envio e recepção de informação de e para o equipamento. No caso de conversores para Wi-Fi temos a vantagem acrescida da facilidade em ultrapassar barreiras físicas. Os conversores Ethernet para fibra óptica possibilitam vencer distâncias de uma forma transparente para o sistema, não limitando a rede aos 100 metros entre equipamentos, característico de redes Ethernet.(11)

Existem até leitores RFID que incorporam alguns destes conversores, fazendo a leitura da *tag*, e disponibilizam a informação directamente por Ethernet ou até Wi-Fi.

2.5 Sumario

Como está patente neste capítulo, o estudo incidiu principalmente na tecnologia RFID que, devido à sua penetração no mercado actual e inerente baixo custo, se torna a escolha natural para o projecto em causa, mitigando a desvantagem da amálgama de Normas existentes actualmente.

Quanto às tecnologias Zigbee e NFC, os seus estados embrionários de disseminação e custo tornam a sua implementação neste contexto proibitiva.

A tecnologia Bluetooth também foi posta de parte nesta altura, devido à sua propensão para a transferência de um grande volume de dados, complexidade relativa para o estabelecimento de comunicação e custo.

De forma análoga à tecnologia Bluetooth, a tecnologia Wi-Fi também tem como principal vocação a transferência de grandes quantidades de dados e as interfaces de comunicação necessárias para obter uma posição continuam com um custo muito elevado.

A tecnologia GPS, dados os requisitos propostos, seria pouco adequada por duas razões. A primeira prende-se com a impossibilidade da tecnologia funcionar em túneis, visto que usa triangulação por satélite. A segunda deve-se à necessidade de um canal de envio de informação. Sendo apenas um receptor, o equipamento GPS teria de integrar uma interface, de forma a transmitir as suas coordenadas ao sistema de localização, encarecendo bastante o equipamento.

Capítulo 3

3. Trabalho relacionado

Este capítulo é dedicado à descrição de alguns sistemas integrados de controlo de acessos existentes, dando a conhecer sucintamente as suas características e princípios de funcionamento. Irá também ser feita uma abordagem a algumas soluções de localização como soluções viáveis de controlo de acessos.

3.1 Sistema Card

O sistema *card* foi desenvolvido pela empresa Octal SA para controlo de acessos a recintos desportivos. A figura abaixo descreve sucintamente o funcionamento do sistema.

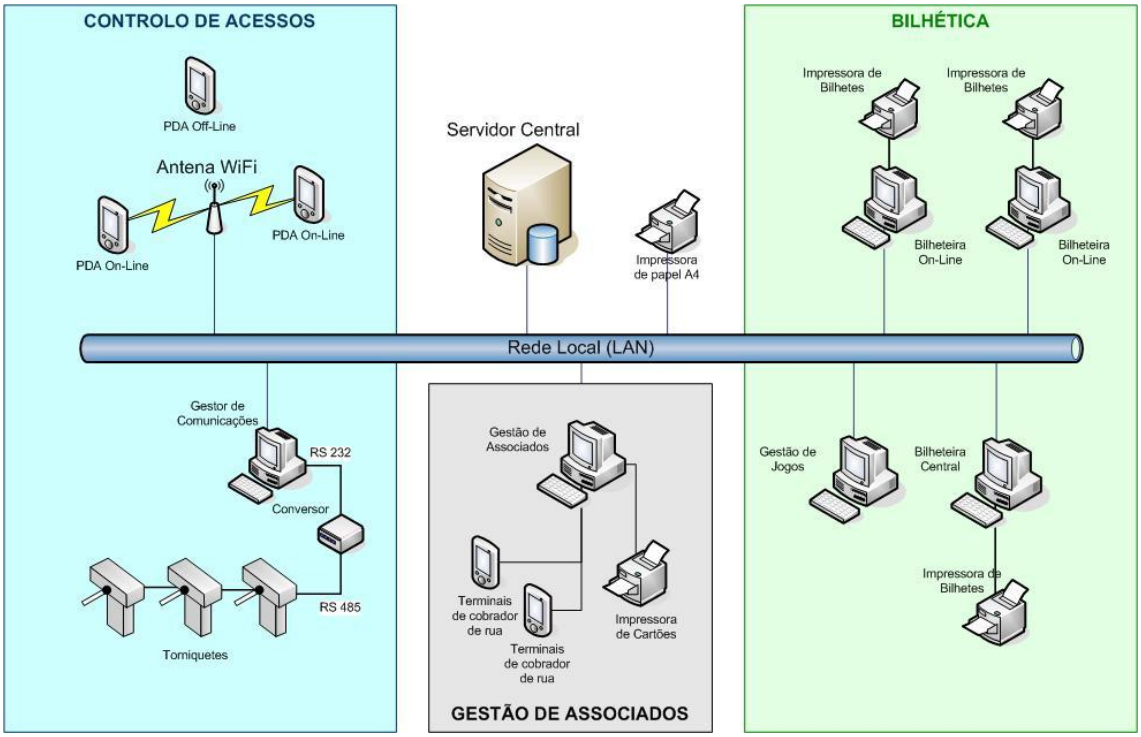

Figura 3-1 – Descrição genérica do sistema card (12)

Como se torna claro a partir da figura, a natureza do sistema é modular e com uma apetência marcante para eventos desportivos, segundo a filosofia natural de controlo de número de entradas no recinto. A descrição que se segue incidirá sobre o módulo de controlo de acessos em detrimento dos restantes módulos que fogem um pouco ao âmbito do trabalho em causa.

A tecnologia dos seus títulos de acesso é tipicamente baseada em códigos de barras, embora a introdução da tecnologia RFID passivo tenha sido implementada em alguns clientes.

Os torniquetes são um conjunto de barreira física, dispositivos informativos, leitor de títulos e módulo de processamento e comunicação.

A comunicação com ao “Gestor de comunicações” é feita recorrendo à norma RS485 de forma a vencer a distância que os separa, que por vezes é superior a 600 metros.

Tendo em conta a natureza half-duplex da tecnologia RS485, é implementado um mecanismo de *polling* para inquirir se algum *datacarrier* foi lido e em caso afirmativo é enviado o número. Também são enviados comandos para os torniquetes, por parte dos gestores de comunicações, para autorizar ou negar o acesso e respectiva informação a apresentar nos dispositivos informativos, depois de uma consulta à base de dados do servidor central.

O ponto de acesso tem uma capacidade de processamento considerável, podendo filtrar e tomar decisões localmente sobre a validade dos *datacarrier* para o evento específico, se assim estiverem configurados.

O software dos pontos de acesso depende dos chassis em que são implementados, visto que os chassis usados são fornecidos por terceiros.

A comunicação entre os sistemas periféricos (bilheteiras, gestor de associados, gestor de comunicações) e o servidor central é baseada em TCP/IP.

3.2 Sistema Skidata

A figura abaixo descreve sucintamente o funcionamento do sistema.

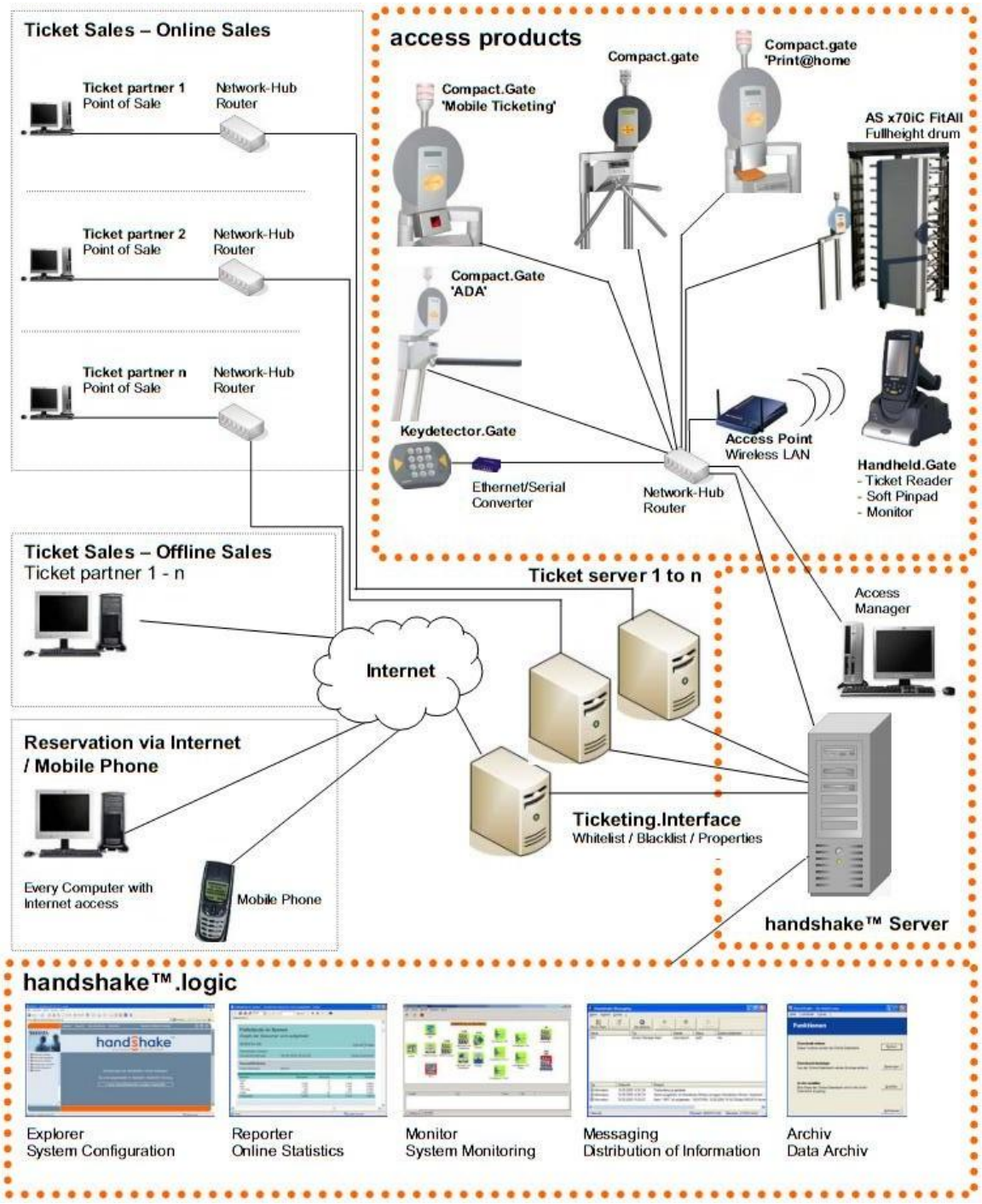

Figura 3-2 – Descrição genérica do sistema *skidata*

Mais recente que os sistema *card*, o sistema *skidata* tem toda a sua infra-estrutura de comunicações baseada em Ethernet e TCP/IP, tendo cada um dos pontos de acesso e máquinas a montante um endereço IP.

Os pontos de acesso, chassis, hardware e software são integralmente fornecidos pela *skidata*, apresentando uma variedade considerável de configurações modulares diferentes. De notar que o conceito de ponto de acesso não se refere somente ao acesso de pessoas, mas também a veículos.

Os pontos de acesso são geridos por uma ou mais máquinas, garantindo escalabilidade, denominadas *Access Managers*. Estas máquinas fornecem serviços que gerem os pontos de acessos e agem como módulo intermédio entre os pontos de acesso e o *handshake server*, reencaminhando os pedidos de acesso e respectivas respostas.

O núcleo do sistema de controlo de acessos é fechado; no entanto existe a possibilidade de expansão e integração do sistema recorrendo a software de terceiros. Por exemplo, a utilização de sistemas de bilhética não *skidata* ou a utilização de leitores de *datacarriers* não *skidata*, desde que sejam implementados mecanismos de conversão para o protocolo *skidata*.(13)

3.3 RTLS em hospitais

Ao contrário das soluções apresentadas vocacionadas abertamente para o controlo de acessos, esta solução é uma solução de localização em tempo real. Esta solução é integralmente implementada com hardware da empresa Kimaldi e baseada em tecnologia RFID activa.(14)

O propósito do sistema é a localizações de pessoal hospitalar. Devido às características da pulseira/tag RFID é possível a implementação de alarme e devido aos sensores da pulseira, detectar se a mesma está ou não a ser usada.(15)

Os leitores RFID estão equipados com interface *wireless* e Ethernet. Logo, todo o processamento de localização e gestão de alarmes é feito a montante do equipamento por software instalado em computadores pessoais.

Para que o sistema funcione convenientemente é de suma importância que todo o edifício esteja coberto pela rede WiFi ou que junto aos leitores existam tomadas Ethernet.

A um nível superior é feita a associação do indivíduo à pulseira/*tag* RFID, podendo ser feita interligação da informação de localização com um sistema de controlo de horário de entradas/saídas, dispensando outros métodos de controlo de assiduidade.

3.4 RTLS Ekahau

A Ekahau tem as suas principais instalações em Saratoga, Califórnia. É uma empresa de prestação de serviços de RTLS (Real Time Location Systems) e tem como objectivo principal fazer a implementação de serviços que permitam a localização de pessoas, inventários e outros objectos.

Este sistema difere do anterior devido à tecnologia usada. O sistema Ekahau é completamente baseado em 802.11. Utiliza a infra-estrutura Wi-Fi existente, e *tags* proprietárias. Como se torna claro, a área necessita de ter uma boa cobertura e as próprias *tags* são alimentadas por baterias. Também é necessário um estudo de propagação anterior à instalação, criando um mapa de cobertura, de forma que o sistema tenha a precisão anunciada pelo fabricante. O RTLS da Ekahau anuncia um erro de 1-3 metros num ambiente “óptimo” usando uma rede Wi-Fi, isto é, a Ekahau recomenda que existam pelo menos três pontos de acesso com pelo menos -75 dbm RSSI em qualquer localização dada.(16)

3.5 Sumário

Os dois sistemas de localização em tempo real que, devido à sua natureza, não prevêm um verdadeiro controlo de acessos, apenas a sua monitorização. A utilização de *tags* activas ou *tags* Wi-Fi (consoante o caso), embora ofereça um alcance significativo ao sistema, tem como desvantagem o tempo limitado de operação devido à necessidade de bateria para operar. A necessidade de um estudo prévio das condições de propagação no edifício também pode ser visto como uma desvantagem à implementação dos sistemas.

Os dois primeiros sistemas apresentados são sistemas de controlo de acessos tradicionais, o acesso é detectado por contacto, código de barras ou RFID passivo (alcance habitual de aproximadamente 8 cm) e não contemplam, de raiz, a aquisição de qualquer informação sobre a localização de utilizadores assim que entram no recinto controlado.

Em antítese, temos os dois sistemas RTLS que, embora tenham uma boa informação de localização e sejam sistemas sem contacto, não prevêem qualquer tipo de barreiras de forma a impedir acessos indevidos. A solução proposta neste trabalho apresenta-se como uma solução híbrida, posicionando-se entre os dois tipos de sistemas, melhorando as características descritas acima, pouco desejáveis face aos requisitos propostos.

Capítulo 4

4. Descrição da Solução

Neste capítulo apresenta-se a descrição da solução proposta, dividida em quatro tópicos. No primeiro é apresentada uma breve introdução para facilitar a compreensão da filosofia do modelo. No segundo é apresentado o modo de operação do modelo lógico, as funções de cada um dos seus módulos e mensagens trocadas entre módulos. No terceiro tópico é descrita a aplicação do modelo ao *hardware* e protocolos de comunicação utilizados. Por último é feita uma análise de alguns pontos relevantes da solução justificando algumas das opções tomadas.

É de realçar que no decorrer do desenvolvimento do modelo, e face aos requisitos propostos, foi necessário ter sempre presente o conceito de zona, principalmente “zonas cegas”. Também está patente no modelo o esforço para afastar o processamento de dados dos pontos de acesso, transferindo-o para montante, de forma a manter os elementos tipicamente em maior número, o mais simples possível, de forma a não encarecer o sistema.

4.1 Conceitos prévios

O conceito de zona é a base da operação do modelo e fulcral para a versatilidade e granularidade. Uma zona é uma área geográfica delimitada por zonas de fronteira leitura/não leitura, ou de potência captada. Neste modelo existem dois tipos de zonas: zonas abrangidas por leitores, cujas áreas dependem dos leitores em causa; e zonas cegas, delimitadas por zonas de leitura.

Na Figura 4-1 apresenta-se um exemplo da utilização de leitores com tecnologia rádio omnidireccional de alcance considerável, por exemplo RFID activo.

Os leitores são representados por quadrados pretos e as semi-circunferências representam as respectivas áreas em que os leitores detectam o *datacarrier*.

O algoritmo proposto para a decisão da zona baseia-se na detecção ou não detecção de um *datacarrier* no raio de alcance do leitor. E relevante salientar que um *datacarrier* é considerando fora de alcance se não for detectado pelo ponto de acesso durante um intervalo de tempo estipulado.

Referindo a Figura 4-1, um *datacarrier* está na zona 3 quando está no alcance dos dois leitores em simultâneo. Quando apenas é detectado pelo leitor da esquerda assume-se que o *datacarrier* está na zona 2, isto significa que nunca foi detectado pelo leitor da direita ou já passou o intervalo de tempo estipulado e é considerado fora do alcance pelo mesmo. O comportamento do leitor da direita para detecção do *datacarrier* na zona 4 é análogo. Quanto à zona 1 (zona cega), a decisão de atribuição zona é tomada assim que o *datacarrier* é considerado fora do alcance do leitor da esquerda, não estando a ser detectado pelo leitor da direita. O funcionamento do algoritmo no que diz respeito à zona 5 é análogo mas, neste caso, o datacarrier fica fora do alcance do leitor da direita, já estando anteriormente fora do alcance do leitor da direita.

Este algoritmo será exemplificado no capítulo 5, pois a implementação foi baseada nele.

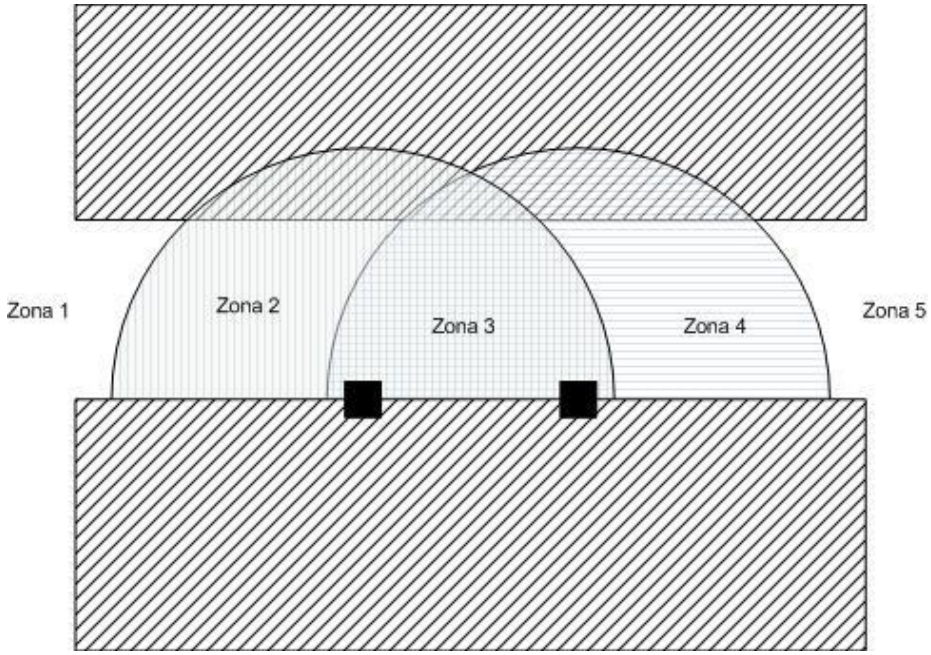

Figura 4-1 – Relação entre as zonas e as áreas de leitura dos *datacarriers,* considerando leitores omnidireccionais.

Na Figura 4-2 está especificada a mesma relação entre a área de leitura dos *datacarriers* e as zonas do modelo mas, neste caso, utilizando apenas um leitor direccional. É relevante notar que, para implementar com sucesso a relação abaixo exemplificada, é necessário que o leitor retorne informação sobre a potência recebida do *datacarrier* para a atribuição da zona.

Para este tipo de leitores a atribuição de zona baseia-se num limiar de potência recebida, acima do qual o *datacarrier* é considerado na zona 3 e abaixo do qual é considerado na zona 2.

O comportamento do algoritmo na decisão quanto à atribuição das zonas cegas, zonas 1 e 4 é também baseado no momento que o *datacarrier* fica fora do alcance do leitor mas, neste caso, se a potência recebida, da última vez que o *datacarrier* foi detectado, estava abaixo do limiar, considera-se o *datacarrier* na zona 1. Se, na última vez que o datacarrier foi detectado a potência recebida estava acima do limiar, considera-se o *datacarrier* na zona 4.

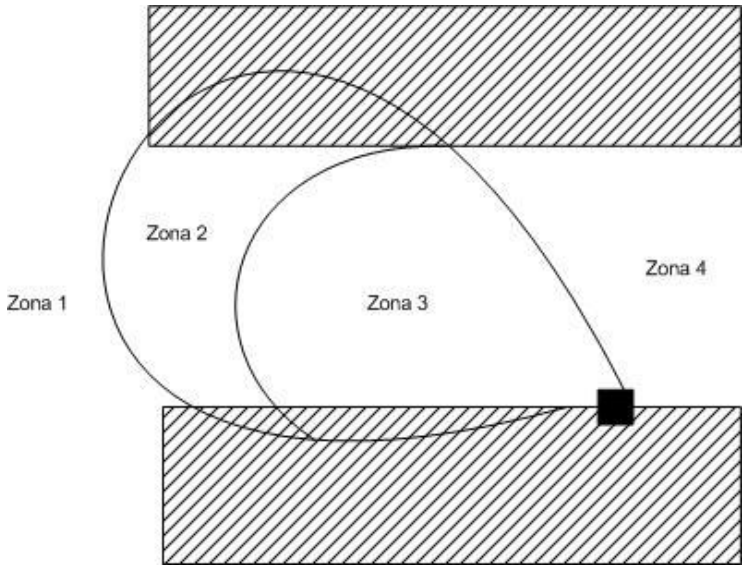

Figura 4-2 - Relação entre as zonas e as áreas de leitura dos *datacarriers,* considerando um leitor direccional.

Por último é apresentado o exemplo de outra possibilidade de relação entre leitores e zonas, neste caso a tecnologia usada será de proximidade, RFID passivo, banda magnética ou até código de barras. No entanto, devido às limitações impostas pela tecnologia, esta última solução deve ser implementada com utilizadores conscienciosos ou complementada com a instalação de barreiras físicas ou monitorização visual de acessos.

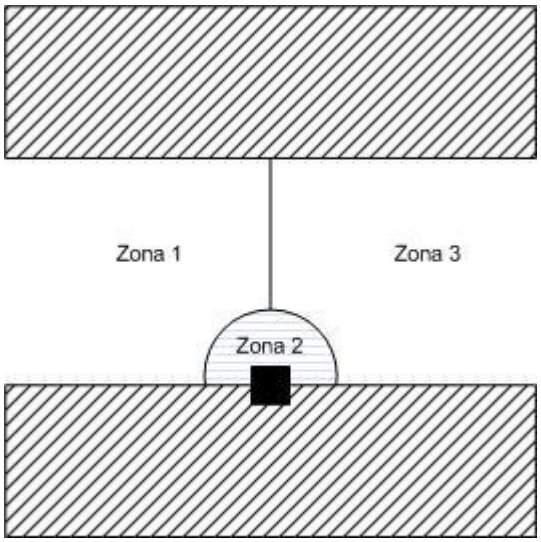

Figura 4-3 - Relação entre as zonas e as áreas de leitura dos *datacarriers,* considerando um leitor de proximidade.

Pontos de acesso como os expostos nas figuras acima podem ser colocados em corredores de acesso ao recinto a controlar e mesmo dentro do recinto, dentro do recinto é necessário garantir a passagem por estes pontos de acesso, sempre que o *datacarrier* sai de uma zona cega para outra. Com esta forma de utilizar os leitores é possível ter uma localização do datacarrier, embora com granularidade considerável.

Este modelo apenas tem a possibilidade de operar *online*, isto é, devido à opção de levar toda a capacidade de processamento para montante, longe dos leitores, perde-se a capacidade do sistema operar sem comunicações.

Outra das características deste modelo é a sua arquitectura cliente/servidor, tendo sido abandonada a hipótese de uma arquitectura em *mesh* ao nível dos leitores, devido ao custo da tecnologia necessária e às implicações que iria ter no modelo, alterando a filosofia de zonas e limitando a versatilidade.

4.2 Modelo Lógico

Na figura seguinte é apresentado o modelo simplificado, enfatizando os blocos lógicos da solução.

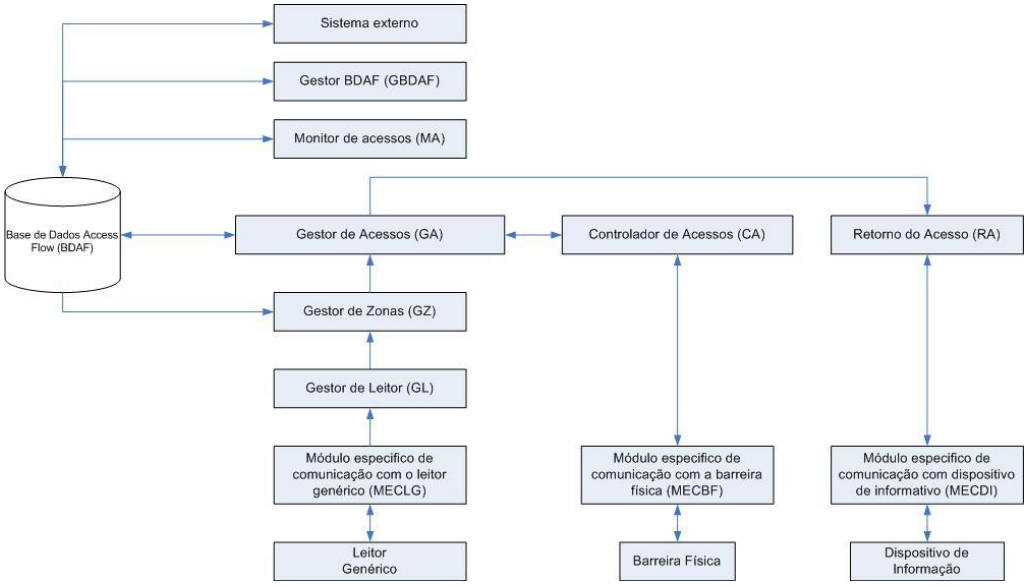

Figura 4-4 – Modelo lógico simplificado

Como irá ser evidente na descrição do modelo, é de importância fulcral haver sincronização temporal entre todos os módulos do sistema, principalmente nos que participam na leitura dos *datacarriers*.

Os módulos do sistema na base do modelo estão os MEC (Módulos Específicos de Comunicação), encarregues de acoplar todo o sistema a hardware e software fornecido por terceiros. Estes módulos deverão ser de implementação muito simples. A montante este módulos todas as mensagens trocadas são normalizadas. O está prevista uma instancia do GL para cada leitor, é este módulo que identifica o leitor e filtra mensagens repetidas de *beacons* consecutivos e decide quando um *datacarrier* está fora do alcance. O GZ agrega vários GL, e decide a zona que o *datacarrier* está no momento, passando-a para montante. O CA é responsável pela comunicação com o MEBF, controlando a abertura ou fecho de barreiras físicas, de forma análoga o módulo RA comunica com o MECDI com mensagens normalizadas e o MECDI apresenta-as no DI de forma apropriada. O GA é o módulo central do sistema, responsável por registar as zonas dos *datacarriers* na base de dados decidir abertura de barreiras e envio de mensagens para dispositivos informativos. De notar que este módulo apenas comunica com os módulos

directamente a jusante. Por fim temos o GBDAF e MA que acedem directamente à base de dados para configuração e monitorização de acessos respectivamente.

4.2.1 Módulo específico de comunicação com o leitor (MECLG)

Módulo de acoplamento como o leitor (MECL) é o módulo responsáveis pela interacção com os leitores, as mensagens envidadas e recebidas e jusante destes módulos são específicas do leitor a utilizar, sendo as mensagens enviadas para montante já normalizadas e de acordo com o protocolo especificado como exposto na figura seguinte.

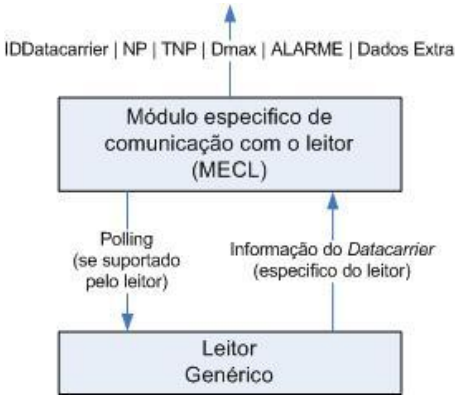

Figura 4-5 - Especificação do módulo MECL

Este módulo é implementado para um leitor específico, respeitando as especificidades do protocolo, incluindo o pedido de dados (*polling*), se necessário para o leitor em causa, e tratamento de dados de forma que a informação enviada ao GL tenha a forma da tabela abaixo.

Tabela 4-1 – Descrição da informação enviada do MECL para o GL

ID *Datacarrier*	Nível de potência	Total dos níveis de potência	DMax	Alarme	Dados extra
tamanho – 3 bytes dados - X bytes	Dados - 3 bytes	Dados - 3 bytes	Dados - 3 bytes	Dados - 1 byte	tamanho – 3bytes dados - X bytes

Os campos NP e TNP foram criados para aproveitar a informação de potência retornada por alguns leitores de RFID e permitir uma localização mais exacta do *datacarrier*. Também é necessário enviar a distância máxima a que o leitor recebe (DMax) para posteriormente estimar a distância a que a *tag* foi lida. Esta funcionalidade é fulcral para o modelo quando se utilizam leitores direccionais. No entanto o seu uso foi tornado mais abrangente e são utilizados na leitura de todos os *datacarriers*, como está descrito no exemplo abaixo.

- Considerando um leitor RFID activo que retorna potência de 150 num máximo de 255:
  - NP – 105 (lido a 105/255 da potência máxima de leitura)
  - TNP - 255

- Considerando um leitor de códigos de barras, banda magnética, RFID passivo ou até RFID activo em que o leitor não tem informação de potência recebida:
    - NP – 1 (lido)
    - TNP - 1

Como irá ser visto no ponto seguinte, estes campos tomam outros valores, com significado mais abrangente.

Os campos “alarme” e “dados extra” são utilizados para não limitar o modelo, sendo uma maneira fácil de enviar informação pela pilha de módulos de leitura caso seja fornecida pelo leitor e necessária em módulos superiores.

4.2.2 Gestor de leitores (GL)

Cada uma das instâncias deste módulo tem associado um ficheiro em XML, especificando as configurações das ligações a jusante e montante. Segue-se um exemplo ilustrativo do mesmo.

```
<GL>
      <leitor id=’43’ tipo=’2’ granularidade=’0.5’ foradealcance=’7’>
            <socket tipo=’serie’>
                  <iface>/dev/ttyS0</iface>
                  <baudrate>115200</baudrate>
                  <bits>8</bits>
                  <paridade>0</paridade>
                  <stopbit>1</stopbits>
            </socket>
      </leitor>
      <GZ>
            <socket tipo=’tcp/ip’>
                  <ip>192.168.30.30</ip>
                  <tcp>9876</tcp>
            </socket>
      </GZ>
</GL>
```

Neste exemplo é intencional a utilização de dois tipos distintos de *sockets*, evidenciando a versatilidade das configurações.

Também é relevante nesta altura referir os atributos “tipos de leitores”, “granularidade” e “fora de alcance”. Estes conceitos existem para permitir a utilização de *datacarriers* de contacto como códigos de barras, bandas magnéticas ou RFID passivo e ao mesmo tempo suportar tecnologia de longo alcance como RFID activo quer com antenas direccionais ou omnidireccionais.

A figura abaixo evidencia o formato das mensagens recebidas pelo MECLG e enviadas para o GZ.

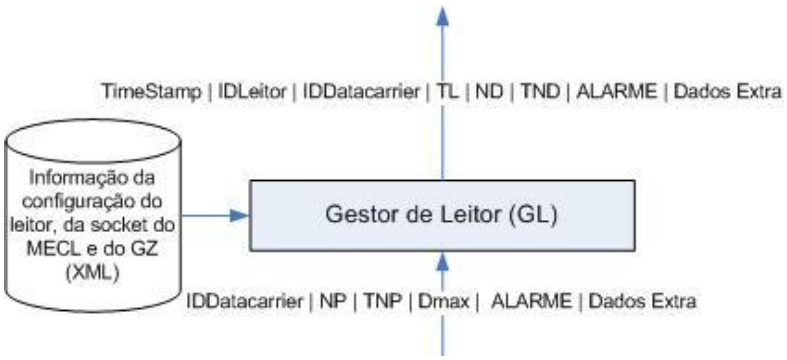

Figura 4-6 – Especificação do módulo GL

Este módulo tem três funções principais: a inserção de campos informativos, filtrar leituras redundantes do MECL e informar o GZ que o *datacarrier* está fora do alcance. O conceito de leituras redundantes e fora de alcance apenas se aplica quando o MECLG está ligado a um leitor de *datacarriers* RFID activos.

A inserção do *TimeStamp* tem o formato YYYYMMDDhhmmss, ocupando um total de 14 bytes em codificação ASCII. Nesta fase é necessário haver uma sincronização temporal dos equipamentos que albergam o módulo GL. Para satisfazer este requisito a implementação de mecanismos de sincronização com base no *network time protocol* (NTP) é fulcral.

O formato da identificação do leitor (IDLeitor) é análogo ao formato utilizado para descrever a identificação do *datacarrier* mas neste campo apenas se utiliza um byte para descrever o tamanho, logo, com um máximo de 9 bytes para a identificação propriamente dita.

Neste modelo são considerados oito tipos de leitores: leitores de códigos de barras (Tipo 00), banda magnética (Tipo 01), RFID passivo (Tipo 02), semi-passivo (Tipo 03), activo. Entre os leitores de RFID activos temos omnidireccionais sem (Tipo 10) e com informação de potência (Tipo 11), e direccionais sem (Tipo 20) e com informação de potência (Tipo 21).

Os campos Tipo Leitor (TL), Nível de Distância (ND) e Total de Níveis de Distância (TND) estão intrinsecamente ligados e em alguns casos dependem do valor de “granularidade” obtido do ficheiro de configuração.

A granularidade é um valor entre um e zero exclusivé. Adquire relevância em leitores de RFID activo, direccionais e omnidireccionais com informação de potência (Tipo 11 e Tipo 21); para todos outros assume-se granularidade igual a 1. Os exemplos abaixo descrevem o cálculo para alteração dos valores ND e TND recebidos do MECLG. Posteriormente são enviados integrados nas mensagens para o GZ.

O cálculo do ND e TND é obtido através da aplicação da equação de Friis, linearizando tendo em conta a atenuação quando a onda se propaga em espaço livre. Posteriormente é aplicada a granularidade que afecta a precisão da localização do *datacarrier*.

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2$$

Figura 4-7 - Equação de Friis(17)

Gt e Gr são o ganho da antena que transmite e recebe, respectivamente; Pt e Pr são a potência transmitida e recebida, respectivamente; λ é o comprimento de onda e R a distância.

Esta operação pode ser feita sem mais considerações devido à inexistência de obstáculos entre os *datacarriers* e os leitores.

Exemplos para todos os leitores excepto do tipo 11 e 21

```
TND (GZ) = 1
ND (GZ) = 0 – Datacarrier lido
ND (GZ) = 1 – Datacarrier fora do alcance
```

Exemplos para leitores do tipo 11 e 21 com granularidade de 0,5.

```
TND (GZ) = 2
ND (GZ) = 0 – Datacarrier lido numa área proxima
ND (GZ) = 1 – Datacarrier numa área mais afastada
ND (GZ) = 2 – Datacarrier fora do alcance
```

Os campos IDDatacarrier, ALARME e Dados Extra são passados ao módulo superior sem alteração. A Tabela 4-2 especifica o formato das tramas enviadas do GL para o GZ.

Tabela 4-2 - Descrição da informação enviada do GL para o GZ

Timestamp	ID Leitor	ID *Datacarrier*	TL	ND	TND	Alarme	Dados extra
dados – 14 bytes	tamanho – 2 bytes dados - X bytes	tamanho – 3 bytes dados - X bytes	dados - 2 bytes	dados - 3 bytes	dados - 3 bytes	dados - 1 byte	tamanho – 3 bytes dados - X bytes

O envio das mensagens para o GZ é efectuado da forma descrita nos fluxogramas seguintes.

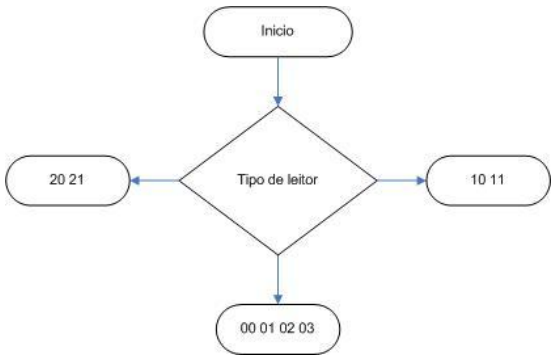

Figura 4-8 – Fluxograma de funcionamento do GL

O fluxograma acima representa o primeiro estágio do módulo, a informação de tipo de leitor, retirada do ficheiro de configuração, de modo a saber como tratar as mensagens recebidas. O fluxograma abaixo, demonstra o funcionamento do módulo quando está ligado a um leitor de proximidade.

Figura 4-9 - Fluxograma de funcionamento do GL, Fluxograma de funcionamento do GL, leitores de proximidade ou contacto

De forma análoga ao fluxograma da Figura 4-9 o fluxograma da figura Figura 4-10 representa o funcionamento do módulo quando está associado a leitores omnidireccionais sem informação de potência. Tipicamente este tipo de leitores funcionam aos pares, mas o problema de localizar o *datacarrier* na zona é tratado no módulo GZ.

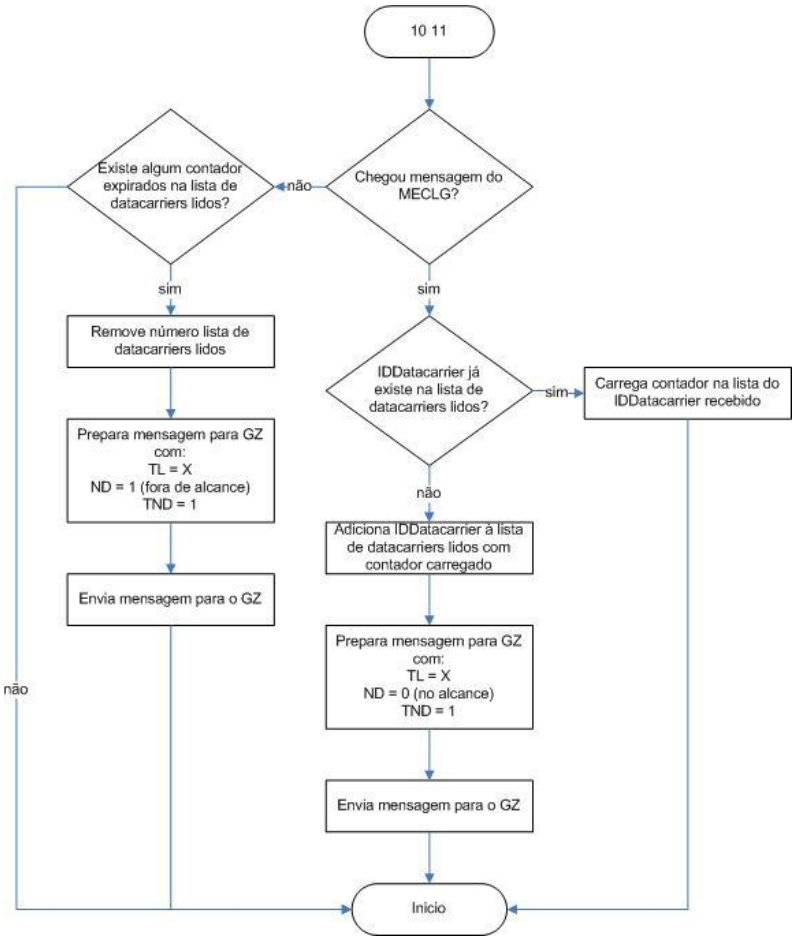

Figura 4-10 - Fluxograma de funcionamento do GL Fluxograma de funcionamento do GL, leitores cuja informação de potência é irrelevante.

É apresentado na Figura 4-11 o fluxograma de tratamento de mensagens quando este módulo está ligado a leitores com informação de potência, tipicamente direccionais.

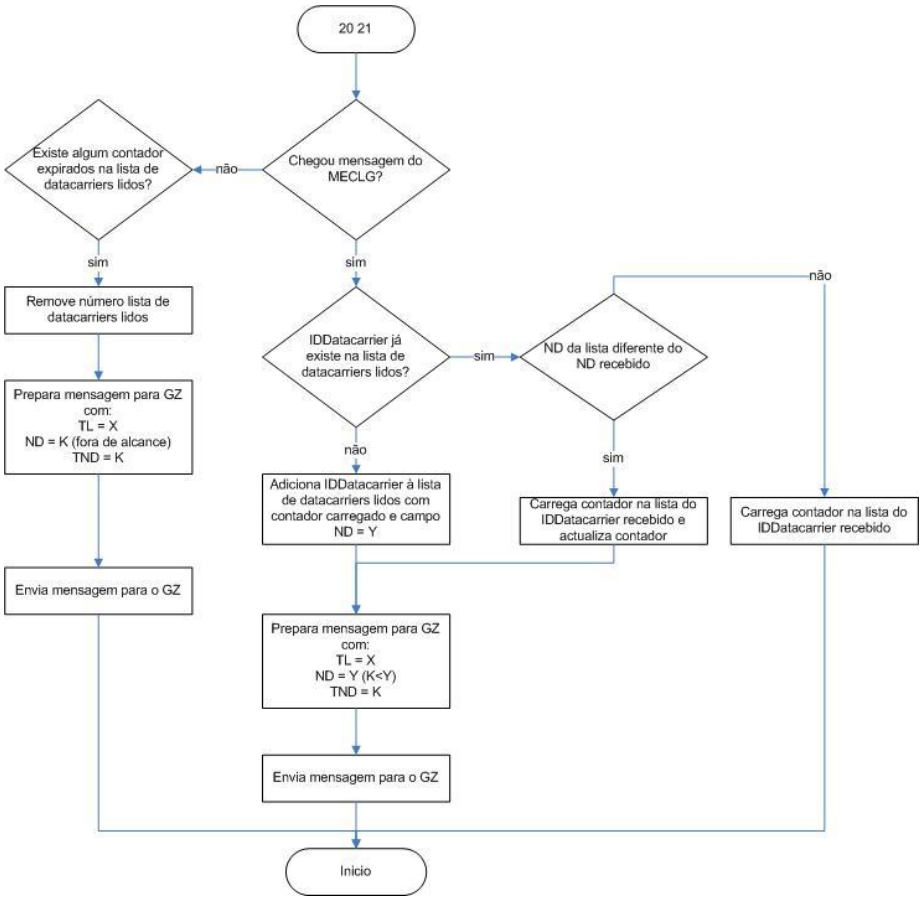

Figura 4-11 - Fluxograma de funcionamento do GL, leitores cuja informação de potência é relevante.

4.2.3 Gestor de zona (GZ)

Este módulo é responsável pela atribuição de zonas aos *datacarriers*. Essa atribuição é feita com base nas mensagens recebidas do GL e consultas à base de dados. O acesso deste módulo à base de dados é apenas de leitura, sendo a informação de zona atribuída passada ao módulo superior. O acesso à base de dados deve-se à inclusão no modelo a possibilidade de funcionar com tecnologias de contacto ou proximidade.

O problema da direcção de acesso é relevante no caso de *datacarriers* de proximidade, necessitando o módulo de ter acesso à zona em que o *datacarrier* se encontrava anteriormente. Também as questões de permissões de acesso são pertinentes, não só no caso de autorização de acesso quando existem barreiras físicas, mas também na geração de alarmes aquando da inexistência das mesmas.

A configuração deste módulo é feita de forma análoga ao módulo anterior, recorrendo a um ficheiro XML de configuração, como exemplificado abaixo.

```
<GZ>
      <BDAF nome = 'BDAF'>
            <host>192.168.30.200</host>
            <user>afgz</user>
            <pass>1234567890</pass>
```

```
	</BDAF>
	<GA>
		<socket tipo='tcp/ip'>
			<ip>192.168.30.80</ip>
			<tcp>9866</tcp>
		</socket>
	</GA>
	<GLS>
		<socket tipo='tcp/ip'>
			<tcp>9999</tcp>
		</socket>
	</GLS>
</GZ>
```

A operação do módulo sobre as mensagens recebidas está patente Figura 4-12.

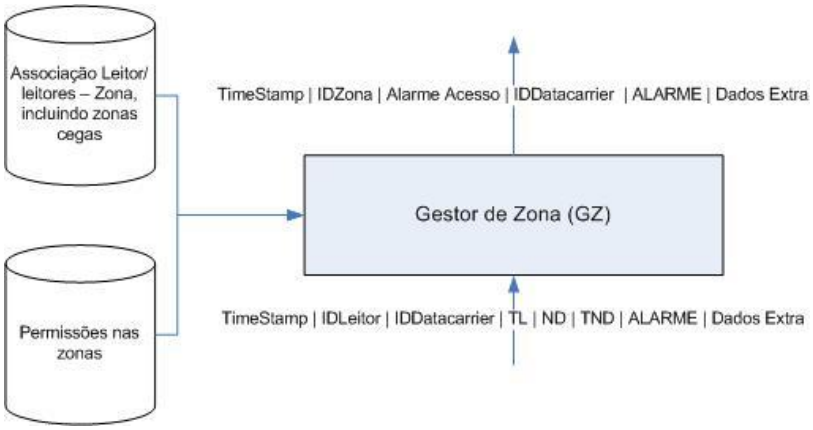

Figura 4-12 - Especificação do módulo GZ

O formato das mensagens enviadas para o GA está exemplificado na Tabela 4-3.

Tabela 4-3 - Descrição da informação enviada do GZ para o GA

Timestamp	ID *Datacarrier*	Alarme acesso	ID Zona	Alarme	Dados extra
dados – 8 bytes	tamanho – 3 bytes dados - X bytes	dados - 3 bytes	dados - 5 bytes	dados - 1 byte	tamanho – 3 bytes dados - X bytes

Os fluxogramas da Figura 4-13, Figura 4-14, Figura 4-15 e Figura 4-16 ilustram o funcionamento do módulo GZ.

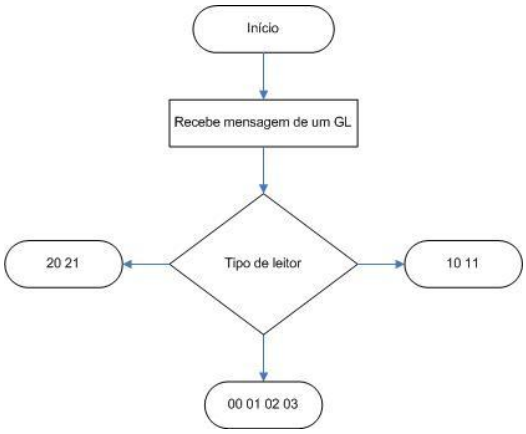

Figura 4-13 - Fluxograma de funcionamento do GZ

O fluxograma da Figura 4-14 descreve o funcionamento do GZ com *datacarriers* de contacto. É de ressalvar que a mensagem indicativa da zona do leitor é muito importante, porque dela pode depender a activação de barreiras físicas e/ou o envio de mensagens para dispositivos informativos.

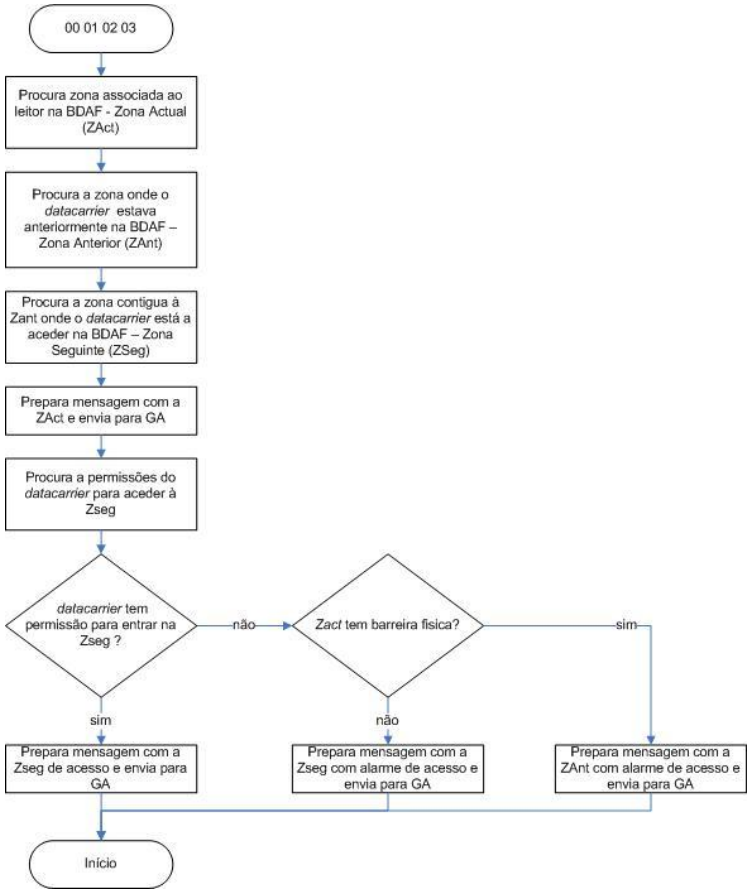

Figura 4-14 - Fluxograma de funcionamento do GZ para associadas zonas a leitores de proximidade

No caso do fluxograma da Figura 4-15 o acesso à base de dados é feito não só para saber a zona atribuída ao leitor, mas também para saber a parelha de leitores que operam nas zonas em questão. Para melhor compreensão do fluxograma sugere-se que estejam presentes os conceitos de zona do tópico “Conceitos prévios”

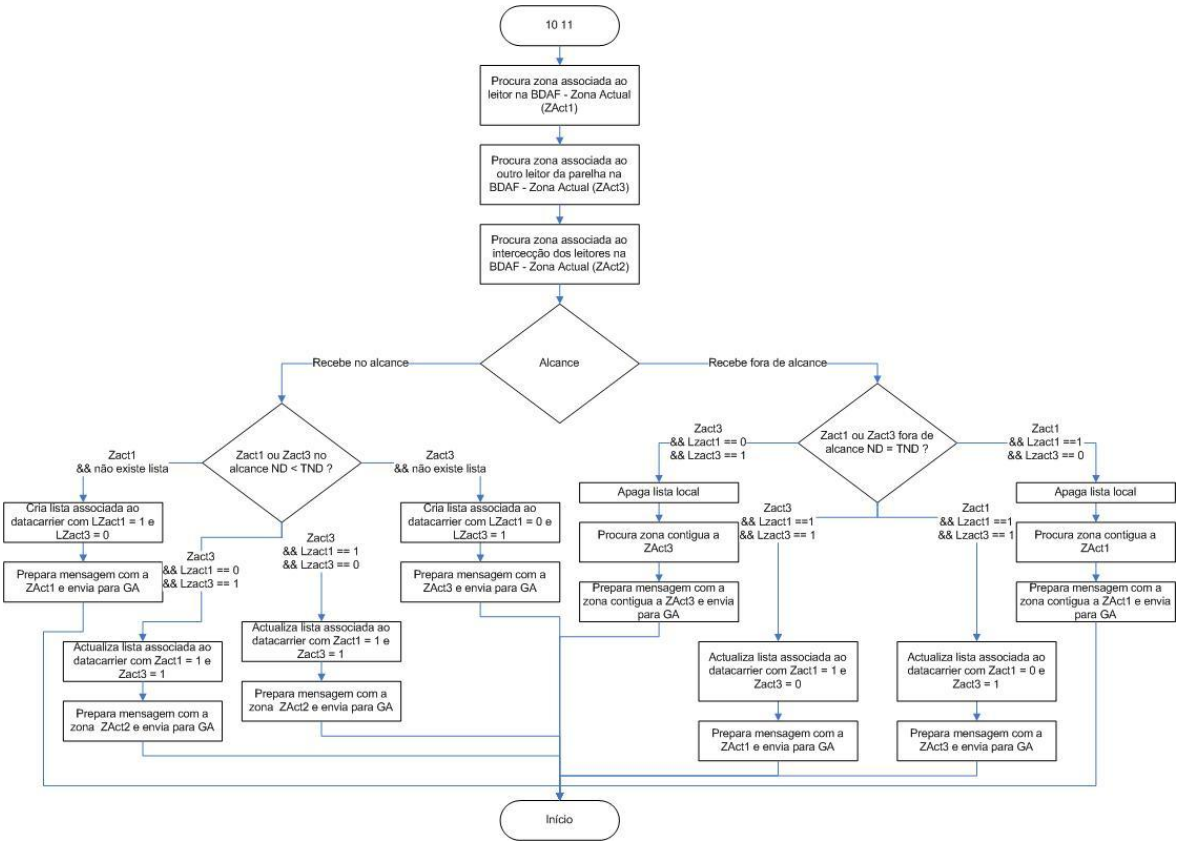

Figura 4-15 Fluxograma de funcionamento do GZ para zonas associadas a leitores de longo alcance não direccionais, sem informação de potência.

No fluxograma da Figura 4-16 está descrito o algoritmo de atribuição de zonas, baseado na potência retornada (ND) pelos leitores direccionais.

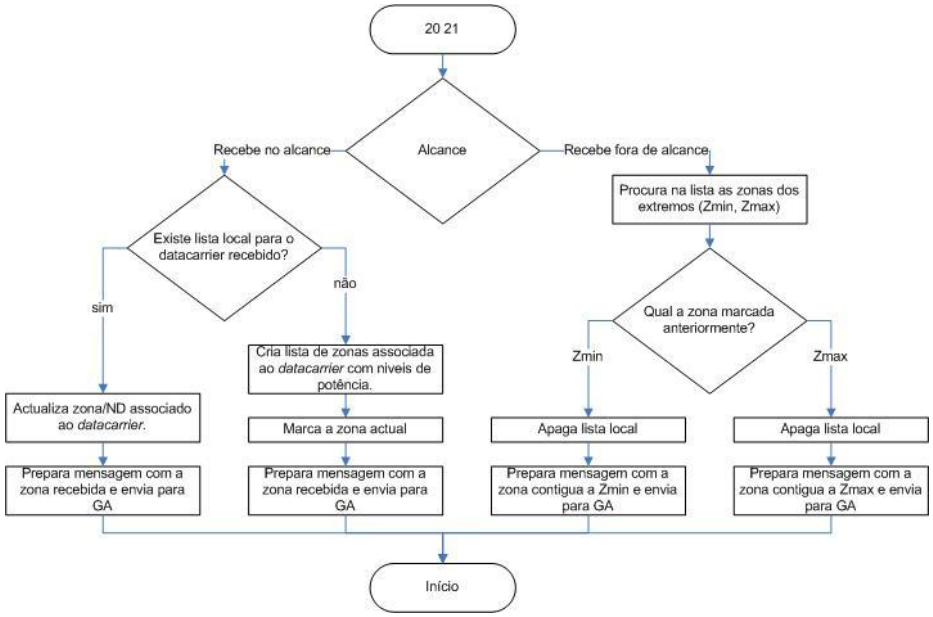

Figura 4-16 - Fluxograma de funcionamento do GZ para zonas associadas a leitores de longo alcance direccionais.

4.2.4 Gestor de Acessos (GA)

Este módulo é responsável pela recepção da informação da zona em que se encontra o *datacarrier* e sua escrita na base de dados e inerente criação do registo de acessos. Para além desta função comunica com os módulos Retorno do acesso (RA) e Controlador de acessos (CA).

Para tornar este modelo mais completo, este módulo regista incoerências nos acessos, isto é, quando um *datacarrier* atravessa zonas não adjacentes.

De forma análoga aos outros módulos a configuração deste módulo está em XML de acordo com o exemplo seguinte.

```
<GA>
      <BDAF nome = 'BDAF'>
            <host>192.168.30.200</host>
            <user>afga</user>
            <pass>1234567890</pass>
      </BDAF>
</GA>
```

É necessário haver cifragem da informação de utilizador e *password*.

4.2.5 Retorno do Acesso (RA)

Este módulo tem como propósito facultar informação da localizações do recinto a controlar, situando-se tipicamente perto dos pontos de acesso, mas não necessariamente. Pode ter como dispositivo associado um monitor, um *display* de sete segmentos, um led ou apenas um dispositivo sonoro, apenas com o propósito de facultar algum tipo de retorno visual ou auditivo aos utilizadores.

4.2.6 Controlador de acessos (CA)

O controlador de acessos é responsável pela permissão dos acessos, que normalmente consistirá em levantar uma barreira ou girar um torniquete. De notar que este módulo supõe bidireccionalidade no fluxo de informação. Isto deve-se à possível existência de sensores nos dispositivos que barram os acessos. Um exemplo ilustrativo da importância da possibilidade de retorno de informação para o GA é o das espiras das barreiras de acesso automóvel; a informação da existência ou não de um carro em cima de uma espira é de importância fulcral para que o acesso seja facultado.

4.2.7 Gestor de BDAF

Este módulo é apenas um interface para o administrador do sistema de controlo de acessos poder configurar a Base de dados, de forma a inserir mais zonas, leitores e políticas de acessos. Não troca mensagens com outros módulos, acedendo directamente à BDAF.

4.2.8 Monitor de Acessos (MA)

De forma análoga ao módulo anterior este módulo acede directamente à base de dados, servindo apenas de interface visual aos acessos, fornecendo, por exemplo, a capacidade de visualização de alarmes.

4.3 Descrição da implementação do modelo

Este tópico descreve a implementação do modelo lógico descrito no tópico anterior, incluindo os protocolos, tecnologias e hardware a utilizar.

4.3.1 Protocolo de troca de mensagens

A transmissão de todas as mensagens entre módulos é feita em codificação ASCII e recorrendo à utilização de *sockets*. Para além dos dados a passar, e com intuito de tornar o protocolo mais robusto, é inserido no início da mensagem o *startbyte* “0x01”. No fim da mensagem são inseridos dois bytes de CS de *checksum* e o *stoptbyte* “0x02” como está exemplificado na Tabela 4-4.

Tabela 4-4 – Formato das mensagens do protocolo

startbyte “0x01”	DADOS	CS_MS	CS_LS	*stoptbyte* “0x02”

Os dois bytes de *checksum* são calculados somando todos os bytes da mensagem e negando a soma. O resultado é truncado, retirando-se apenas o último byte. A representação hexadecimal desse byte é então codificada em ASCII sendo colocada a representação dos quatro bytes mais significativos (CS_MS) no antepenúltimo byte e a representação dos quatro bytes menos significativos (CS_LS) no penúltimo byte da mensagem.

Como todos os bytes da mensagem estão codificados em ASCII, assim como os dois bytes de *checksum*, nunca existe o problema de má interpretação dos *startbyte* e *stoptbyte* do protocolo.

Qualquer formato de dados retornado por um leitor genético que não seja codificado em ASCII deve ser transmitido alterando a sua representação hexadecimal do *byte* para dois caracteres codificados em ASCII.

4.3.2 Comunicação entre módulos.

Na implementação das comunicações do modelo lógico existem duas regiões a considerar. A região perto de leitores, barreiras físicas ou dispositivo de informação simples que comunicam com normas como RS232, RS485 ou até usando o protocolo *wiegand* como é o caso de alguns leitores RFID. A segunda já assenta em normas e protocolos de rede.

Para todos os módulos que operam em máquinas distintas e cujas comunicações operam suportadas por TCP/IP existem duas limitações: obstáculos físicos intransponíveis e distâncias superiores a 100 metros entre equipamentos activos. No segundo caso parte-se do pressuposto que a rede é Ethernet e existe impossibilidade de instalar regeneradores. Para os primeiros a solução óbvia passará pelo recurso a rede Wi-Fi, e se necessário com a implementação de

"*Wireless Distribution System*". Para solucionar o problema das distâncias a solução residirá no uso de conversores de meio, Ethernet/fibra óptica. O custo dos conversores e da fibra óptica está intrinsecamente ligado à distância a vencer.

A ligação dos MECL ao hardware de acesso é feita usando RS232 ou RS485. Caso a interface do hardware de acesso seja mais atípica, a utilização de conversores é uma forma económica de solucionar o problema.

4.3.3 Hardware

A implementação de todos os módulos com a excepção dos MECL deve ser feita em máquinas com sistema operativo, de forma a poderem ser acedidas remotamente para administração. Dependendo da carga de processamento pretendida e dimensão do sistema, os módulos que não necessitam de interacção com o utilizador podem ser implementados num router Linksys WRT54G/GS com a distribuição de Linux "Openwrt" que, devido à versatilidade do equipamento e quantidade de interfaces disponíveis, seria uma solução muito mais interessante do que a implementação em computadores pessoais tradicionais. Também deve ser feita uma excepção ao GA devido ao papel fundamental que possui no sistema.

A implementação dos MECL será feita tipicamente recorrendo a uma PIC que tenha no mínimo duas USARTs e a conversores de nível TTL para RS485 ou RS232. A utilização da norma RS485 pode ser interessante caso o hardware dos módulos superiores esteja localizado a mais de 100 metros e menos de 1000 dos respectivos MEC, sendo a conversão de RS485 para Ethernet feita numa zona mais próxima aos módulos superiores.

Outra possibilidade para a implementação dos MEC será em máquinas já dentro da rede local. Neste caso seria necessária a existência de um ficheiro de configuração do módulo para atribuição dos parâmetros da *socket* e apenas a existência de um conversor do protocolo e norma do interface do leitor para Ethernet.

4.4 Sumário

A opção da transmissão das mensagens em codificação ASCII foi tomada por duas razões: a primeira devido ao formato dos dados de identificação retornados pela maior parte dos leitores serem codificados em ASCII e a segunda para facilitar a implementação dos módulos e a interacção do protocolo com sistemas externos.

A utilização de *sockets* torna os módulos mais versáteis e simples, podendo com o mínimo de modificações alterar as interfaces pelas quais os dados são enviados.

Torna-se claro que a preocupação principal do protocolo de troca de mensagens é a compatibilidade e a clareza. Não foram feitas quaisquer considerações sobre a optimização da eficiência no uso da rede. Isto deve-se principalmente ao número e tamanho reduzido das mensagens trocadas a níveis superiores do sistema. Também foi dada mais atenção à flexibilidade e compatibilidade do sistema em detrimento da segurança.

No modelo lógico, o papel do GZ poderia estar mais associado ao leitor ou conjunto de leitores formando o conceito de porta. As vantagens desta abordagem seriam a diminuição de complexidade neste módulo, passando os algoritmos de atribuição de zona para o GA, e a não

necessidade de acesso à base de dados, visto que as configurações seriam locais. Na opção tomada valoriza-se a clareza das mensagens e possibilidade de compatibilidade com sistemas externos, em detrimento da simplicidade dos módulos.

A escalabilidade foi um factor importante no desenvolvimento do modelo lógico, podendo o módulo “gestor de zona” ter várias instâncias, em hardware distinto, e cada uma delas ter associado um grupo de instâncias de ”Gestores de leitores”.

Todos os módulos com a excepção dos MEC podem ser administrados remotamente. Para isso contribui a existência dos ficheiros de configuração. É também relevante ressalvar que o identificador do leitor é atribuído pelo respectivo GZ, não havendo qualquer operação de administração possível nos MEC.

É relevante salientar que no modelo foi feito um esforço para levar o processamento para longe do hardware de controlo de acessos propriamente dito (barreiras, leitores e torniquetes), não encarecendo os elementos que estão presentes em maior número.

Capítulo 5

5. Implementação

Neste capítulo apresenta-se a implementação e testes baseados numa parte do modelo descrito anteriormente. Pretende-se apenas a prova do conceito, pelo que a implementação executada foi parcial e focada num cenário de utilização. Foram implementadas algumas funcionalidades dos módulos MECL, GL e GZ, considerando que a decisão da zona é feita neste último.

5.1 Descrição do cenário

A implementação foi focalizada na detecção de fluxo de pessoas movimentando-se num "*bottle-neck*". A detecção foi feita através de dois leitores de RFID activos sem informação de potência.

5.2 Leitores

O modelo dos leitores utilizados é o RF8315R-s, fabricado pela Ananiah Electronics.(18)

Abaixo estão expostas as características funcionais mais relevantes dos leitores adoptando uma abordagem pragmática.

- Frequência de operação - 315 Mhz.
- Dados disponibilizados – Identificador enviado pela *tag* RF8315T (4 caracteres) + 1 espaço.
- Interface - RS232, 9600 Baud, 8 *bit words*, 1 *stop bit*, 1 *start bit*, sem paridade.
- Capacidade – Lê até 160 identificadores simultaneamente.

Na Figura 5-1 pode ser vista uma imagem do tipo de *leitores* utilizados neste teste.

Figura 5-1 – Leitor RFID Activo - RF8315R-s

5.3 Tags

O modelo das *tags* utilizadas é o RF8315T, fabricado pela Ananiah Electronics. De forma análoga aos leitores, as características funcionais mais relevantes das *tags* serão expostas adoptando uma abordagem pragmática(19).

- Baterias - CR2025 / CR2032
- Consumo de energia - 4mA a transmitir, 19uA sem transmitir.
- Frequência de operação - 315 Mhz.
- Dados enviados - 4 caracteres (A-Z, a-z, 0-9). Todos os transmissores enviam um indicador único.
- Alcance eficaz - 8 metros com a antena incluída de fábrica, até 15 metros com uma antena de 40 centímetros.

É de realçar que as *tags* enviam *beacons* de 2 em 2 segundos e este valor não é reprogramável no equipamento utilizado.

Foram retiradas as antenas às *tags* de forma a diminuir o seu alcance para os testes 1, 2 e 3. É de notar que com a antena colocada, a *tag* era detectada por ambos os leitores em todo o piso do edifício, incluindo o poço de escadas. Quanto ao teste 4, efectuado em espaço aberto, as antenas não foram retiradas das *tags*.

Na Figura 5-2 pode ser vista uma imagem do tipo de *tags* utilizadas neste teste.

Figura 5-2 - *Tag* RFID Activo - RF8315T

5.4 Delimitação de zonas e espaço físico

Os primeiros três testes foram efectuados no terceiro piso do edifício do INESC Porto, foi utilizado um corredor para criar o *bottleneck*, o quarto teste foi efectuado no parque de estacionamento do INESC Porto. Foram posicionados os dois leitores de forma a criarem 3 zonas detectáveis e duas zonas cegas. Foi feita uma delimitação inicial das zonas, sem obstáculos entre *tag* e leitor; as zonas foram marcadas no local e serviram de referência para os resultados obtidos. A delimitação inicial das zonas e posição dos leitores dos testes 1, 2 e 3 pode ser visualizada nas Figura 5-3 e Figura 5-4. A delimitação inicial das zonas e posição dos leitores do teste 4 pode ser visualizada na Figura 5-5.

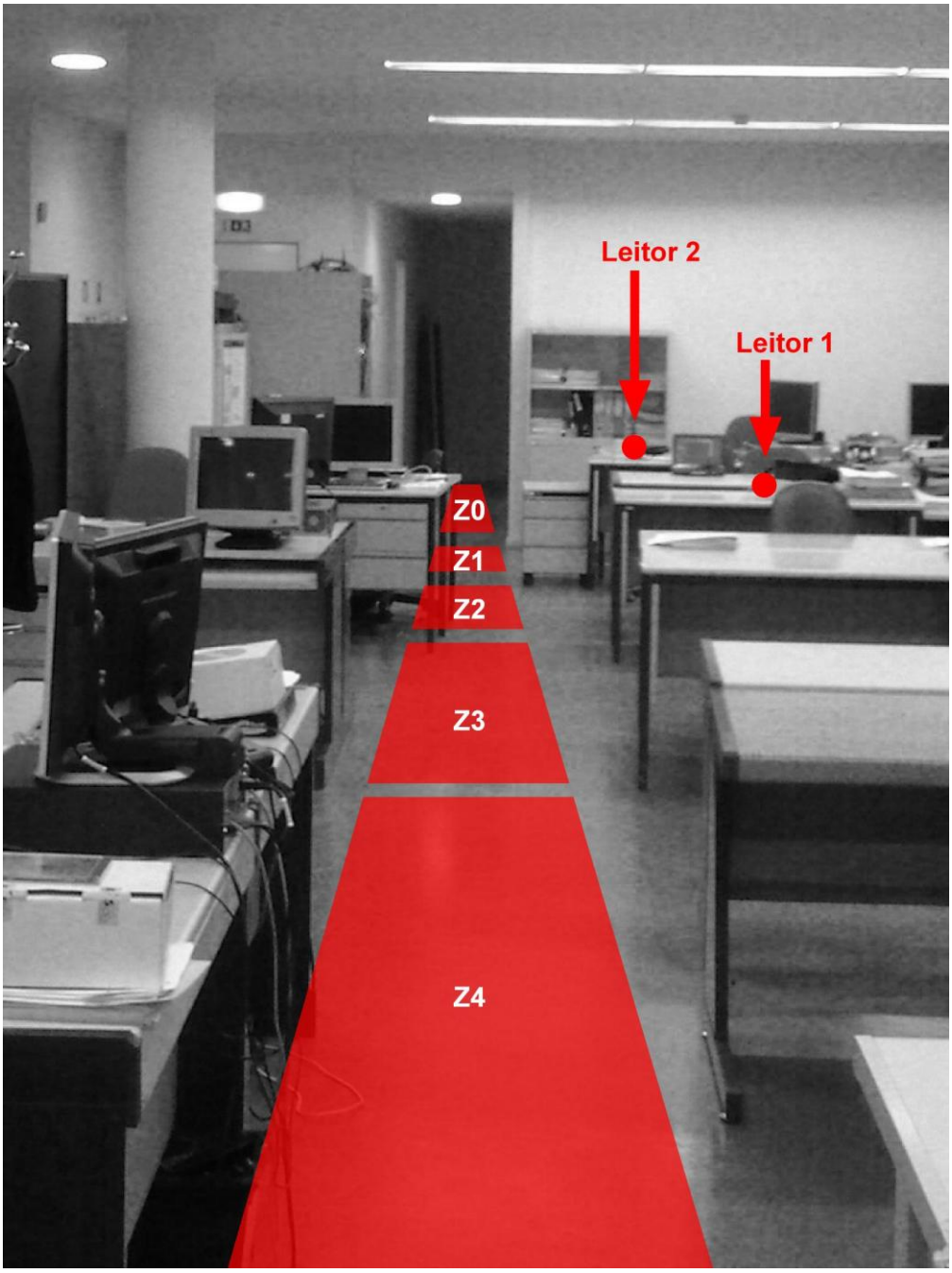

Figura 5-3 – Fotografia do espaço de testes 1, 2 e 3 com representação das zonas e localização dos leitores

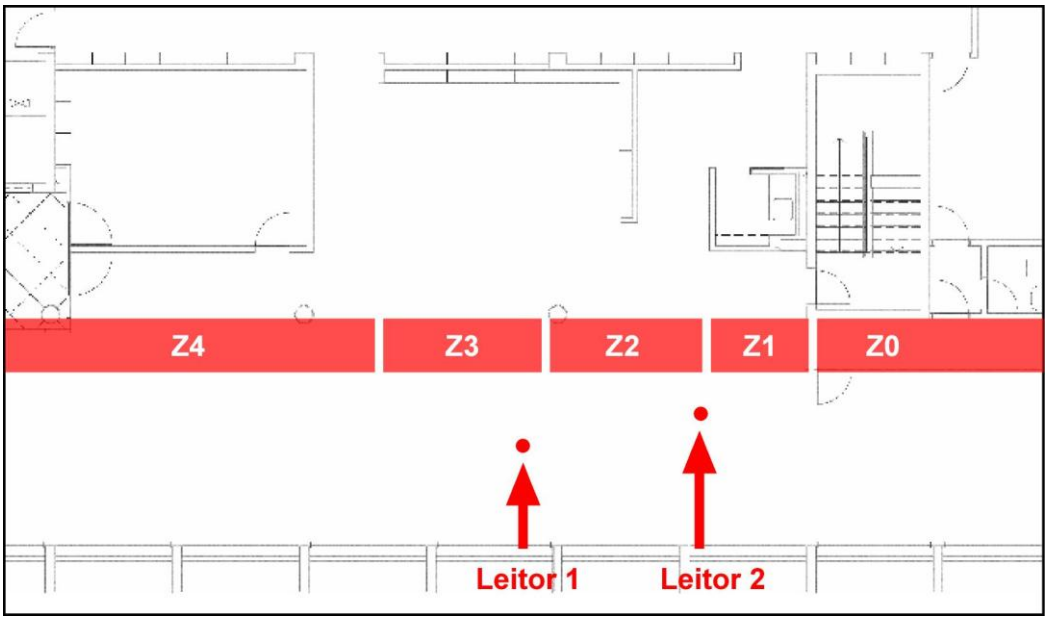

Figura 5-4 – Planta do espaço de testes 1, 2 e 3 com representação das zonas e localização dos leitores

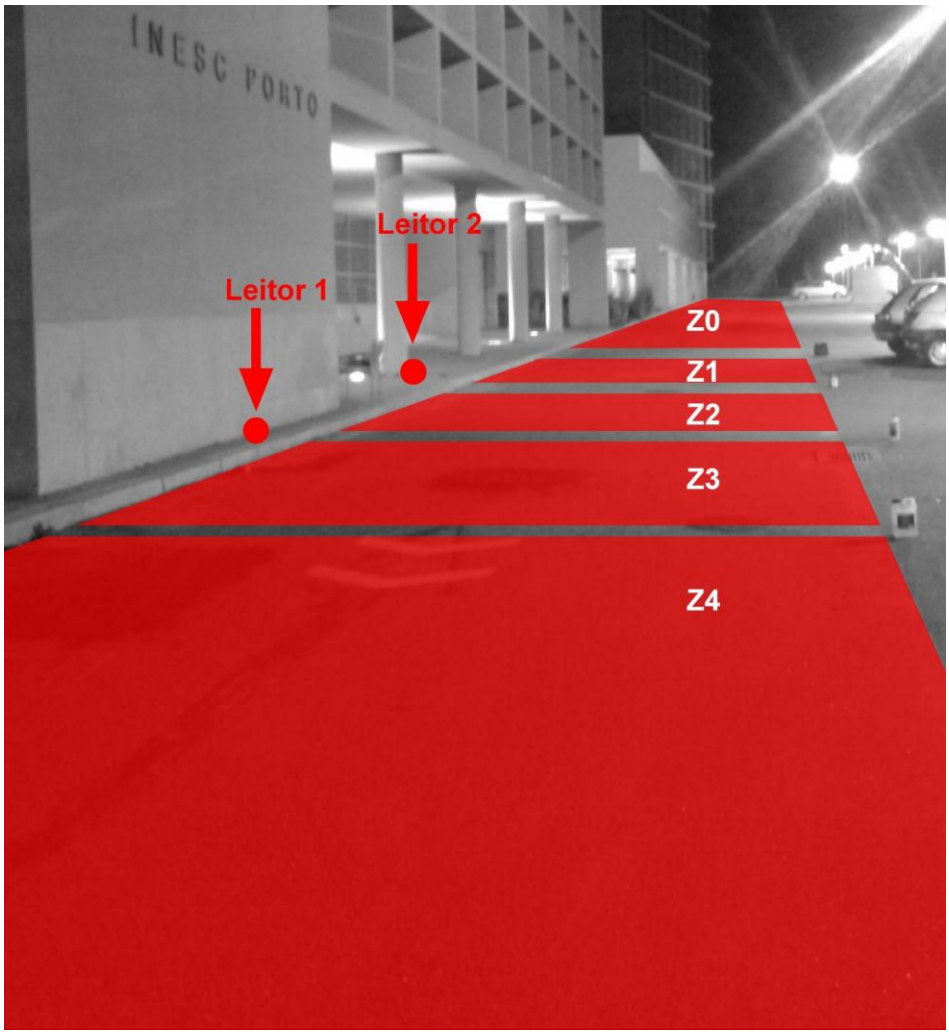

Figura 5-5– Fotografia do espaço do teste 4 com representação das zonas e localização dos leitores

5.5 Programa de testes

A decisão da zona é feita ao segundo, a não ser que chegue um *beacon* de uma *tag* e, nesse caso, a decisão é tomada logo de seguida.

De forma a considerar que uma *tag* está fora do alcance, o algoritmo tem que estar 5 segundos sem receber qualquer trama.

Em seguida apresenta-se a parte do código que implementa o algoritmo de decisão de zona.

```
t_actual = time(&time_s);
t_actual_atraso = t_actual-5;

      //Both readers detect tag
      if(t_actual_atraso < tag.arrival_time2
      &&t_actual_atraso < tag.arrival_time1){
            return 2; //zone
```

```
}
//Was in zone 3, and now is out of range of Z3 Reader
if (t_actual_atraso >= tag.arrival_time2 && zone == 3 ){
      return 4;    //zone
}
//Was in zone 1, and now is out of range of Z1 Reader
if (t_actual_atraso >= tag.arrival_time1 && zone == 1){
      return 0;    //zone
}
//Out of range of both readers
if (t_actual_atraso >= tag.arrival_time2
&& t_actual_atraso >= tag.arrival_time1  ){
      return zone;    //zone
}
if (t_actual_atraso >= tag.arrival_time2
&& t_actual_atraso < tag.arrival_time1  ){
      return 1; //zone
}
if (t_actual_atraso >= tag.arrival_time1
      && t_actual_atraso < tag.arrival_time2  ){
      return 3;    //zone
}
```

5.6 Resultados

Os resultados para os testes 1, 2 e 3, foram obtidos percorrendo as cinco zonas definidas na Figura 5-3 e Figura 5-4. Para o teste 4 os resultados foram obtidos percorrendo as cinco zonas definidas na Figura 5-5.

Os percursos dos testes podem ser vistos abaixo. Em cada teste o percurso foi repetido no mínimo cinco vezes.

- Teste 1 – Z2 Z1 Z0 Z1 Z2 Z3 Z4 Z3 Z2
- Teste 2 - Z2 Z1 Z0 Z1 Z2
- Teste 3 - Z2 Z3 Z4 Z3 Z2
- Teste 4 - Z2 Z1 Z0 Z1 Z2 Z3 Z4 Z3 Z2 (área aberta)

Os resultados obtidos e consequente tratamento estatístico dos testes estão expostos na tabela seguinte.

Tabela 5-1 – Resultados e tratamento estatístico dos testes efectuados

Teste 1

Zonas detectadas \ Zonas Marcadas previamente	Z0	Z1	Z2	Z3	Z4
Z0	54	14	2	1	0
Z1	21	22	18	1	0
Z2	1	14	24	10	0
Z3	0	4	24	39	41
Z4	0	0	0	7	52

Total de Leituras	349
Percentagem de leituras correctas	54,73%
Percentagem de leituras correctas ou em zonas contiguas	97,42%
Erro de amostragem (Distr. Normal Int.Conf. 95% e p=0,5)	5,246%

		Marcado Zona	Marcado N zona
Z0	Zona	71,05%	6,23%
	N zona	28,95%	93,77%
Z1	Zona	40,74%	13,38%
	N zona	59,26%	86,62%
Z2	Zona	35,29%	8,90%
	N zona	64,71%	91,10%
Z3	Zona	67,24%	23,71%
	N zona	32,76%	76,29%
Z4	Zona	55,91%	2,73%
	N zona	44,09%	97,27%

Teste 2

Zonas detectadas \ Zonas Marcadas previamente	Z0	Z1	Z2	Z3	Z4
Z0	46	12	1	0	0
Z1	18	17	10	0	0
Z2	12	17	28	0	0
Z3	0	3	6	0	0
Z4	0	0	0	0	0

Total de Leituras	170
Percentagem de leituras correctas	53,53%
Percentagem de leituras correctas ou em zonas contiguas	90,59%
Erro de amostragem (Distr. Normal Int.Conf. 95% e p=0,5)	7,516%

		Marcado Zona	Marcado N zona
Z0	Zona	60,53%	13,83%
	N zona	39,47%	86,17%
Z1	Zona	34,69%	21,05%
	N zona	65,31%	78,95%
Z2	Zona	62,22%	23,20%
	N zona	37,78%	76,80%
Z3	Zona		5,29%
	N zona		94,71%
Z4	Zona		
	N zona		

Teste 3

Zonas detectadas \ Zonas Marcadas previamente	Z0	Z1	Z2	Z3	Z4
Z0	0	0	0	0	0
Z1	0	0	2	2	0
Z2	0	0	15	14	0
Z3	0	0	20	44	31
Z4	0	0	1	6	48

Total de Leituras	183
Percentagem de leituras correctas	58,47%
Percentagem de leituras correctas ou em zonas contiguas	98,36%
Erro de amostragem (Distr. Normal Int.Conf. 95% e p=0,5)	7,244%

		Marcado Zona	Marcado N zona
Z0	Zona		
	N zona		
Z1	Zona		2,37%
	N zona		97,63%
Z2	Zona	39,47%	9,66%
	N zona	60,53%	90,34%
Z3	Zona	66,67%	43,59%
	N zona	33,33%	56,41%
Z4	Zona	60,76%	6,73%
	N zona	39,24%	93,27%

Teste 4

Zonas detectadas \ Zonas Marcadas previamente	Z0	Z1	Z2	Z3	Z4
Z0	35	7	9	1	0
Z1	23	63	27	6	0
Z2	0	11	37	13	0
Z3	0	0	7	24	1
Z4	0	0	3	13	40

Total de Leituras	320
Percentagem de leituras correctas	62,19%
Percentagem de leituras correctas ou em zonas contiguas	94,06%
Erro de amostragem (Distr. Normal Int.Conf. 95% e p=0,5)	5,478%

		Marcado Zona	Marcado N zona
Z0	Zona	60,34%	6,49%
	N zona	39,66%	93,51%
Z1	Zona	77,78%	24,03%
	N zona	22,22%	75,97%
Z2	Zona	44,58%	10,13%
	N zona	55,42%	89,87%
Z3	Zona	42,11%	3,04%
	N zona	57,89%	96,96%
Z4	Zona	97,56%	5,73%
	N zona	2,44%	94,27%

Na Tabela 5-1 à esquerda, são apresentados os resultados obtidos dos testes efectuados. Em cada elemento da matriz estão os valores obtidos a cada decisão de zona, representando a cada segundo as decisões certas e erradas. A diagonal principal da matriz apresenta as decisões correctas e todos os restantes elementos da matriz, decisões erradas. Na mesma tabela, ao centro, é feito o tratamento estatístico dos resultados, de ressalvar o erro de amostragem (e) calculado a partir do número de amostras (n), intervalo de confiança de 95% (de onde se obtém Z), e grau de variação da população amostrada (p), sendo 50% o pior caso. Como está exposto na fórmula da Figura 2-1.(20)

$$e = \pm \sqrt{\frac{Z^2 p(1-p)}{n}}$$

Figura 5-6 – Equação para o cálculo do erro de amostragem

Ainda na Tabela 5-1 à direita é feita uma análise de erro (Tipo I e Tipo II), para cada uma das zonas. A tabela abaixo ilustra esta análise.

Tabela 5-2 - análise de erro (Tipo I e Tipo II)

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Localização real da tag</td></tr>
<tr><td>Na zona analisada</td><td>Fora da zona analisada</td></tr>
<tr><td rowspan="2">Localização da tag
fornecida pela aplicação</td><td>Na zona analisada</td><td>Positivo verdadeiro</td><td>Falso Positivo
Erro tipo I</td></tr>
<tr><td>Fora da zona analisada</td><td>Falso Negativo
Erro tipo II</td><td>Negativo verdadeiro</td></tr>
</table>

Na Tabela 5-3 foi feito também o tratamento dos dados de forma a evidenciar a passagem pelo ponto de acesso, sendo agregadas as zonas em que a *tag* é detectada pelos leitores e procedendo a um tratamento estatístico análogo ao efectuado sobre os dados originais

Tabela 5-3 Agregação dos dados e tratamento estatístico baseados nos mesmos

Teste 1

Zonas detectadas \ Zonas Marcadas previamente	Z0	Z123	Z4
Z0	54	17	0
Z123	22	156	41
Z4	0	7	52

Total de Leituras	349
Percentagem de leituras correctas	75,07%
Erro de amostragem (Distr. Normal Int.Conf. 95% e p=0,5)	5,246%

		Marcado Zona	N zona
Z0	Zona	71,05%	6,23%
	N zona	28,95%	93,77%
Z123	Zona	86,67%	37,28%
	N zona	13,33%	62,72%
Z4	Zona	55,91%	2,73%
	N zona	44,09%	97,27%

Teste 2

Zonas detectadas \ Zonas Marcadas previamente	Z0	Z123	Z4
Z0	46	13	0
Z123	30	81	0
Z4	0	0	0

Total de Leituras	170
Percentagem de leituras correctas	74,71%
Erro de amostragem (Distr. Normal Int.Conf. 95% e p=0,5)	7,516%

		Marcado Zona	N zona
Z0	Zona	60,53%	13,83%
	N zona	39,47%	86,17%
Z123	Zona	86,17%	39,47%
	N zona	13,83%	60,53%
Z4	Zona		
	N zona		

Teste 3

Zonas detectadas \ Zonas Marcadas previamente	Z0	Z123	Z4
Z0	0	0	0
Z123	0	97	31
Z4	0	7	48

Total de Leituras	183
Percentagem de leituras correctas	79,23%
Erro de amostragem (Distr. Normal Int.Conf. 95% e p=0,5)	7,244%

		Marcado Zona	N zona
Z0	Zona		
	N zona		
Z123	Zona	93,27%	39,24%
	N zona	6,73%	60,76%
Z4	Zona	60,76%	6,73%
	N zona	39,24%	93,27%

Teste 4

Zonas detectadas \ Zonas Marcadas previamente	Z0	Z123	Z4
Z0	35	17	0
Z123	23	188	1
Z4	0	16	40

Total de Leituras	320
Percentagem de leituras correctas	82,19%
Erro de amostragem (Distr. Normal Int.Conf. 95% e p=0,5)	5,478%

		Marcado Zona	N zona
Z0	Zona	60,34%	6,49%
	N zona	39,66%	93,51%
Z123	Zona	85,07%	24,24%
	N zona	14,93%	75,76%
Z4	Zona	97,56%	5,73%
	N zona	2,44%	94,27%

5.7 Discussão de Resultados

Os resultados foram obtidos com a *tag* ao nível do peito, logo quando nos afastamos da posição de qualquer leitor temos o corpo como barreira entre a *tag* e o leitor criando uma atenuação considerável fazendo com que o leitor deixe de detectar a *tag* mais cedo do que esperado. De forma idêntica, ao aproximarmo-nos, existe uma probabilidade de sermos detectados pelo leitor, visto que desta forma não existem obstáculos entre a *tag* e o leitor.

Outro factor a ter em consideração é o tempo de espera até considerar a *tag* fora do alcance, neste caso 5 segundos. Este atraso é, na maior parte dos casos, responsável pela demora na decisão aquando da passagem entre zonas, causando um efeito de histerese na tomada de decisão. Este efeito é mais facilmente observado nos resultados aquando da passagem para as zonas cegas Z0 e Z4. Chama-se a atenção para o número elevado de decisões erradas quando a zona real é Z4 e a detectada é Z3 ou quando a zona real é Z0 e a detectada é Z1. Este efeito não é muito relevante, visto que a passagem para a zona cega é sempre detectada. Este efeito seria mitigado diminuindo o tempo de espera para considerar a *tag* fora de alcance, mas para tal seria necessário diminuir o intervalo entre *beacons* das *tag* o que com este equipamento não é possível.

A utilização de um sistema RFID com maior alcance (incorporando a antena nas *tags*) e necessariamente maior espaçamento entre leitores, como está patente no teste 4, faz com que a solução se comporte melhor, porque aumenta a probabilidade de recepção de pelo menos uma trama pelos leitores a cada passagem.

Como está patente na Figura 5-3, e no que diz respeito aos primeiros três testes, o espaço de testes não é ideal, sendo muito propenso a reflexões e atenuação do sinal enviado pelas *tags*. No entanto, e não obstante as adversidades, a solução revelou-se bastante robusta, detectando quase sempre as passagens pelo ponto de acesso como está mais patente na Tabela 5-3.

Capítulo 6

6. Conclusões e Trabalho Futuro

Neste capítulo é feita uma análise crítica do trabalho desenvolvido até aqui. Também são dadas sugestões para melhoramentos futuros

6.1 Satisfação dos objectivos

O modelo ficou estruturalmente bem especificado e de acordo com os requisitos. A natureza modular e aberta dão ao modelo uma flexibilidade e simplicidade notórias face a outras soluções. A especificação das mensagens entre módulos merecia mais detalhe, ficando, em alguns casos, aquém do desejado. No entanto, o nível de detalhe desejado só seria atingido com uma implementação integral do modelo.

6.2 Trabalho futuro

O trabalho futuro deve incluir uma descrição mais completa do modelo, principalmente os módulos de comunicação com a base de dados, os módulos que são responsáveis pela comunicação com barreiras físicas e dispositivos informativos.

O protocolo de comunicação entre módulos poderia ser mais robusto, com a implementação de *handshakes* para o início de comunicação entre módulos e confirmações de mensagens recebidas. Para além disso a implementação de mecanismos para o registo automático em alguns módulos de forma que dispensem a respectiva configuração.

6.3 Considerações finais

Embora longe de um produto comercial, penso que este trabalho apresenta uma nova abordagem às soluções de localização e controlo de acessos, contendo alguns conceitos e ideias interessantes que fariam baixar drasticamente o custo de implantação desse tipo de sistemas.

Referências

1. **Bhuptani Manish, Moradpour Shahram.** *RFID Field Guide: Deploying Radio Frequency Identification Systems.* s.l. : Prentice Hall PTR, 2005. 0-13-185355-4.

2. **Dobkin, Daniel M.** *The RF in RFID : passive UHF RFID in practice.* Burlington, USA : Elsevier, 2008. 978-0-7506-8209-1.

3. **München, Carl Hanser Verlag.** *RFID-Handbuch.* s.l. : Hanser, 2006.

4. **Himanshu Bhatt, Bill Glover.** *RFID Essentials.* s.l. : O'Reilly, 2006. 0-596-00944-5.

5. *EPC Gobal WebSite.* [Online] http://www.epcglobalinc.org/standards/TagClassDefinitions_1_0-whitepaper-20071101.pdf.

6. *NXP Semiconductors.* [Online] http://www.nxp.com.

7. *A Practical Attack on the MIFARE Classic.* **Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia.** Netherlands : s.n.

8. *NXP Semiconductors.* [Online] http://www.nxp.com/#/pip/pip=[pfp=53424]|pp=[t=pfp,i=53424].

9. *ZigBee Alliance.* [Online] http://www.zigbee.org.

10. **Sousa, Daniel Marcos Fernandes.** *Redes ad hoc como uma extensão da infra-estrutura.* 2007.

11. *Moxa Inc.* [Online] http://www.moxa.com/.

12. **Octal, Engenharia de Sistemas, SA.** SISTEMA DE BILHÉTICA E CONTROLO DE ACESSOS A RECINTOS DESPORTIVOS. 2007.

13. *SKIDATA Global Website.* [Online] http://www.skidata.com/.

14. Hospital personnel localization system. *Kimaldi Electronics.* [Online] http://www.kimaldi.com/kimaldi_eng/sectores/geriatricos_y_centros_sanitarios/sistema_de_localizacion_de_personal_hospitalario_mediante_rfid_activa.

15. Active RFID tag SYTAG245-TM-BA1-G. *Kimaldi Electronics.* [Online] http://www.kimaldi.com/kimaldi_eng/productos/sistemas_rfid/lectores_rfid_y_tags_activos/tags_rfid_activos/tag_rfid_activo_sytag245_tm_ba1_g.

16. Ekahau RTLS. *Ekahau, Inc.* [Online] http://www.ekahau.com/?id=4200.

17. *A Friis-based Calibrated Model for WiFi Terminals Positioning.* **Frédéric Lassabe, Philippe Canalda, Pascal Chatonnay, François Spies.** 25201 Montbéliard Cedex, France : s.n.

18. Ananiah electronics. [Online] http://www.ananiahelectronics.com/RF8315R-s.htm.

19. Ananiah electronics. [Online] http://www.ananiahelectronics.com/RF8315T.htm.

20. *Determining Sample Size.* **Israel, Glenn D.** s.l. : University of florida, 1992. PEOD6.

21. *Active RFID Tag in Real Time Location System.* **sourish behera, Chandan Maity.** CDAC Noida : s.n.

22. *An Improvement Approach of Indoor Location Sensing Using Active RFID.* **Sung-Tsun Shih, Kunta Hsieh, and Pei-Yuan chen.**

23. **Huang, Zhibin Zhou and Dijiang.** 2007.