Pedro André Rodrigues Simão

Controlo de Assiduidade com Multiposto e Comunicações Wireless

Pedro André Rodrigues Simão

Controlo de Assiduidade com Multiposto e Comunicações Wireless

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações (Mestrado Integrado), realizada sob a orientação científica do Dr. José Alberto Gouveia Fonseca, Professor Associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

O júri

Presidente

Doutor António Ferreira Pereira de Melo
Professor Catedrático da Universidade de Aveiro

Vogais

Doutor Mário Jorge de Andrade Ferreira Alves
Professor Coordenador do Departamento de Engenharia Electrotécnica do Instituto Superior de Engenharia do Porto

Doutor José Alberto Gouveia Fonseca
Professor Associado da Universidade de Aveiro (Orientador)

Doutor Alexandre Manuel Moutela Nunes da Mota
Professor Associado da Universidade de Aveiro (Co-Orientador)

Agradecimentos

Agradeço à Micro I/O pelo apoio técnico e pela disponibilização das suas instalações e equipamentos essenciais na realização deste trabalho. Um agradecimento especial ao Pedro Alvarenga pelo apoio no desenvolvimento e assemblagem das placas de circuito impresso.

Aos meus orientadores prof. José Alberto Fonseca e prof. Alexandre Mota pela orientação exemplar, pelas sábias dicas essenciais no desenvolvimento de todo o sistema e pelos conhecimentos transmitidos.

Agradeço ainda a todos os professores, colegas e amigos da Universidade de Aveiro aos quais devo a minha formação académica.

Aos meus pais, irmão, restantes familiares e amigos pela amizade, apoio e carinho. À minha namorada Carol pelo constante apoio.

A todos, o meu muito obrigado!

Palavras-Chave

Controlo de assiduidade, gestão de acessos, comunicações sem fios, *WPANs*, *ZigBee,* reconhecimento biométrico, impressão digital.

Resumo

A crescente competitividade entre o sector industrial aliada às evoluções tecnológicas tem dado lugar à introdução de mecanismos automáticos que procuram a eficiência dos recursos humanos. Sistemas de controlo de assiduidade em ambientes industriais são um exemplo de uma ferramenta automática de gestão dos recursos humanos.

No âmbito desta dissertação é proposto um sistema de controlo de assiduidade com múltiplas estações de validação e com comunicações sem fios, designado por *Wireless Temp I/O*. A abordagem sem fios permite que a importação do sistema de controlo de assiduidade seja facilitada aquando da alteração da disposição da empresa. A existência de múltiplos postos permite a integração de várias estações de registo nos diferentes acessos ao espaço laboral, permitindo o controlo de acessos físico ao mesmo.

De forma a garantir a fiabilidade na identificação de funcionários é utilizada a emergente tecnologia biométrica.

Nesta dissertação são apresentados estudos comparativos das tecnologias biométricas e de comunicações sem fios assim como a arquitectura e caracterização técnica do sistema de controlo de assiduidade.

Keywords

Time attendance systems, access managment, wireless communications, *WPANs*, *ZigBee,* biometric recognition, fingerprint.

Abstract

The increasing competitiveness among the industry allied to technological developments has given rise to the introduction of automatic mechanisms seeking the efficiency of human resources. An employee's attendance control system is an example of an automated tool for the management of human resources in industrial environments.

This dissertation concerns the development of an attendance system with multiple stations of time record and wireless communications, named *Wireless Temp I/O*. The wireless approach allows the enterprise layout to be changed and that the attendance system to be redeployed easily. The existence of multiple stations allows the integration of several stations for time record in the different access to workplace, as well as makes it possible to control physical access to it.

To ensure the identification reliability of employees is used the emerging biometric technology.

In this dissertation are presented comparative studies of biometric technologies and wireless communications as well as the architecture and technical characterization of the attendance system.

Índice de conteúdos

1 Introdução....1.1
1.1 .Descrição geral....1.1
1.2 .Estrutura da dissertação....1.2

2 Registo de assiduidade e o produto Temp I/O....2.1
2.1 .Introdução....2.1
2.2 .Registos de tempos e controlo de acessos nas empresas....2.1
2.3 .Objectivos, operação e arquitectura de um produto: o Temp I/O....2.2
2.3.1 FrontOffice....2.2
2.3.2 BackOffice....2.3

3 Tecnologias de identificação biométrica....3.1
3.1 .Introdução....3.1
3.2 .Vista geral das tecnologias biométricas....3.1
3.2.1 Voz....3.4
3.2.2 Face....3.6
3.2.3 Iris....3.7
3.2.4 Geometria da mão....3.9
3.3 .Impressão digital....3.9
3.3.1 Princípio de Funcionamento....3.10
3.3.2 Tecnologia....3.11
3.3.3 Módulos Comerciais....3.12
3.3.4 Módulos Comerciais Suprema....3.15

4 Tecnologias de comunicações sem fios para redes pessoais....4.1
4.1 .Introdução....4.1
4.2 .Bluetooth....4.1
4.2.1 Topologia de rede....4.2
4.2.2 Arquitectura....4.2
4.3 .Wifi....4.4
4.3.1 Arquitectura....4.4
4.3.2 Topologia de rede....4.6
4.4 .UWB – Ultra Wide Band....4.6
4.5 .ZigBee....4.8
4.5.1 Pilha Protocolar....4.8
4.5.2 Camada Física....4.9
4.5.3 Controlo de Acesso ao Meio....4.10
4.5.4 Camada de rede....4.12
4.5.5 Camada de Aplicação....4.14
4.5.6 Serviços de segurança....4.16
4.6 .Soluções Comerciais ZigBee....4.16
4.6.1 Transceptores IEEE 802.15.4....4.17
4.6.2 Soluções embebidas....4.17
4.6.3 XBee/XBee-PRO da MaxStream....4.21

5 Arquitectura, operação e caracterização técnica do sistema Wireless Temp I/O....5.1
5.1 .Introdução....5.1
5.2 .Arquitectura do sistema Wireless Temp I/O....5.2
5.2.1 Data sink....5.3
5.2.2 Estações remotas....5.4
5.3 .Modo de utilização das estações remotas....5.5
5.4 .Máquina de estados dos WVMs....5.5
5.4.1 Inicialização....5.6
5.4.2 Identificação....5.6
5.4.3 Configuração....5.7
5.5 .Comunicações sem fios....5.8
5.5.1 Protocolo wireless Temp I/O....5.9

5.6 .Caracterização técnica.....5.11
5.6.1 Data sink.....*5.11*
5.6.2 Módulos locais WVM.....*5.14*

6 Ensaio e avaliação do desempenho.....6.1
6.1 .Introdução.....6.1
6.2 .Módulo de impressões digitais.....6.1
6.3 .Ensaio dos módulos de comunicação wireless.....6.2
6.3.1 Indoor.....*6.2*
6.3.2 Outdoor.....*6.3*
6.3.3 Medição da latência.....*6.4*
6.4 .Overhead computacional dos módulos WVM.....6.4
6.5 .Ensaio do sistema com ligação ponto-a-ponto.....6.6
6.6 .Ensaio do sistema com ligação ponto-multiponto.....6.6

7 Conclusões e trabalhos futuros.....7.1

Índice de Figuras

Figura 2.1: Aplicação FrontOffice do sistema Temp I/O. Janela de selecção de operação [2].....2.3
Figura 2.2: Aplicação BackOffice com os diversos menus [2].....2.4
Figura 3.1: Diagrama de blocos de um sistema biométrico genérico [5].....3.3
Figura 3.2: Parâmetros de classificação de um sistema biométrico [7].....3.4
Figura 3.3: Componentes de um sistema genérico de identificação por reconhecimento de voz [4].....3.5
Figura 3.4: Eigenfaces usadas no processo PCA [13].....3.6
Figura 3.5: Diversas classes para a abordagem LDA do reconhecimento facial [12].....3.7
Figura 3.6: Grelha de elásticos, a base do processo de Elastic Bunch Graph Matching [14].....3.7
Figura 3.7: Constituição do olho humano à esquerda [17] e estrutura da iris à direita [18].....3.8
Figura 3.8: Fronteiras da iris através de IrisCode [16].....3.8
Figura 3.9: Esquerda: Imagem retirada com uma câmara CCD incluindo imagens de espelho. Direita:Exemplos de medições de distâncias [20].....3.9
Figura 3.10: Características de uma impressão digital. a,b) loop; c) whorl; d) arch e)tented arch [9]. 3.11
Figura 3.11: Ilustração de uma minutiae (círculos pretos) e poros (círculos transparentes) [9].....3.12
Figura 3.12: Módulo OEM Liahren, o LHID-FM200A [60] 3.13
Figura 3.13: Gama de soluções OEM da Nitgen [21].....3.14
Figura 3.14: SFM3000 com leitor capacitivo.....3.16
Figura 3.15: Estrutura de mensagens dos leitores Suprema para interface de rede (Network Packet Protocol).....3.17
Figura 4.1: Topologia de rede Bluetooth.[26].....4.2
Figura 4.2: Pilha protocolar Bluetooth [27].....4.3
Figura 4.3: Perfis Bluetooth [26].....4.4
Figura 4.4: Arquitectura da pilha protocolar da tecnologia IEEE 802.11.....4.4
Figura 4.5: Dispositivos do protocolo IEEE 802.11 [26].....4.5
Figura 4.6: Topologias de rede suportados pelo protocolo IEEE 802.11.[26].....4.6
Figura 4.7: Largura de banda e potência de transmissão autorizadas pela FCC para a tecnologia UWB.....4.7
Figura 4.8: Plataforma UWB da Aliança WiMedia.[31].....4.7
Figura 4.9: Pilha protocolar ZigBee [35].....4.8
Figura 4.10: Estrutura de uma trama PPDU.....4.10
Figura 4.11: Estrutura Superframe [36].....4.10
Figura 4.12: Comunicação para o Coordinator em modo beacon.....4.11
Figura 4.13: Comunicação do Coordinator para outro dispositivo.....4.11
Figura 4.14: Formato de trama da camada MAC.....4.12
Figura 4.15: Topologias de rede ZigBee.....4.13
Figura 4.16: Parâmetros máximos do número de nós numa rede ZigBee.....4.13
Figura 4.17: Protocolo de endereçamento baseado no algoritmo de tree-routing.....4.14
Figura 4.18: Exemplo de encaminhamento por vizinho (Neightbour-routing).....4.14
Figura 4.19: Exemplo de encaminhamento mesh (Mesh-routing).....4.14
Figura 4.20: Diagrama de blocos tipico de um módulo ZigBee.....4.16
Figura 4.21: Módulo ZigBit da Meshnetics (ZDMA1281 – A2).....4.19
Figura 4.22: Módulo IP-Link da Helicomm [46].....4.19
Figura 4.23: Módulo integrado JN5139 da Jennic [53].....4.20
Figura 4.24: Módulo XBee-PRO com antena chip.....4.21
Figura 4.25: Arquitectura dos módulos XBee da Maxstream.....4.22
Figura 4.26: Estrutura das mensagens em modo API [54].....4.22
Figura 5.1: Ilustração da nova proposta do sistema Wireless Temp I/O.....5.2
Figura 5.2: Diagrama de blocos generalizado do sistema.....5.2
Figura 5.3: Arquitectura e ligações entre os periféricos internos à WVM.....5.4
Figura 5.4: Mensagem no LCD referente à data e operação.....5.5
Figura 5.5: Mensagem de LCD para confirmação de operação.....5.5
Figura 5.6: Mensagem de confirmação de operação quando existe falha de conectividade.....5.5
Figura 5.7: Diagrama de estados de operação para uma WVM.....5.6
Figura 5.8: Processo de registo e actualizações para data sink de operações guardadas localmente.....5.7

Figura 5.9: Mapeamento de memória não volátil para registo de períodos de marcação por defeito.....5.8
Figura 5.10: Diagrama de rede sem fios com topologia mesh [1].....5.9
Figura 5.11: Diagrama das comunicações entre o data sink e uma WVM.....5.9
Figura 5.12: Estrutura base de uma trama destinada ao MCU (API wireless Temp I/O).....5.9
Figura 5.13: Fluxo de mensagens para processo de registo de novo utilizador.....5.10
Figura 5.14: Módulos que compõem a interface com o data sink.....5.11
Figura 5.15: Protótipo do gateway.....5.11
Figura 5.16: Diagrama da aplicação Wireless Temp I/O no data sink.....5.13
Figura 5.17: Aplicação de teste do sistema wireless Temp I/O.....5.14
Figura 5.18: Protótipo do módulo WVM.....5.14
Figura 5.19: Arquitectura do software dos módulos WVM.....5.16
Figura 6.1: Localização geográfica dos módulos XBee para o teste Indoor.....6.2
Figura 6.2: Cálculo do tempo de comunicação.....6.4
Figura 6.3: Processo de agrupamento de tramas ZigBee.....6.6
Figura 6.4: Rede ZigBee ipara ensaio ponto-multiponto com 3 saltos.....6.7

Índice de tabelas

Tabela 3.1: Comparação de diversas tecnologias biométricas [9].....3.3
Tabela 3.2: Características dos módulos OEM da Liahren.[60].....3.13
Tabela 3.3: Características dos módulos OEM da Nitgen [21].....3.14
Tabela 3.4: Características dos módulos Secugen [61].....3.15
Tabela 3.5: Características dos módulos Unifinger da Suprema Inc [22]. 3.16
Tabela 3.6: Tramas do protocolo de comunicações Unifinger usadas na aplicação wireless Temp I/O.....3.17
Tabela 3.7: Tempos (em ms) de identificação para os módulos Unifinger da Suprema Inc. 3.18
Tabela 3.8: Valores de FRR para os modos normal e rápido dos módulos Unifinger.....3.18
Tabela 4.1: Descrição das especificações técnicas da camada PHY do standard IEEE 802.15.4 [37].....4.9
Tabela 4.2: Funcionalidades da camada NWK para diferentes dispositivos ZigBee [39].....4.12
Tabela 4.3: Lista de perfis em desenvolvimento [41].....4.15
Tabela 4.4: Características técnicas de diversos transceptores IEEE 802.15.4 comerciais.....4.17
Tabela 4.5: Características técnicas de sistemas integrados ZigBee.....4.18
Tabela 4.6: Características técnicas dos módulos ZigBit [52].....4.19
Tabela 4.7: Características técnicas dos módulos da helicomm [46.....4.20
Tabela 4.8: Características técnicas dos módulos JN5139 da Jennic [53].....4.20
Tabela 4.9: Características técnicas dos módulos XBee [54].....4.21
Tabela 4.10: Exemplos de comandos AT.....4.22
Tabela 5.1: Descrição das base de dados presentes no data sink.....5.3
Tabela 5.2: Campos da base de dados local para registo de operações.....5.6
Tabela 5.3: Tipos de tramas possíveis do protocolo de comunicações wireless Temp I/O.....5.10
Tabela 5.4: Configurações do módulo XBee para a interface do data sink [54].....5.12
Tabela 5.5: Configurações do módulo XBee para a WVM [54].....5.15
Tabela 5.6: Parâmetros configurados no módulo SFM3000 para operar nas WVM do wireless Temp I/O.....5.15
Tabela 6.1: Tempos de matching medidos no leitor Unifinger SFM3000.....6.1
Tabela 6.2: Força de sinal recebido para diferentes módulos e distâncias em ambiente Indoor.....6.3
Tabela 6.3: Valores de RSSI para diferentes distâncias no teste Outdoor.....6.3
Tabela 6.4: Latência obtida em função do baud rate para comunicação unicast.....6.4
Tabela 6.5: Latência XBee para diversos saltos.....6.4
Tabela 6.6: Resultados da taxa de utilização do processador.....6.5
Tabela 6.7: Tempo de execução e taxa de utilização das diferentes tarefas para baudrate de 19200 bps.....6.5
Tabela 6.8: Taxa de identificações com sucesso para periodicidade de 5 segundos.....6.7

Lista de Acrónimos

AES	*Advanced Encryption Standard*
AL	*Application Layer*
AODV	*Adhoc On-Demand Distance Vector Routing*
API	*Application Programmable Interface*
ASCII	*American Standard Code for Information Interchange*
BDF	*Base de Dados de Funcionários*
BDO	*Base de Dados de Operações*
BDT	*Base de Dados de Templates*
BDW	*Base de Dados de WVMs*
CAP	*Contention Access Period*
CCA	*Clear Channel Assessment*
CFP	*Contention Free Period*
CPU	*Central Processing Unit*
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*
DH	*Destination Address High*
DL	*Destination Address Low*
DLL	*Dynamic Link Library*
DSSS	*Direct Sequential Spread Spectrum*
EBGM	*Elastic Bunch Graph Matching*
EEPROM	*Electrically Erasable Programmable Read-Only Memory*
EER	*Equal Error Rate*
FAR	*False Acceptance Rate*
FCC	*Federal Communications Commission*
FFD	*Full Function Device*
FHSS	*Frequency-Hop Spread Spectrum*
FPS	*Fingerprint Sensor*
FRR	*False Rejection Rate*
GTS	*Guaranteed Time Slots*
HMI	*Human Machine Interface*
IEEE	*Institute of Electrical and Electronic Engineers*
ISM	*Industrial Scientific and Medical*
LCD	*Liquid Crystal Display*
LDA	*Linear Discriminant Analysis*
LED	*Ligtht Emitting Diode*
LNA	*Low Noise Amplifier*
LQI	*Link Quality Indication*
LR-WPAN	*Low Rate Wireless Personal Area Network*
MAC	*Medium Access Control*
MCU	*Micro Controller Unit*
MRD	*Modo de Registo Degradado*
MRN	*Modo de Registo Normal*
NWK	*Network*
OEM	*Original Equipment Manufacturer*
OFDM	*Orthogonal Frequency Division Multiplex*
OSI	*Open Systems Interconnections*
PA	*Power Amplification*
PC	*Personal Computer*
PCA	*Principal Components Analysis*
PDA	*Personal Digital Assistant*
PHY	*Physical*
PIN	*Personal Identification System*
RF	*Radio Frequency*
RFD	*Reduced Function Device*
RISC	*Reduced Instruction Set Computer*
SAP	*Service Access Point*
SIP	*System in Package*
SOC	*System On Chip*
UART	*Universal Asynchronous Receiver Transmitter*
USB	*Universal Serial Bus*
UWB	*Ultra Wide Band*
VCP	*Virtual COM Port*
WCM	*Wireless Communication Module*
WLAN	*Wireless Local Area Network*
WPAN	*Wireless Personal Area Network*
WVM	*Wireless Validation Module*
ZC	*ZigBee Coordinator*
ZDO	*ZigBee Device Object*
ZED	*ZigBee End Device*
ZR	*Application Programmable Interface*

Capítulo 1

Introdução

1.1 . Descrição geral

A presente dissertação aborda o estudo e desenvolvimento de um sistema de controlo de assiduidade com múltiplas estações de registo e comunicações sem fios entre os diversos módulos. Este trabalho insere-se no núcleo de I&D da empresa *Micro I/O - Serviços de Electrónica Lda*.

O sistema proposto é baseado num produto desenvolvido e comercializado pela *Micro I/O*, o *Temp I/O*. O referido produto executa o controlo de assiduidade de funcionários em empresas usando identificação por análise da impressão digital. O produto *Temp I/O* possui limitações de operação e de interface com o funcionário. Na sua versão comercial, o módulo de identificação biométrica é conectado fisicamente a um *PC*, sendo esta a interface com o utilizador. Este trabalho visa projectar e desenvolver uma nova interface com o utilizador para o produto *Temp I/O*.

A utilização de sistemas de controlo de assiduidade em ambientes laborais é essencial para que os funcionários procurem um balanço entre a sua vida profissional e familiar. Os processos automáticos de registo de assiduidade garantem fiabilidade no cálculo do tempo de trabalho, sem que existam erros na determinação do mesmo, evitando assim conflitos de interesses entre a entidade patronal e os funcionários. Existem no mercado diversas soluções automáticas de controlo de assiduidade, quer sejam baseados em cartões (*RFID* ou *smartcard*) ou tecnologia biométrica. Sistemas baseados em cartões podem ser ludibriados pois o funcionário pode separar-se do cartão e o registo pode ser efectuado por qualquer outra pessoa. A emergente tecnologia biométrica preenche a lacuna da fiabilidade na identificação de pessoas. Através de tecnologia biométrica os funcionários não necessitam de transportar nenhum identificador, evitando que sejam efectuados registos manuais por esquecimento ou perda do identificador.

A instalação de sistemas de controlo de assiduidade depende da organização do espaço empresarial, o qual pode ser alterado com frequência. Soluções cabladas tradicionais implicam custos de instalação em adição ao custo dos equipamentos sendo para além disso inflexíveis ou, pelo menos, implicam despesas acrescidas sempre que existe mudança na arrumação da empresa. Uma

solução para obviar este problema é a introdução de comunicações sem fios (*wireless*).

O sistema proposto no âmbito deste trabalho permite a existência de múltiplas estações de registo que operam em simultâneo, podendo registar os tempos de entrada e saída de funcionários nos mais diversos pontos de acesso ou de início de trabalho.

A nova proposta para o sistema *Temp I/O* permite o controlo de assiduidade com múltiplos postos de validação, em que a interacção com os utilizadores é simplificada e amigável. A interacção do utilizador é agora efectuada por módulos de validação autónomos com comunicação sem fios com a base de dados de operações. Esta permanece armazenada num *PC* onde existe uma aplicação de gestão. A presente abordagem ao sistema *Temp I/O* permite ainda a introdução de diversas novas funcionalidades ao sistema. A principal funcionalidade introduzida é o controlo de acessos. A possibilidade de existência de múltiplos postos de validação permite que sejam acoplados sistemas mecânicos de abertura de acesso automático. Pretende-se com o controlo de acessos atribuir a cada utilizador diferentes permissões de acesso para diferentes locais controlados por um terminal sem fios.

O objectivo maior desta tese consiste no desenvolvimento de um protótipo funcional do sistema definido também no âmbito desta dissertação. Para a implementação do protótipo é necessária a avaliação das tecnologias a utilizar, definição da arquitectura do sistema, selecção dos componentes comerciais, definição do protocolo de comunicações entre os dispositivos, implementação dos circuitos electrónicos e programação dos diversos componentes.

O presente trabalho foi submetido ao *12th Annual IEEE International Symposium on Consumer Electronics* (*ISCE 2008*) sob a forma de artigo (*Time attendance system with multistation and wireless communicatios [1]*) e aceite para publicação nos *proceedings* da mesma. A *ISCE 2008* decorreu em Vilamoura nos dias 14, 15 e 16 de Abril de 2008.

1.2 . Estrutura da dissertação

A motivação para a utilização de sistemas de controlo de assiduidade em ambientes laborais é destacada no capítulo 2 assim como os cenários de utilização e operação do produto *Temp I/O*.

Um dos objectivos desta dissertação consiste na avaliação das tecnologias a utilizar no sistema. De entre as tecnologias em avaliação é necessário seleccionar uma tecnologia de identificação e uma de comunicações sem fios. No capítulo 3 são estudadas as tecnologias biométricas de identificação, tais como: reconhecimento por voz, face, íris e geometria da mão. A tecnologia de identificação utilizada no sistema *Wireless Temp I/O* é a impressão digital. No capítulo 3 definem-se alguns conceitos inerentes a esta tecnologia.

No capítulo 4 são avaliadas as tecnologias de redes sem fios para redes pessoais: *WPANs* (*Wireless Personal Area Networks*). Entre as tecnologias de comunicações sem fios serão introduzidas as tecnologias *Bluetooth, Wifi* e *UWB.* Será dada especial ênfase à tecnologia *ZigBee* por ter sido seleccionada para implementação da rede de comunicações sem fios.

A arquitectura do sistema é definida no capítulo 5. O sistema é constituído por diversos módulos independentes, pelo que será efectuada uma abordagem modular ao sistema. No capítulo 5 é também apresenta a forma de operação com as interfaces remotas e uma caracterização técnica dos diversos módulos desenvolvidos. Neste capítulo é também definida a arquitectura do sistema global, dos módulos que o compõem e do sistema de comunicações definido.

O capítulo 6 apresenta os resultados dos ensaios realizados ao protótipo do sistema. São apresentados os resultados dos ensaios dos módulos comerciais utilizados, de identificação por impressão digital e das comunicações sem fios, assim como do sistema global.

Por fim, no capítulo 7 são apresentadas as conclusões ao trabalho efectuado nesta dissertação, assim como são enumerados diversos trabalhos futuros a desenvolver tendo em vista a comercialização desta versão do produto *Temp I/O*.

Capítulo 2

Registo de assiduidade e o produto Temp I/O

2.1 . Introdução

O *Temp I/O* é uma solução de controlo de assiduidade baseada em tecnologia de reconhecimento biométrico. O referido produto disponibiliza os registos de tempos de entrada, saída e ausência de funcionários assim como permite calcular os tempos de trabalho de cada funcionário.

A análise deste tipo de informação torna um sistema automático de controlo de assiduidade uma ferramenta adequada para a monitorização do tempo de trabalho de funcionários assim como permite reduzir o esforço disponibilizado para o cálculo dos tempos de trabalho e horas extraordinárias. Este tipo de tarefa é normalmente desempenhado por profissionais dedicados exclusivamente à gestão de recursos humanos. Este capítulo explica a importância da utilização de sistemas de controlo de assiduidade e de acessos em espaços laborais assim como introduz as funcionalidades e modo de operação do produto *Temp I/O*.

2.2 . Registos de tempos e controlo de acessos nas empresas

A crescente competitividade empresarial tem potenciado a introdução de soluções tecnológicas diversas que permitam a maximização da eficiência dos recursos, essencialmente dos recursos humanos.

A determinação automática de tempos de permanência de funcionários em empresas é uma das referidas soluções tecnológicas. Com os relatórios extraídos deste tipo de ferramenta, os gestores de recursos humanos conseguem quantificar a carga de trabalho de cada um dos seus funcionários. A constante vigilância de uma linha de produção pode ser também confirmada através da análise dos tempos de entrada e saída dos funcionários.

Os seguintes pontos indicam algumas das aplicações em que os registos de tempos são fundamentais numa empresa:

- ✔ Verificação das horas de trabalho de um funcionário pelo gestor ou mesmo pelo próprio funcionário.

- ✔ Quantificação das horas extraordinárias executadas por um funcionário.
- ✔ Verificação da constante vigilância de determinada local (confirmação de área vigilada por um segurança) ou tarefa (linhas de produção).

Recentemente, assistiu-se a uma evolução deste tipo de sistemas, desde o simples assinar de um livro de ponto aos mais recentes sistemas automáticos. A utilização de tecnologia biométrica permite o desenvolvimento de aplicações de controlo de assiduidade com um custo reduzido e de elevada fiabilidade.

Os sistemas de controlo de acessos são utilizados em empresas de forma a restringir o acesso apenas a pessoas previamente autorizados. Para o controlo de acessos impõe-se fiabilidade na identificação do funcionário. Tal como os sistemas de controlo de assiduidade, os sistemas de controlo de acessos permitem efectuar relatórios, sendo uma importante ferramenta para a segurança em empresas. O controlo de acessos de forma automática evita a presença de um segurança constantemente a vigiar cada local de acesso reservado.

2.3 . Objectivos, operação e arquitectura de um produto: o Temp I/O

O produto *Temp I/O* permite a extracção dos tempos de entrada e saída de utilizadores de forma fiável e automática. A fiabilidade do sistema é garantida recorrendo a leitores biométricos de impressões digitais.

O produto *Temp I/O* é constituído por um leitor de impressões digitais e um PC. O leitor de impressões digitais extrai a informação biométrica do dedo do utilizador de forma a identificá-lo. A identificação do utilizador permite que o registo seja armazenado em base de dados no PC. A aplicação que corre no PC opera no sistema como gestor da base de dados assim como implementa a interface com o utilizador da aplicação, quer este seja um funcionário ou o gestor/administrador.

De forma a separar as interfaces com os dois tipos de utilizadores referidos foram desenvolvidas duas aplicações visualmente independentes, *FrontOffice* e *BackOffice*.

O leitor biométrico disponibilizado com o produto *Temp I/O* é o *Hamster I* da *Nitgen.* Este dispositivo possui interface USB 2.0 (*Universal Serial Bus versão 2.0*), usa a tecnologia óptica para extracção da impressão digital e possui resolução de 500 dpi. O leitor biométrico é directamente ligado a um PC. O PC pode porém encontrar-se a executar outras tarefas para além da gestão de assiduidade da aplicação *Temp I/O*.

As próximas secções apresentam as funcionalidades e modo de utilização das aplicações *BackOffice* e *FrontOffice* do produto *Temp I/O*.

2.3.1 FrontOffice

A aplicação *FrontOffice* é a interface com os funcionários. A selecção da operação que o funcionário pretende executar assim como o estado da operação realizada são dois processos executados nesta interface.

Existem dois processos possíveis para registo de operação no sistema *Temp I/O*: manual e automático. O método de autenticação manual permite que um utilizador seleccione qual a operação que pretende executar enquanto no método de autenticação automático a operação é configurada previamente segundo diferentes períodos do dia.

Para que um funcionário efectue um registo em modo manual, este tem de colocar o dedo previamente registado no leitor biométrico e seleccionar a operação que pretende efectuar (*Entrada, Saída* ou *Ausência).* O registo de novos funcionários é efectuado através da aplicação *BackOffice.* O sucesso do processo de identificação é informado ao utilizador. Neste passo, o funcionário ainda não completou o registo de operação. A Figura 2.1 ilustra a janela da aplicação *FrontOffice* quando um utilizador acaba de ter sucesso na sua identificação através da análise da impressão digital.

Figura 2.1: Aplicação FrontOffice do sistema Temp I/O. Janela de selecção de operação [2].

Caso o processo de identificação tenha sido executado com sucesso, o utilizador tem de seleccionar qual a operação que pretende efectuar. As possíveis operações são *Entrada, Saída* e *Ausência*. A *Entrada* inicia a contagem das horas de trabalho do funcionário e a *Saída* pára a mesma contagem. A operação *Ausência* é usada quando o funcionário deixa o seu local de trabalho por um curto espaço de tempo, esse tempo não é descontado nas horas de trabalho finais.

Para além do processo de identificação manual existe um método de identificação automático. O processo de autenticação automático consiste na atribuição da operação (*Entrada, Saída* ou *Ausência*), dependendo da configuração efectuada na aplicação *BackOffice*, para determinados períodos de tempo. Neste modo de operação, o funcionário apenas necessita de colocar o dedo no leitor de impressões digitais para efectuar um registo de operação.

Para que os modos de operação manual e automático sejam distinguidos pelos funcionários, existe um sinal sonoro diferente para cada um dos modos de operação. Quando a aplicação *FrontOffice* opera em modo manual, são emitidos três sinais sonoros na aplicação informando o utilizador que este ainda tem de seleccionar a operação a executar. Caso a aplicação opere em modo automático com períodos de marcação pré-definidos apenas é emitido um sinal sonoro, sinalizando o utilizador que a operação foi realizada com sucesso.

2.3.2 BackOffice

A aplicação *BackOffice* permite efectuar configurações do sistema e do leitor biométrico, análise e impressão de relatórios. A execução destas tarefas apenas é possível após a introdução de autenticação de administrador de sistema.

Existem diversas operações passíveis de serem realizadas na aplicação *BackOffice* tais como:

- ✔ Adicionar, editar ou remover grupos de funcionários.
- ✔ Adicionar, editar ou remover funcionários.
- ✔ Visualizar eventos de funcionários.
  - ○ Adicionar, editar ou remover movimentos.
- ✔ Imprimir e visualizar relatórios.
- ✔ Configurar períodos de marcação por defeito.
- ✔ Configurar informação da empresa e outras definições.

A Figura 2.2 apresenta a janela principal da aplicação *BackOffice* do sistema *Temp I/O*. Na figura é possível verificar diversos movimentos efectuados por um utilizador. No canto inferior direito é indicado o número total de horas realizadas pelo utilizador durante o mês seleccionado.

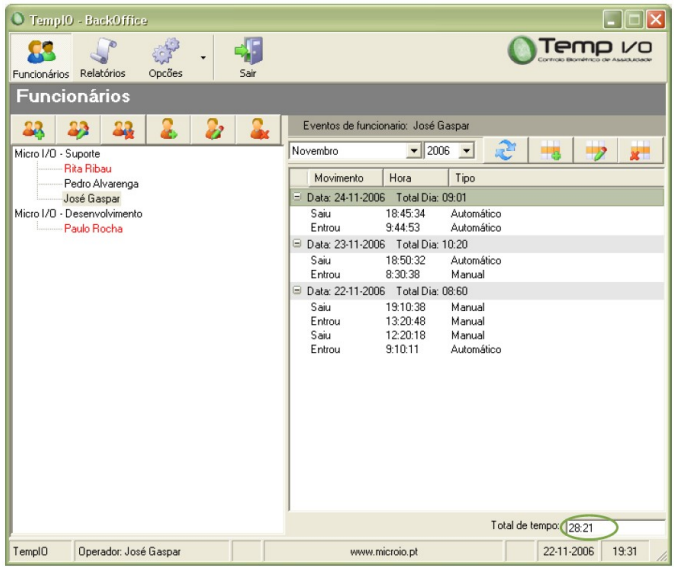

Figura 2.2: Aplicação BackOffice com os diversos menus [2].

A aplicação *BackOffice* possui diversos menus de configuração: *Funcionários, Relatórios* e *Opções*. No menu *Funcionários* é possível adicionar, remover ou editar um funcionário assim como um grupo de funcionários. Neste menu é possível a configuração das permissões de acesso de determinado funcionário à aplicação *BackOffice*. As permissões podem ser totais às configurações em *BackOffice*, apenas aos relatórios ou ser negado o acesso ao *BackOffice*.

Durante o processo de registo de um novo funcionário é necessário proceder à extracção da impressão digital para posterior reconhecimento do utilizador. Este processo de registo de informação biométrica é efectuado durante o processo de registo de funcionário e pode ser alterado a qualquer momento.

De uma forma simplificada podem ser extraídos os relatórios com maior ou menor detalhe de informação. O acesso aos relatórios é efectuado no menu *Relatórios.* O relatório resumido apenas indica o número de horas totais realizado por um funcionário durante um período de tempo. O relatório descritivo possui maior detalhe dos movimentos efectuados. Pode ser ainda extraída uma lista de movimentos que foram editados pelo administrador, sendo dada a informação da operação inicial e da operação modificada assim como quem a alterou e quando.

No menu *Opções* podem ser configurados os períodos de marcação por defeito e as informações da empresa.

Capítulo 3

Tecnologias de identificação biométrica

3.1 . Introdução

Neste capítulo são apresentadas diversas tecnologias de identificação de pessoas baseadas em parâmetros biométricos. Na secção *Vista geral das tecnologias biométricas* explicam-se os factos tidos em conta para a selecção da tecnologia biométrica para a identificação de pessoas no sistema de controlo de assiduidade em desenvolvimento. Serão ainda introduzidos os mecanismos de funcionamento de um sistema biométrico genérico assim como alguns conceitos e definições usuais em sistemas de reconhecimento por biometria.

O reconhecimento de pessoas por análise da impressão digital é apresentado com maior nível de detalhe na secção seguinte, *Impressão digital,* por ser o método de reconhecimento escolhido para o sistema *Wireless Temp I/O*.

A análise das características técnicas de diversos módulos comerciais *OEM* (*Original Equipment Manufacturer*) de diferentes fabricantes é também efectuada neste capítulo.

3.2 . Vista geral das tecnologias biométricas

De entre os diversos métodos de identificação de pessoas, os processos biométricos têm adquirido especial relevância nos últimos anos, sobretudo devido à elevada fiabilidade no reconhecimento de pessoas. Os métodos de identificação podem ser divididos em três tipos diferenciados por [4]:

- ✔ Aquilo que se tem (cartão magnético, chave, ...);
- ✔ Aquilo que se sabe (código *PIN* (*Personal Identification System*), palavra chave, ...);
- ✔ Aquilo que se é (dados biométricos).

Os processos referentes ao *que se tem* e *se sabe* podem ser facilmente ludibriados por utilizadores

mal intencionados relativamente ao sistema. A posse de um objecto de identificação pode ser transmitida ou o mesmo o objecto pode ser extraviado do seu utilizador original. Situação idêntica pode ocorrer para as palavras-chave.

Existem no entanto, diversos sistemas que combinam as vantagens de cada um dos processos, os sistemas híbridos. Estes sistemas combinam a utilização de um cartão com um código secreto. Este tipo de sistema têm grande utilidade quando o utilizador não pretende que outros acedam aos seus dados, tal como a conta bancária (cartão e código PIN). Por outro lado, a utilização da combinação destes sistemas possui reduzida fiabilidade em sistemas em que o utilizador pode ter intenções de ludibriar o sistema, tal como num sistema de controlo de assiduidade.

Recentemente, diversos fabricantes de sistemas de controlo de acessos baseados em biometria e identificação por cartão juntaram estas tecnologias no mesmo sistema. O cartão possui em memória a informação biométrica do utilizador. Estes dados biométricos são transferidos para o sistema de controlo de acessos. Os dados biométricos retirados do cartão são depois comparados com os dados extraídos directamente do utilizador. O acesso apenas é concedido em caso de sucesso no processo de verificação da identidade do utilizador. Estes sistemas possuem vantagem em sistemas multiposto sem rede de comunicações entre os diferentes postos.

O uso da tecnologia biométrica para identificação de pessoas vem preencher a lacuna da fiabilidade dos restantes processos de identificação. O custo de um sistema baseado em biometria pode ser mais elevado no momento de implementação mas o custo de operação é mais reduzido, pois não são necessários elementos físicos adicionais, por exemplo cartões magnéticos.

Após os ataques terroristas de 11 de Setembro de 2001, o nível de segurança na identificação de pessoas aumentou exponencialmente, proporcionando o crescimento na investigação de tecnologias de identificação fiáveis. A tecnologia que mais emergiu foi a biométrica pois em certas condições de utilização permite elevada garantia de fiabilidade. Um elevado número de países decidiram adoptar sistemas biométricos para reforçar a segurança nacional evitando falsas atribuições de identidade. Diversas aplicações têm emergido na área da segurança baseadas em tecnologias biométricas, tais como o controlo de acessos físico e lógico, investigação forense, prevenção e detecção de fraudes e ataques terroristas [5].

A palavra biometria deriva do grego *bio* e *metric* que significam a medição de parâmetros vivos. A biometria é então a ciência da medição de uma característica humana única, tanto física (impressão digital, geometria da mão, retina, íris ou imagens faciais) como comportamental (assinatura, reconhecimento de voz ou ritmo de escrita em teclados) [5].

Um determinado parâmetro biológico pode ser utilizado num sistema biométrico desde que cumpra os seguintes requisitos: [9]

- ✔ *Universalidade*: Todas as pessoas devem possuir a referida característica;
- ✔ *Distintividade*: A característica biométrica deve ser única entre quaisquer dois indivíduos;
- ✔ *Durabilidade*: A característica deve ser invariável por um largo período de tempo.
- ✔ *Coleccionabilidade* A característica deve poder ser medida ou extraída por um mecanismo automático.

Existem ainda outros parâmetros práticos que devem ser tidos em conta nos sistemas biométricos:

- ✔ *Desempenho*: Refere-se à precisão de reconhecimento, velocidade, robustez, quais os requisitos para implementação e que seja operacional segundo variadas condições de operação que possam afectar a precisão do reconhecimento.
- ✔ *Aceitabilidade*: Define o factor de aceitação do dado biométrico entre a sociedade.
- ✔ *Fiabilidade*: Reflecte a capacidade do sistema ser enganado por um impostor através de

técnicas fraudulentas.

Existem diversos processos biométricos com vantagens e desvantagens no desenvolvimento de uma aplicação. A escolha do melhor recurso biométrico para o reconhecimento de utilizadores depende da aplicação em desenvolvimento. Os parâmetros acima mencionados são vulgarmente tidos em conta durante o processo de selecção da tecnologia biométrica. A Tabela 3.1 apresenta o grau de cumprimento dos requisitos definidos atrás para cada um dos parâmetros, tendo em conta as tecnologias biométricas mais estabelecidas.

Tabela 3.1: Comparação de diversas tecnologias biométricas [9].
(A – Alto, M – Médio, B - Baixo)

Tecnologia Biométrica	***Universalidade***	***Distintividade***	***Durabilidade***	***Coleccionabilidade***	***Desempenho***	***Aceitabilidade***	***Fiabilidade***
ADN (Ácido desoxirribonucleico)	A	A	A	B	A	B	B
Face	A	B	M	A	B	A	A
Impressão digital	M	A	A	M	A	M	M
Comportamento ao Andar	M	B	B	A	B	A	M
Geometria da mão	M	M	M	A	M	M	M
Vasos sanguíneos das mãos	M	M	M	M	M	M	B
Iris	A	A	A	M	A	B	B
Ritmo de escrita em teclados (keystroke)	B	B	B	M	B	M	M
Retina	A	A	M	B	A	B	B
Assinatura	B	B	B	A	B	A	A
Voz	M	B	B	M	B	A	A

A generalidade dos sistemas biométricos utiliza o mesmo modo de operação, ilustrado na Figura 3.1. A primeira parte do processo é o registo (*enrollment*). No processo de registo, os dados biométricos relativos ao utilizador são extraídos e armazenados em base de dados. A informação biométrica é extraída através do sensor biométrico. A referida informação é tratada por um algoritmo que simplifica utilizando uma codificação específica a informação extraída. A nova informação resultante do referido algoritmo é denominada por *template*. Apenas o *template* é guardado na base de dados por ser uma representação simplificada da informação biométrica.

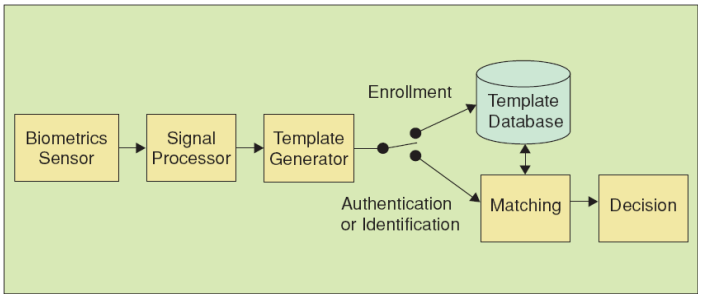

Figura 3.1: Diagrama de blocos de um sistema biométrico genérico [5].

O processo de reconhecimento de um utilizador começa no processo de extracção das

características biométricas deste, transformando-as num *template*. O *template* é posteriormente comparado com os demais armazenados em base de dados. Duas extracções de dois dados biométricos do mesmo utilizador nunca são exactamente iguais, pelo que dificilmente se geram dois *templates* iguais. Assim o processo de *matching* é um processo algo complexo, pois este não se limita à verificação directa entre *templates*, mas apenas à verificação de parte das características dos dois *templates*, o registado e o extraído.

As aplicações de tecnologia biométrica podem-se dividir em dois grupos: *autenticação* e *identificação*. O termo *autenticação* descreve o processo de confirmação da identidade de um utilizador com uma previamente registada num dado sistema. Trata-se de um reconhecimento 1:1 que pretende verificar se o utilizador é realmente quem diz ser. Este processo é também designado por alguns autores por *verificação*. As aplicações do tipo *identificação* consistem num processo de *matching* de um registo biométrico de um utilizador desconhecido com um conjunto de dados previamente registados. O processo de *identificação* refere-se a uma comparação de um para muitos (1:N).

Cada dispositivo de identificação biométrica pode ser avaliado segundo diversos parâmetros. De entre os mais utilizados estão o *False Acceptance Rate* (*FAR*), *False Rejection Rate* (*FRR*) e *Equal Error Rate* (*EER*). Os referidos parâmetros permitem a classificação de um sistema biométrico.

Num sistema biométrico são utilizadas pontuações para expressar a semelhança entre uma informação biométrica extraída e o *template* registado. O acesso ao sistema só é garantido caso a pontuação para um utilizador registado no sistema (cliente) seja superior a um certo limiar. Em teoria, a pontuação de um utilizador registado deve ser sempre superior à pontuação de um impostor. Na prática, este pressuposto nem sempre se verifica.

Num sistema biométrico o *FAR* define a probabilidade do sistema considerar um *template* como válido sendo este falso, ou seja alguém consegue enganar o sistema e uma pessoa desautorizada consegue aceder ao sistema. O *FAR* é definido pela divisão entre *templates* aceites de impostores sobre o número total de *templates* de impostores processados. O *FAR* assume valor 1 se todos os impostores forem aceites como válidos e zero caso nenhum dos impostores seja aceite. O *FRR* é semelhante ao *FAR* mas do ponto de vista dos clientes: O *FRR* consiste no número de *templates* de clientes rejeitados sobre o número total de verificação de clientes.

Existe um ponto em que o *FAR* e *FRR* se intersectam, este ponto é designado de *Equal Error Rate* (*EER*). O *EER* é útil por fornecer uma definição independente do limiar. Quanto menor for o *EER*, melhor é o desempenho do sistema [7].

A Figura 3.2 ilustra graficamente os parâmetros de classificação de sistemas biométricos.

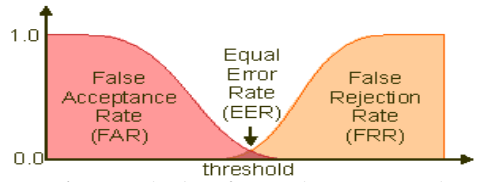

Figura 3.2: Parâmetros de classificação de um sistema biométrico [7].

Nas próximas secções serão introduzidas as tecnologias biométricas mais disseminadas na identificação de pessoas, tais como a voz, geometria da face, íris ocular e a geometria da mão. Na secção seguinte será dada especial relevância à tecnologia de identificação por análise da impressão digital, pois será a usada no âmbito desta dissertação.

3.2.1 Voz

A identificação de pessoas através da análise da sua voz é um dos processos biométricos socialmente mais aceites. A interacção com o utilizador pode ser efectuada sem que este entre em

contacto físico com qualquer equipamento, podendo ser utilizado em diversas aplicações ubíquas que permitem garantir o acesso remotamente, através de rede telefónica por exemplo. O reconhecimento de voz não é um sistema biométrico de elevada distintividade para permitir identificação de um utilizador em bases de dados complexas [9]. Além disso, a forma do sinal vocal pode ser degrada na qualidade devido às distorções introduzidas pelos microfones, canal de comunicação e técnicas de digitalização. Outros factores difíceis de controlar podem também afectar as características da voz, tais como a saúde do utilizador, *stress* e emotividade.

O reconhecimento através da análise da voz baseia-se na estrutura física da voz assim como do comportamento do utilizador ao comunicar [3]. A componente fisiológica está relacionada com a forma física do trato vocal de cada indivíduo, resultante das vias respiratórias e cavidade do tecido vocal. Para produzir discurso, os componentes físico combinam com o movimento físico da maxila, língua e laringe e da ressonância na parede nasal. Os padrões acústicos do discurso provêm então das características físicas das vias respiratórias.

Existem duas formas de reconhecimento por voz, com dependência em relação ao texto e de forma independente ao texto. Num sistema do tipo dependente do texto é indicado ao utilizador qual o discurso que este deve proferir, como por exemplo uma *password* ou uma sequência de algarismos pedidos pelo sistema de validação. Por outro lado, os sistemas independentes do texto não apresentam frases pré definidas, aumentando a flexibilidade do sistema.

O sistema de reconhecimento de voz analisa os dados de frequência do discurso e compara diversas características como qualidade, duração e dinamismo da intensidade. As características de voz referidas são extraídas no momento do registo (*enrollment*) no qual o utilizador diz uma palavra ou frase capturada por um microfone. A amostra de voz extraída é convertida em formato digital, da qual são extraídas as características vocais acima referidas, criando-se o modelo. A maioria das soluções usa o modelo de *Hidden Markov* baseado num modelo aleatório que providencia uma representação estatística dos sons produzidos. Os modelos de *Hidden Markov* modelam as variações temporais e espectrais em simultâneo [15]. O modelo *Gaussian Mixture* cria diversos vectores de características vocais que representam as várias formas sonoras produzidas, que são as características fisiológicas e comportamentais de um indivíduo.

No processo de reconhecimento, as mesmas características de voz (qualidade, duração e volume) são extraídas e comparadas com a amostra previamente registada (*verificação)* ou com diversas amostras de um conjunto possível de utilizadores (*identificação*). Os modelos *anti-speaker* contêm características de diversos indivíduos com excepção da identificação hipotética ou do utilizador. Ambas as amostras do utilizador e da identificação hipotética são comparadas e produzem a probabilidade de serem da mesma pessoa. Se a amostra de entrada pertencer ao utilizador ou à identificação hipotética, a probabilidade irá reflectir que a amostra é semelhante à do utilizador ou à identificação hipotética em relação à do *anti-speaker*.

A Figura 3.3 ilustra o processo genérico de operação de um sistema de reconhecimento por voz.

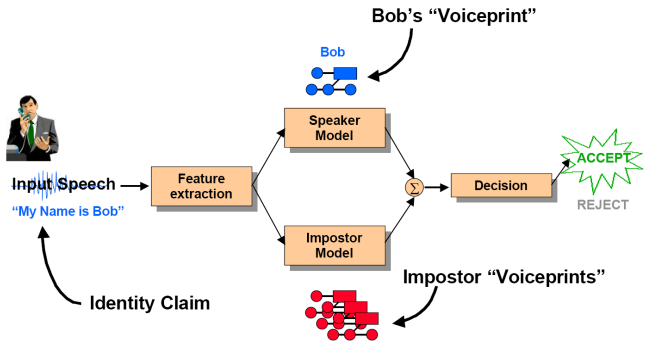

Figura 3.3: Componentes de um sistema genérico de identificação por reconhecimento de voz [4].

3.2.2 Face

O método natural para reconhecimento de pessoas entre interacções visuais usado pelos seres humanos é o reconhecimento facial. Com os avanços da tecnologia, o reconhecimento facial pode também ser processado de forma automática. Existem algoritmos de identificação baseados na simples análise da geometria da face, mas nos últimos anos este processo entrou numa sofisticada ciência de representações matemáticas e de *matching*. O processo de reconhecimento biométrico pela análise da face permite ambos os métodos de *verificação* e *identificação.*

Existem diversos desafios no desenvolvimento de aplicações baseado no reconhecimento facial tais como o uso de disfarces pelos utilizadores, aumento da idade, expressões faciais, cancelamento do ambiente circundante na recolha da imagem, variações na pose em relação à câmara (2D ou 3D).

De entre os diversos algoritmos de reconhecimento facial são apresentados três dos mais relevantes: *Principal Components Analysis* (*PCA), Linear Discriminant Analysis* (*LDA)* e *Elastic Bunch Graph Matching* (*EBGM)*.

A técnica pioneira no reconhecimento facial é a *PCA* que usa o conceito de *eigenfaces.* No processo de *matching PCA,* a *probe* (imagem do utilizador cujo reconhecimento se pretende efectuar) e a *galeria* (base de dados de imagens de utilizadores registados) devem possui o mesmo tamanho e o alinhamento normalizado com os olhos e a boca de ambas as imagens. A abordagem *PCA* reduz a dimensão dos dados ignorando diversas informações que não são úteis. A estrutura da face na imagem é então decomposta em componentes ortogonais, as referidas *eigenfaces*. Cada imagem pode ser representada pela soma ponderada de *eigenfaces*, que são guardadas num vector de uma dimensão. A *probe* é então analisada com a *galeria* medindo a diferença entre a distância das respectivas características. Esta técnica apenas garante sucesso caso seja disponibilizada toda a parte frontal da face [13]. A Figura 3.4 ilustra as *eigenfaces* usadas no processo de *matching PCA.*

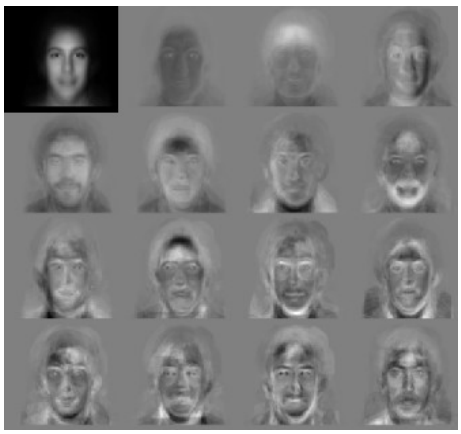

Figura 3.4: Eigenfaces usadas no processo PCA [13].

O algoritmo de reconhecimento facial *LDA* usa uma abordagem estatística para classificação de amostras de classes desconhecidas baseadas nas amostras previamente treinadas de classes conhecidas. O objectivo desta técnica é maximizar a variância entre classes (utilizadores diferentes) e minimizar a variância entre amostras dentro da mesma classe (mesmo utilizador). Quando se processam dados de uma amostra de elevada dimensão, esta técnica enfrenta o problema da pequena dimensão da amostra. O problema da pequena dimensão das amostras verifica-se caso existam poucas amostras treinadas comparadas com a dimensão do espaço da amostra [13].

As imagens de faces possuem diversas características não lineares que não são consideradas nos dois métodos lineares anteriormente apresentados, tais como a variação na iluminação (luz solar ou iluminação artificial), pose (recto ou curvado) e expressões.

Na Figura 3.5 cada rectângulo representa uma classe e em cada classe existem diversas amostras.

Figura 3.5: Diversas classes para a abordagem LDA do reconhecimento facial [12].

O método de *Elastic Bunch Graph Matching* (*EBGM)* considera os efeitos não lineares das imagens extraídas usando uma arquitectura de ligações dinâmicas que transforma a face numa grelha elástica, através de um processo designado por *Gabor wavelet* [13]. Um *Gabor jet* é um nó na referida grelha elástica que descreve o comportamento envolvendo um pixel. O *Gabor jet* resulta da convolução da imagem com um filtro de *Gabor*, que é usado para detecção das formas e para extracção das características da face, usando processamento de imagem. O reconhecimento baseado no método de *EBGM* resulta da semelhança entre a resposta do filtro de *Gabor* em cada nó de *Gabor*. A dificuldade da implementação do método de *EBGM* resulta da necessidade de extracção de coordenadas precisas dos diversos nós. Essa extracção pode ser conseguida com técnicas que combinam os métodos de *PCA* e *LDA*. A Figura 3.6 apresenta a grelha de elásticos usada no método de *EBGM.*

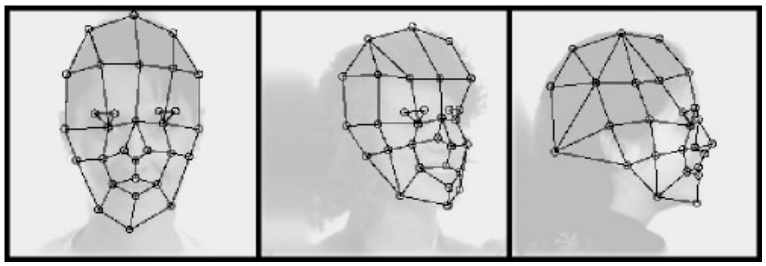

Figura 3.6: Grelha de elásticos, a base do processo de Elastic Bunch Graph Matching [14].

3.2.3 Iris

O reconhecimento pela íris é o método biométrico de reconhecimento de pessoas através da análise dos padrões aleatórios da íris. A íris é o músculo dentro do olho que regula o tamanho da pupila, controlando a quantidade de luz que entra no olho. A íris é a parte colorida do olho. A coloração é por sua vez definida a partir da quantidade de pigmentos de melanina no músculo [16]. A captura da imagem da íris é efectuada através de um processo sem contacto com o utilizador, implicando que o utilizador se deva colocar a uma determinada distância do plano do sensor de extracção. O processo de reconhecimento por análise da íris é um dos processos biométricos mais rápidos e precisos [9].

A coloração e estrutura da íris estão geneticamente ligadas, embora os padrões não o estejam. A iris desenvolve-se durante o período pré-natal crescendo através de um processo de formação regulado de desdobramento do tecido da membrana. Antes do nascimento ocorre a degeneração, resultando na abertura da pupila e dos padrões da íris. Mesmo que dois indivíduos sejam geneticamente idênticos, as suas íris são únicas e estruturalmente diferentes, o que permite a sua utilização como processo biométrico. As duas íris de um mesmo indivíduo são também únicas entre

si. A Figura 3.7 descreve a constituição interna de um olho humano, onde são evidenciadas a pupila, íris e a retina (esquerda) assim como a estrutura da íris (direita).

Figura 3.7: Constituição do olho humano à esquerda [17] e estrutura da íris à direita [18].

O primeiro passo para efectuar reconhecimento através da análise da íris ocular consiste na determinação da localização geográfica desta. As coordenadas e forma da íris permitem posteriores processamentos de imagem, isolamento das características relevantes e extracção da imagem. A localização da íris na imagem extraída é um procedimento importante para o reconhecimento através da análise da íris porque, caso seja efectuada indevidamente, dá origem a ruído (pestanas, reflexões, pupila e pálpebras) conduzindo a um fraco desempenho.

A extracção da informação da íris requer a utilização de câmaras digitais de elevada resolução, tipicamente utilizando radiação infravermelha para iluminar a íris sem prejudicar nem incomodar o utilizador. Após extracção da imagem são aplicados filtros de *Gabor* 2D e segmentação em mapas da íris em fasores. Os fasores incluem informação da orientação, frequência espacial (qual a característica) e posição. Essa informação é usada para mapear o *IrisCode*.

A Figura 3.8 representa a localização das fronteiras da íris definidas através do *IrisCode*.

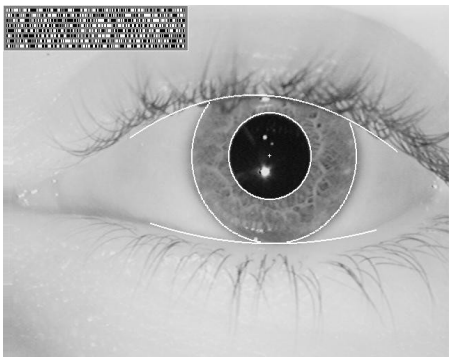

Figura 3.8: Fronteiras da iris através de IrisCode [16].

Os padrões da íris são descritos segundo um *IrisCode* usando a informação de fase retirada dos fasores. A fase não é afectada pelo contraste, ganho da câmara ou nível de iluminação. A característica da fase de uma íris pode ser descrita usando algumas centenas de bytes de dados em sistema de coordenadas polares. Na descrição de uma íris existem mecanismos de exclusão de informação inútil.

Para execução do *matching*, dois *IrisCodes* são comparados, e a diferença entre eles (distância de *Hamming*) é usada como teste de independência estatística entre os dois códigos *IrisCode*. Caso a distância de *Hamming* indique que menos de um terço dos *bytes* da *IrisCode* são diferentes, o *IrisCode* falha o teste de independência estatística, indicando que o *IrisCode* é da mesma íris [16]. A chave do reconhecimento pela íris consiste na falha do teste de independência estatística.

3.2.4 Geometria da mão

Algumas características relacionadas com a mão humana (tamanho e espessura dos dedos) são relativamente peculiares e invariantes num indivíduo, embora não possuam elevada distintividade [9]. Devido a estas limitações, este tipo de recurso biométrico é apenas usado em sistemas de *verificação,* sendo difícil a sua implementação em processos de *identificação*.

A captura de informação acerca da geometria da mão requer a cooperação do utilizador de forma a capturar as vistas frontal e laterais da palma da mão. A palma da mão deve ser colocada num painel de extracção com os dedos esticados. Os requisitos para registo de um *template* baseado em reconhecimento por geometria da mão são mínimos (tipicamente de 9 bytes), o que torna um sistema baseado na geometria da mão atractivo para aplicações de largura de banda e memória reduzidas.

O modo de operação dos dispositivos de reconhecimento por geometria da mão baseia-se na medição e gravação do tamanho, largura, espessura e área de superfície da mão de um individuo quando colocada num vidro do dispositivo. Os sistemas vulgares usam uma câmara *CCD (Charge-Coupled Device*) para captura da silhueta da mão [19]. A imagem esquerda da Figura 3.9 ilustra uma imagem extraída com a referida câmara, em que a posição da mão é guiada por cinco pinos cilíndricos. Os pinos cilíndricos permitem ainda a detecção de presença de uma mão, iniciando a captura dos respectivos dados biométricos.

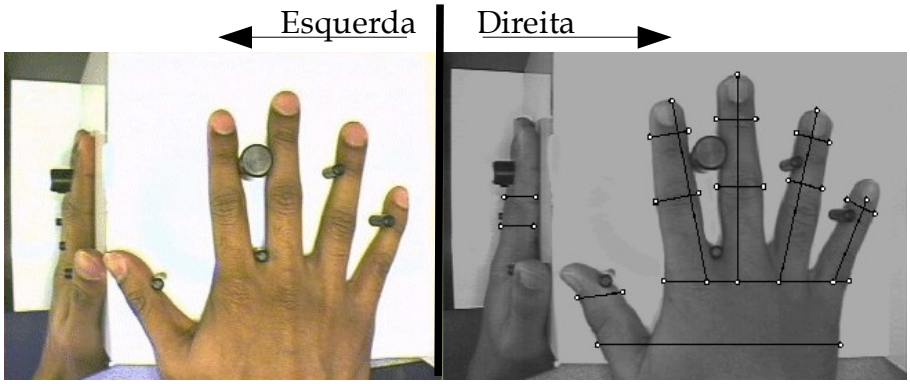

Figura 3.9: Esquerda: Imagem retirada com uma câmara CCD incluindo imagens de espelho. Direita:Exemplos de medições de distâncias [20]

A imagem da direita da Figura 3.9 ilustra a localização das diferentes medições possíveis. O processo de registo da geometria da mão requer tipicamente a captura de três imagens sequenciais da mão, a partir das quais é criado o *template*. O processo de *matching* consiste na comparação do *template* do utilizador que pretende efectuar o reconhecimento, a qual está guardada em memória, com o *template* extraído das três imagens. Da referida comparação resulta uma pontuação que define a probabilidade da verificação ser verdadeira ou falsa.

3.3 . Impressão digital

O processo de identificação por análise da impressão digital é um dos mais conhecidos métodos de reconhecimento biométrico. Segundo um estudo da *International Biometric Group* de 2007, as aplicações baseadas em impressões digitais possuem 58,9% do mercado em relação a outras tecnologias biométricas, das quais 33,6% são referentes a AFIS (*Automated Fingerprint Identification System*) [6]. A popularização desta tecnologia ao longo dos anos relaciona-se com o fácil processo de extracção e as inúmeras fontes (dez dedos) de informação.

Historicamente, e em finais do século XIX, *Sir Francis Galton* verificou que os pontos característicos de uma impressão digital poderiam ser extraídos. A partir dos pontos de *Galton* toda

a tecnologia de identificação baseada em impressões digitais evoluiu. Com a evolução das tecnologias de computação, o reconhecimento de impressões digitais passou a ser um processo automático. Na segunda metade do século *XX* foram desenvolvidos inúmeros algoritmos e técnicas de identificação por impressão digital [10].

Fisiologicamente, uma impressão digital é a configuração de relevos (*ridges*) separados por vales (*valleys*). Estes são suportados por uma estrutura de vasos sanguíneos localizados imediatamente abaixo da pele. A formação da impressão digital acontece durante o período fetal do ser humano, não se altera com a idade e reaparece na mesma forma em caso de deformação da mesma. Com o desenvolvimento do ser humano, a impressão digital permanece com o mesmo tamanho desde criança. Gémeos verdadeiros não possuem impressões digitais parecidas [9]. A morfologia de uma impressão digital está associada com características eléctrica e de temperatura da pele de suporte. O que significa que a luz, calor ou capacidades eléctricas podem ser usadas para extracção de uma impressão digital.

3.3.1 Princípio de Funcionamento

Um sistema biométrico de reconhecimento por impressões digitais é normalmente caracterizado por possuir um sensor de impressões digitais e um módulo de processamento. O sensor de impressões digitais é o *hardware* responsável pela extracção de uma impressão digital. A unidade de processamento interpreta a imagem extraída pelo sensor e transforma-a num *template*. É nesta unidade que se processam os mecanismos de *verificação* ou *identificação.*

Diversas tecnologias de extracção de impressões digitais foram desenvolvidas ao longo dos últimos anos. De entre as tecnologias implementadas salientam-se a óptica, capacitiva, ultrasons e temperatura.

Os sensores ópticos são os mais usados comercialmente. Estes extraem a imagem da impressão digital de forma semelhante ao processo usado numa máquina fotográfica digital. O dedo é colocado em cima de um vidro devidamente iluminado. Um conjunto de lentes adaptativas colocadas a determinada distância do dedo captura a imagem da impressão digital. A captura da impressão digital é determinada pela extracção em partes com determinada resolução e convertida numa imagem à escala de cinzentos. Um dos problemas deste sensor é que, como se coloca o dedo no vidro do sensor óptico, a impressão digital permanece neste e pode ser reutilizada para fins fraudulentos [8].

Nos sensores capacitivos o dedo é colocado sobre um conjunto de pixéis sensíveis a cargas eléctricas. A extracção da impressão digital é baseada nas medições de capacidade para cada pixel. Existem diferenças entre o dieléctrico dos relevos (maioritariamente água) e de um vale (normalmente ar) que causam variação de capacidade entre estes dois tipos de relevo que existe num dedo. Com a identificação dos diversos relevos de um dedo é possível a construção da imagem biométrica do mesmo.

Existem outros sensores que aplicam frequências na gama dos ultrasons ao dedo e utilizam prismas para a detecção das alterações nos feixes emitidos em relações aos feixes reflectidos no dedo. Estes sensores são designados por sensores de ultrasons.

Os sensores de leitura biométrica que recorrem à temperatura para capturar imagens biométricas possuem a vantagem de serem de extrema eficiência na distinção entre dedos vivos e artificiais. Este tipo de sensores usa materiais piro-eléctricos que convertem a diferença de temperatura numa tensão eléctrica específica. O sensor detecta a diferença de temperatura entre as extremidades do dedo que está em contacto com o sensor e os que estão em vales, criando assim uma imagem do dedo. Esta tecnologia possui a desvantagem de a imagem durar poucos instantes, pois no instante de contacto com o sensor dá-se um equilíbrio térmico entre o dedo e o sensor. Como consequência do referido equilíbrio, a imagem térmica perde-se. Em sistemas de alta segurança os sensores térmicos são utilizados em paralelo com outro tipo de sensores, em que o sensor térmico apenas

detecta se o dedo que se está a identificar está vivo. O sensor *FingerChip* da *Atmel* [8] é um exemplo de um sensor deste tipo.

O sensor *FingerLoc,* desenvolvido pela *AuthenTec Inc,* utiliza sensores de silício monolítico de modo a determinar a impressão digital da pele viva do dedo. A pele externa do dedo, também designada por pele morta, pode encontrar-se danificada ou suja tornando difícil a extracção da impressão digital. Os sensores *FingerLoc* detectam a impressão digital onde esta é formada, ou seja na pele viva no interior do dedo. Este sensor aplica uma tensão alternada de baixo valor ao dedo, que é depois convertida num campo eléctrico que varia em amplitude ao longo do dedo, devido à capacidade de condução de um líquido salino existente na pele viva. Este líquido modela o campo eléctrico com a impressão digital do dedo [11].

3.3.2 Tecnologia

De entre os diversos métodos de criação de um *template* a partir de uma impressão digital, os mais populares são baseados em *image-based representation* e *minutiae* [9].

A *image-based representation* é constituída por linhas de *pixels* com informação acerca da impressão digital. A qualidade deste procedimento pode ser afectada pelas variações de contraste, variação de qualidade da imagem, cicatrizes e distorções da própria imagem. Por outro lado, o método de *image-based representation* preserva o máximo de informação de uma impressão digital e pode ser robusto desde que não existam estruturas de relevos danificadas.

Num algoritmo baseado em *minutiae* e em larga escala (visível ao olho humano) uma impressão digital é caracterizada por arcos (*arch),* laços (*loops)* e círculos fechados (*whorls*). A Figura 3.10 define os tipos de características referidos. Estas características não são suficientes para um *matching* preciso mas quando associadas a outras de mais fina escala possuem elevada fiabilidade. As características de mais fina escala utilizadas pelo método *minutiae* são as bifurcações e terminações de relevo. Cada *minutiae* ou *ponto de Galton* é caracterizada pelas suas coordenadas, tipo (bifurcação ou terminação) e orientação. Tipicamente são guardados cerca de 30 a 40 destas características num *template* baseado no método de representação *minutiae*.

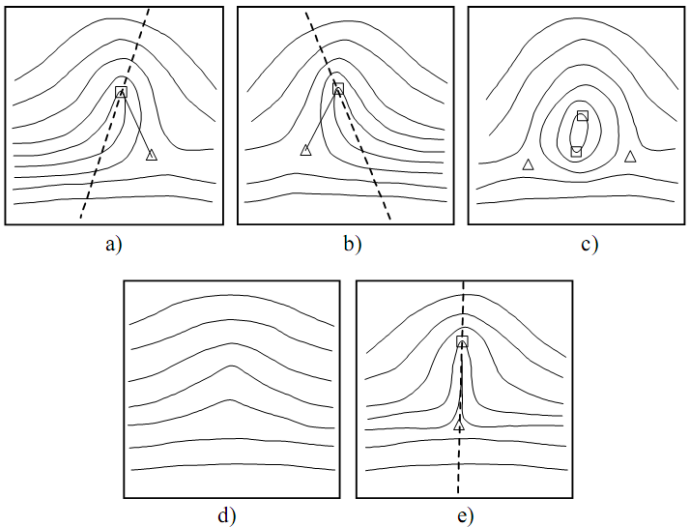

Figura 3.10: Características de uma impressão digital. a,b) loop; c) whorl; d) arch e)tented arch [9].

Num nível de escala ainda mais baixo, existem os poros da pele cujas posições e forma são altamente diferentes entre cada ser humano. As características dos poros da pele são difíceis de extrair, apenas sensores de elevada resolução o conseguem fazer, tipicamente com 1000 dpi [9].

A Figura 3.11 ilustra os detalhes de *minutiae* e poros da pele de uma impressão digital.

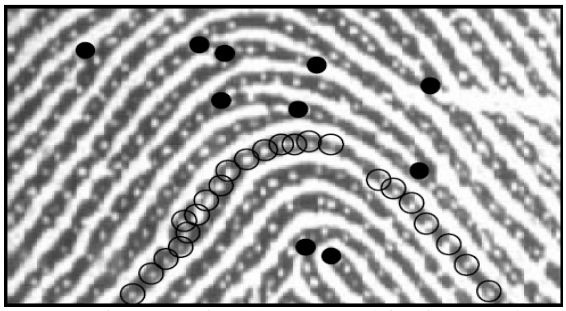

Figura 3.11: Ilustração de uma minutiae (círculos pretos) e poros (círculos transparentes) [9].

O *matching* de diferentes impressões digitais é um processo extremamente complexo, principalmente devido à variação entre diferentes impressões digitais extraídas do mesmo dedo em instantes diferentes. As principais razões para as diferenças verificadas entre impressões digitais do mesmo dedo são devidas ao deslocamento, rotação, sobreposição parcial, distorções não lineares, variações de pressão, alterações das condições da pele e ruído. Os diversos métodos de *matching* podem ser divididos em três categorias [9]:

- *Correlation-based matching* – A correlação entre duas imagens de impressões digitais entre os pixels correspondentes são analisadas automaticamente para diferentes variações (por exemplo, rotações e deslocamentos).
- *Minutiae-based matching* – O processo de *matching* baseado em *minutiae* é composto por duas etapas, alinhamento e *matching*. Como entre ambas as *minutiae* que se pretendem comparar não se sabe a direcção e posição de extracção, deve-se proceder a um alinhamento prévio. Caso o alinhamento seja efectuado com sucesso é então dado inicio à etapa de *matching*. Nesta etapa, duas *minutiae* são comparadas baseando-se na sua posição direcção e tipo. É então emitido um resultado do número de *minutiae* coincidentes.
- *Ridge feature-based matching* – A extracção de um *minutiae* é um processo extremamente difícil em imagens de impressões digitais como baixa qualidade, no entanto existem outros parâmetros (por exemplo orientação local, frequência, forma dos relevos e textura) que podem ser retirados de forma mais fiável que uma *minutiae,* mesmo que o nível de distinção seja menor. Neste tipo de *matching* são comparados os padrões de relevo do dedo com o previamente registado.

3.3.3 Módulos Comerciais

Existem diversas soluções de identificação de utilizadores através da extracção da informação biométrica. Nesta secção são apresentados alguns módulos comerciais de identificação usando o método biométrico de impressão digital.

Os diversos módulos comerciais apresentados são soluções *OEM* (*Original Equipment Manufacturer*). As soluções *OEM* têm como principal finalidade serem integradas em soluções embebidas para desenvolvimento de novas aplicações. Os módulos comerciais analisados são de diferentes fabricantes, como a *Liahren*, *Nitgen* e *Secugen*. São apresentadas as principais características técnicas e de desempenho dos diversos módulos avaliados. Na secção seguinte são analisadas as soluções da *Suprema Inc* por serem os módulos usados no protótipo *wireless Temp I/O*.

Liahren

A *Liahren* [60] é uma empresa Chinesa produtora de soluções baseadas em reconhecimento biométrico por impressão digital.

A *Liahren* possui três soluções comerciais *OEM* de identificação por impressão digital, o *LHID-*

*FM200A (*Figura 3.12*)*, o *LHID-FM200S* e o *LHID-FM200SF*. Os três módulos diferem entre si essencialmente pelo espaço de memória de armazenamento que dispõem. O módulo *LHID-FM200SF* é usado em aplicações de segurança onde o número de utilizadores com permissões de acesso é bastante limitado (5) e os requisitos de mobilidade são exigidos, daí este dispositivo ser normalmente alimentado por pilhas.

Figura 3.12: Módulo OEM Liahren, o LHID-FM200A [60]

A Tabela 3.2 apresenta as características dos três módulos *Liahren*.

Tabela 3.2: Características dos módulos OEM da Liahren.[60].
(0 – Não se verifica. X – Informação não acessível.)

Característica		***LHID-FM200A***	***LHID-FM200S***	***LHID-FM200SF***
Sensor	*Tipo*	*Óptico*	*Óptico*	*Óptico*
	Resolução	*500 dpi*	*500 dpi*	*500 dpi*
Processador		*ARM*	*DSP*	*S3C44B0X*
Autenticação	*Tempo matching*	*< 1 s*	*< 1 s*	*< 1 s*
	Tempo resposta	*< 3 s*	*X*	*X*
	FRR	*0,01 %*	*0,01 %*	*0,01 %*
	FAR	*0,0001%*	*0,0001%*	*0,0001%*
	Método	*1:1, 1:N*	*1:1, 1:N*	*1:1, 1:N*
	Máx. registos (log)	*0*	*0*	*0*
	Máx. utilizadores	*1000 / 3000*	*50*	*5*
I/O	*Com. host*	*RS-232C*	*RS-232C*	*0*
	In	*0*	*0*	*0*
	Out	*0*	*0*	*0*
Tensão alimentação		*5 V*	*5 – 7,5 V*	*6 V (4 Pilhas AA)*
Consumo de energia		*300 mA*	*600 mA*	*X*
Encriptação de dados		*0*	*0*	*0*

Nitgen

A *Nitgen* [21] é uma empresa Coreana especializada em soluções de controlo de assiduidade e sistemas de gestão de acessos baseados em identificação por impressão digital. A *Nitgen* comercializa também módulos *OEM* de identificação por impressão digital para serem embebidas por terceiros. Os módulos *OEM* da *Nitgen* podem ser divididos em três famílias (*FIM11 --*, *FIM20 --* e

FIM30 --) com as características apresentadas na Tabela 3.3.

Tabela 3.3: Características dos módulos OEM da Nitgen [21].
(0 – Não se verifica. X – Informação não acessível)

Característica		**FIM11 --**	**FIM20 --**	**FIM30 --**
Sensor	*Tipo*	*Óptico*	*Óptico*	*Óptico*
	Resolução	*500 dpi*	*500 dpi*	*500 dpi*
Processador		*ARM9, SDRAM:8MB Flash Mem.: 1MB*	*ARM9, SDRAM:8MB Flash Mem.: 2/2+4MB*	*DSP, SDRAM:8MB Flash Mem.: 1MB*
Autenticação	*Tempo matching*	*0*	*0*	*< 1 s*
	Tempo resposta	*< 1 s*	*< 1s*	*< 2 s (extracção + match)*
	FRR	*1/1000*	*1/1000*	*1/1000*
	FAR	*1 / 100 000*	*1 / 100 000*	*1 / 100 000*
	Método	*1:1, Password, Device Password*	*1:1, Password, Device Password*	*1:1, 1:N, Password, Device Password*
	Máx. registos (log)	*2000*	*2000*	*8000*
	Máx. utilizadores	*1000*	*1000/4000*	*1000*
I/O	*Com. host*	*2 x RS-232*	*2 x RS-232*	*RS-232*
	In	*0*	*(4): Novo registo, apagar, Verificar e Reset*	*(3): Novo registo, apagar e verificar*
	Out	*(3): Sucesso, Falha, Cartão accionado*	*(2): Sucesso, Falha.*	*(2): Sucesso, Falha.*
Tensão alimentação		*5 V*	*5 V*	*3,3V ou 5V*
Consumo de energia		*Máx: 350 mA*	*Máx: 300 mA*	*Máx: 250 mA*
Encriptação de dados		*AES*	*AES*	*AES*

A principal diferença entre os diversos módulos *OEM* da *Nitgen* tem que ver com o método de autenticação usado. As famílias *FIM 10--* e *FIM 20--* apenas executam tarefas de verificação (1:1), enquanto os módulos *FIM 30--*, para além da verificação, também executam o método de identificação (1:N). A família *FIM30--* apresenta ainda um conjunto de módulos que podem ser alimentados a *3,3V*.

A Figura 3.13 ilustra os diferentes módulos das três famílias *OEM* da *Nitgen*. O módulo *FIM 3141* possui uma interface entre o sensor de extracção da impressão digital e a unidade de processamento diferente dos demais, embora possua as mesmas características de desempenho e operação dos módulos da família *FIM 30--*.

Figura 3.13: Gama de soluções OEM da Nitgen ***[21]****.*

Cada um dos módulos das famílias apresentadas pode usar como sensor de impressões digitais dois módulos distintos, o *OPP03* e o *OPP04.* Ambos os sensores são ópticos de resolução de 500 dpi, embora apresentem diferentes tamanhos.

Secugen

A empresa norte americana *Secugen* [61] é uma prestigiada empresa de desenvolvimento e comercialização de soluções de identificação por impressão digital. Esta empresa possui uma gama de soluções comerciais de módulos *OEM* de identificação por impressão digital.

A Tabela 3.4 descreve as principais características dos módulos *FDA02DL* e *FDA02*.

Tabela 3.4: Características dos módulos Secugen [61].
(0 – Não se verifica. X – Informação não acessível.)

Característica		**FDA02DL**	**FDA02**
Sensor	*Tipo*	*Óptico*	*Óptico*
	Resolução	*500 dpi*	*500 dpi*
Processador		*Hyperstone E1-32XSR 128 MHz*	*Hyperstone E1-32XS 96 MHz*
Autenticação	*Tempo matching*	*0.8 s (1:1000)*	*0.8 s (1:1000)*
	Tempo resposta	*1,2 s (1:1000)*	*1,2 s (1:1000)*
	FRR	*X*	*X*
	FAR	*X*	*X*
	Método	*1:1, 1:N*	*1:1, 1:N*
	Máx. registos (log)	*0*	*0*
	Máx. utilizadores	*(v1.x) 4,400 for 1:1 Matching* *(v1.x) 200 for 1:N Matching* *(v2.x) 1,000* *(v3.x) 100*	*(v1.x) 4,400 for 1:1 Matching* *(v1.x) 200 for 1:N Matching* *(v2.x) 1,000* *(ANSI378) 1,000*
I/O	*Com. host*	*8 Bit MCU-Friendly Bus Interface / USART*	*USART*
	In	*0*	*0*
	Out	*0*	*0*
Tensão alimentação		*3.6 ~ 5.5 V*	*4.75 ~ 5.25 V*
Consumo de energia		*Máx: 200 mA*	*Máx: 200 mA*
Encriptação de dados		*0*	*0*

3.3.4 Módulos Comerciais Suprema

A *Suprema Inc.* [22] é uma empresa Coreana especializada em soluções biométricas, possuindo uma vasta gama de produtos comerciais baseados na análise da impressão digital.

As soluções *embedded* da *Suprema Inc.* constituem a família *Unifinger*. Os módulos *Unifinger* permitem a identificação *stand-alone* e podem ser integrados em sistema em desenvolvimento. Estas soluções integram duas componentes: o sensor de impressões digitais e o módulo de processamento, o *SFM3000* (Figura 3.14) ou o *SFM3500*. O sensor de impressões digitais é o módulo responsável pela extracção de informação do dedo. Os módulos de processamento transformam os dados provenientes do sensor de impressões digitais num *template.* Os módulos *Unifinger* executam ainda a

identificação do utilizador a partir de uma base de dados interna de *templates*.

As especificações técnicas dos módulos *SFM3500* e *SFM3000* são identificadas na Tabela 3.5.

Tabela 3.5: Características dos módulos Unifinger da Suprema Inc [22].
(X – Informação não acessível.) Comparação genuína de 1/1000 incluindo tempo de extracção*

Característica		***SFM3000***	***SFM3500***
Sensor	*Tipo*	*Óptico, Capacitivos, térmico ou FingerLoc*	*Óptico, Capacitivos, térmico ou FingerLoc*
	Resolução	*Óptico e Térmico: 500 dpi Capacitivo: 508 dpi FingerLoc: 250 dpi*	*Óptico e Térmico: 500 dpi Capacitivo: 508 dpi FingerLoc: 250 dpi*
Processador		*DSP 400 MHz*	*DSP 400 MHz*
Autenticação	*Tempo matching*	*680 ms a 990 ms **	*680 ms a 990 ms **
	Tempo verificação	*5580 ms a 850 ms*	*5580 ms a 850 ms*
	FRR	*1,31%*	*1,31%*
	FAR	*X*	*X*
	EER	*< 0.1%*	*< 0.1%*
	Método	*1:1, 1:N*	*1:1, 1:N*
	Máx. registos (log)	*0*	*12 800*
	Máx. utilizadores	*1900 para 1MB ou 9500 para 4 MB*	*9000 para 4 MB*
I/O	*Com. host*	*UART (3.3V)*	*1 RS-232 ou RS-485 + 1 RS-232 ou TTL*
	In/out	*8 (configuráveis como entrada ou saída)*	*3 Leds, 3 Entradas e 3 Saídas*
Tensão alimentação		*3.3V*	*5V*
Consumo de energia		*150 mA*	*170 mA*
Encriptação de dados		*AES 256 bits*	*AES 256 bits*

As diferenças entre os módulos de processamento *SFM3000* e *SFM3500* são essencialmente ao nível das interfaces para o exterior que possuem e na capacidade de memória que disponibilizam. O módulo de processamento *SFM3000* possui, no entanto, menor consumo de energia.

Figura 3.14: SFM3000 com leitor capacitivo.

Comandos

As tramas da estrutura *UniFinger SFM Packet Protocol* apresentam tamanho fixo, um *start code* e um *End Code*. Nos protocolos de comunicação, o tamanho máximo e o *start code* das tramas diferem [55]. A Tabela 3.6 resume as tramas de comunicações usadas pelos leitores *Suprema Inc*.

Tabela 3.6: Tramas do protocolo de comunicações Unifinger usadas na aplicação wireless Temp I/O.

Nome	***Descrição***
Enroll by Scan	Regista um utilizador na base de dados local do módulo *UniFinger* a partir da extracção da impressão digital do dedo do utilizador. Pode ser atribuído o identificador do utilizador que se vai registar no campo *Param.* Existem diversos modos de registo com uma ou mais *templates*.
Read Template	Lê os *templates* de um utilizador previamente registado. É enviado o identificador do utilizador do qual se pretende ler os *templates* no campo *Param.*
Identify by Scan	Esta trama pode ser usada para fazer *polling* ao módulo *Unifinger*. Sempre que um utilizador coloca o seu dedo no sensor é enviada uma trama deste tipo com o *User ID* do utilizador, em caso de sucesso de *matching* com registo prévio ou erro de identificação.
Enroll by Template	Regista um utilizador através do envio do seu *template* pelo *host* via interface externa. O *template* tem de ser extraído do dedo do utilizador previamente. Esta trama é usada para distribuição do *template* pela rede de sensores *Unifinger*.
Delete Template	Apaga um *template* de um utilizador cujo identificador é introduzido no campo *Param.* Através desta trama é possível apagar toda a informação registado no módulo *Unifinger* acerca de determinado utilizador.
System Parameter Read	Lê o valor configurado de um parâmetro de configuração do módulo *Unifinger*.
System Parameter Write	Altera o valor de um parâmetro do módulo *Unifinger*.
System Parameter Save	Regista em memória não volátil as configurações de registos previamente definidas através da trama de *System Parameter Write*.
Get Module ID	Quando enviado para endereço de *broadcast* permite a identificação dos dispositivos *UniFinger* a operar na rede.

A *Application Programmable Interface (API)* definida pelo fabricante de leitores de impressões digitais *Suprema* pode usar três distintos tipos de comunicação. A primeira forma é usada para comunicação ponto a ponto entre o leitor e um *host*. Os dois restantes modos são usados para trocas de dados em cenários de rede. Em cenários de rede existe um campo de 2 bytes para atribuição do identificador do módulo na rede. Os dois modos de rede diferem no endereço de destino, o primeiro pode ser endereçado a qualquer módulo *Unifinger* remoto (*unicast*) e usa mecanismos de *acknowledge*. O último modo de comunicações em rede permite transmissões para todos os módulos da rede (*broadcast*), não sendo possível a transmissão de tramas de reconhecimento de integridade de mensagem recebida (*acknowledge*).

A Figura 3.15 ilustra a estrutura base das tramas utilizada para modo de comunicação em rede. A estrutura de comunicação para *broadcast* possui a mesma estrutura, mas em que o campo *Terminal ID* é colocado a zero.

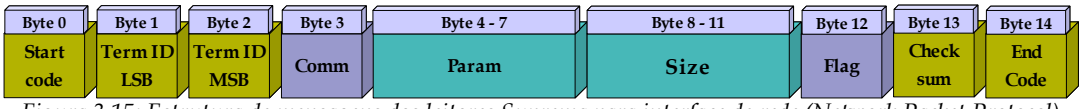

Figura 3.15: Estrutura de mensagens dos leitores Suprema para interface de rede (Network Packet Protocol)

Desempenho

Os processos de identificação de utilizadores através das tecnologias biométricas são por vezes muito demorados. A *Suprema Inc.* desenvolveu um algoritmo que acelera o processo de identificação em cerca de 10 vezes, permitindo menores tempos de identificação em detrimento de ligeira degradação na precisão da identificação. O referido modo de identificação é denominado de *Fast Mode* e possui cinco variantes.

Na Tabela 3.7 são apresentados os desempenhos dos módulos *Unifinger* em relação aos tempos de extracção e identificação para os diversos modos de operação e variando o tipo de sensor. As referidas medições foram executadas pelos investigadores da *Suprema Inc.*

Tabela 3.7: Tempos (em ms) de identificação para os módulos Unifinger da Suprema Inc. (Tempo de matching para base de dados com 1000 entradas (1:1000))*

Sensor	*Tempo Extracção**	*Normal**	*Fast 1**	*Fast 2**	*Fast 3**	*Fast 4**	*Fast 5**
Óptico	792 ms	1662 ms	405 ms	329 ms	267 ms	221 ms	176 ms
Capacitivo TC1	675 ms	1097 ms	343 ms	288 ms	233 ms	190 ms	154 ms
Capacitivo TC2	483 ms	652 ms	402 ms	306 ms	237 ms	195 ms	159 ms
FingerLoc	506 ms	566 ms	393 ms	312 ms	253 ms	210 ms	168 ms
Térmico	815 ms	1101 ms	491 ms	343 ms	279 ms	226 ms	175 ms

Da análise da Tabela 3.7 é possível concluir que o processo de *matching* não depende apenas do sensor de impressões digitais e da sua precisão, mas sim do algoritmo de identificação. Em cada coluna os valores não alteram significativamente, com excepção do modo *Normal*. O processo de identificação é composto pelos processos de extracção e de *matching*. O tempo mínimo de uma identificação (tempo de extracção + tempo de *matching)* é de 642 ms para o módulo capacitivo *Upek* do tipo 2 no modo *fast 5* e máximo para o módulo *Óptico* no modo normal (1,66 s).

A análise da degradação foi também efectuada para os modos *fast*. Apenas a componente *FRR (False reject rate)* foi afectada no desempenho. A *FRR* define a probabilidade de um utilizador válido ver rejeitado a seu acesso ao sistema. Este parâmetro não tem muita importância em aplicações em que o utilizador interage com o sistema de forma voluntária, pois caso não seja atribuído acesso, este pode voltar a tentar a validação.

A Tabela 3.8 apresentada os valores de *FRR* para os diferentes modos de identificação.

Tabela 3.8: Valores de FRR para os modos normal e rápido dos módulos Unifinger.

	Normal Mode	*Fast 1*	*Fast 2*	*Fast 3*	*Fast 4*	*Fast 5*
FRR (%)	1,31	1,44	1,45	1,57	1,77	1,95

O parâmetro *FAR (false acceptance rate)* não é afectado significativamente nos modos de *matching fast*. Este parâmetro define a percentagem de utilizadores que conseguiram acesso sem a isso estarem autorizado.

Capítulo 4

Tecnologias de comunicações sem fios para redes pessoais

4.1 . Introdução

Uma rede de comunicações sem fios para áreas pessoais (*WPAN: Wireless Personal Area Network*) é definida como o conjunto de dispositivos envolventes ao utilizador, podendo estes serem móveis e que comunicam entre si usando tecnologias de comunicação sem fios. Estes dispositivos podem estar sob o controle de um indivíduo ou sob o controle de dispositivos de outros utilizadores. A partir deste conceito, uma *WPAN* pode ser definida como uma rede composta por dispositivos pessoais usando tecnologias para comunicação sem fios de curto alcance.

O grupo de trabalho *IEEE (Institute of Electrical and Electronics Engineers*) *802.15* concentra-se sobre as redes do tipo *WPAN,* permitindo o desenvolvimento de inúmeras tecnologias deste tipo de comunicações *wireless,* tais como a *Bluetooth (IEEE 802.15.1*), *Ultra Wide Band (UWB) (IEEE 802.15.3*) e *ZigBee* (*IEEE 802.15.4).*

Nas próximas secções são apresentados os protocolos de comunicação sem fios mais comuns inseridos no grupo *WPAN*, nomeadamente o *Bluetooth*, *UWB* e *ZigBee*. O protocolo *wifi (IEEE 802.11*) é também abordado neste capítulo apesar de pertencer ao grupo *WLAN (Wireless Local Access Network*) de maior raio de acção em relação ao *WPAN*. O protocolo *wifi* foi avaliado por definir uma rede de comunicações sem fios implementada em diversos locais onde a aplicação em desenvolvimento pode operar.

4.2 . Bluetooth

O *Bluetooth* [23] é um protocolo de comunicações sem fios para aplicações de transferência de dados multimédia entre dispositivos a curtas distâncias. Esta tecnologia possui inúmeras aplicações para trocas de dados entre periféricos e equipamentos móveis (telemóveis, *smartphones* e *PDAs*). O protocolo *Bluetooth* foi desenvolvido para permitir a utilização das comunicações sem fios de forma

fácil para o utilizador final, sem a necessidade de configurações prévias pelo utilizador.

O protocolo opera na banda não licenciada de 2,4 GHz e as suas principais características são a robustez, complexidade reduzida, baixo consumo de energia e custo. A versão actual do protocolo *Bluetooth* é a *2.1+Enhanced Data Rate* (*EDR*) editada em Julho de 2007. O grupo de trabalho *IEEE 802.15* adoptou em 2002 a versão 1.1 do protocolo *Bluetooth* do *Special Interest Group* (*SIG)* e criou o standard *IEEE 802.15.1* [24].

A versão 2 do protocolo *Bluetooth* introduz novas funcionalidades em relação à versão anterior, com especial relevância para o aumento da taxa de transmissão de dados para 3 Mbps. A versão 1.1 permitia a transmissão de dados até 720 kbps.

Existem diversas classes de rádio que permitem a selecção do alcance e consequentemente menor ou maior consumo de energia. O alcance máximo do protocolo é de 100 metros com consumo de 100 mW. No mínimo, um dispositivo *Bluetooth* pode consumir 1 mW para um raio de alcance de 10 metros.

Os circuitos integrados *Bluetooth* são de pequenas dimensões, o que lhes confere uma fácil integração em sistema móveis com controladores de baixa complexidade, tipicamente *RISC* (*Reduced Instruction Set Computer*), garantindo uma conectividade sem fios de elevada robustez. A robustez de performance do protocolo *Bluetooth* deriva do mecanismo de *FHSS* (*Frequency-Hop Spread Spectrum*) minimizando a interferência entre sinais rádio na mesma gama de frequências.

Os dados podem ser transmitidos usando comunicação assíncrona ou síncrona. A tecnologia *Bluetooth* suporta um canal assíncrono para dados e pelo menos três canais síncronos para transmissão de voz.

4.2.1 Topologia de rede

O elemento atómico de uma rede *Bluetooth* é denominado por *piconet*. Cada rede *piconet* é composta por um *master* e pelo menos um *slave*, até ao máximo de sete *slaves* activos. Tipicamente, nas aplicações *Bluetooth*, podem coexistir várias *piconets* independentes e não sincronizadas nos saltos de frequência, evitando interferência entre *piconets*. Neste caso é formado um sistema *ad-hoc* denominado por *scatternet* composto de múltiplas redes *piconet*, cada uma contendo um número limitado de dispositivos. A Figura 4.1 apresenta a topologia de rede *Bluetooth scatternet*.

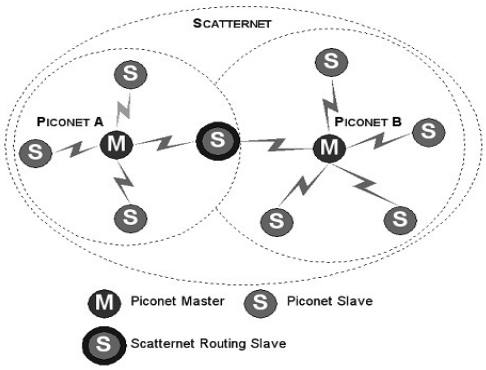

Figura 4.1: Topologia de rede Bluetooth.[26]

Um dispositivo *Bluetooth* pertencente a uma *piconet* pode participar em outras *piconets* usando o mecanismo de *Time Division Multiplex* (*TDM*). Um *master* de uma *piconet* pode ser um *slave* da *piconet* vizinha.

4.2.2 Arquitectura

A arquitectura da tecnologia *Bluetooth* é definida segundo duas componentes [25], o núcleo e os

perfis. As especificações do núcleo definem o funcionamento da tecnologia (meio físico, pilha protocolar e topologia de rede). As especificações dos perfis focam o desenvolvimento de dispositivos interoperaráveis que utilizam as tecnologias do núcleo.

Pilha protocolar

As especificações *Bluetooth* não definem apenas o protocolo de comunicações sem fios, mas também diversos perfis de aplicação. A pilha protocolar *Bluetooth* é responsável pela definição dos protocolos de comunicação e por permitir que os dispositivos encontrem os seus vizinhos e anunciem os seus serviços.

A pilha protocolar *Bluetooth* pode ser dividida em três blocos distintos: *application, middleware* e *transport.* O grupo de protocolos *application* é constituído pelas aplicações (baseadas em *Bluetooth* ou não) que utilizam a tecnologia *Bluetooth*. O grupo de tecnologias *middleware* consiste em protocolos específicos *Bluetooth*, como a emulação da porta série (RCFCOMM) e outros protocolos adaptados, como o *Object Exchange Protocol* (*OBEX).* Por fim, o grupo de protocolos de *transport* é constituído por protocolos desenvolvidos exclusivamente para a tecnologia *Bluetooth*, como o *Logic Link Control and Application Protocol (L2CAP)* e o *Host Controller Interface (HCI).*

A Figura 4.2 descreve a pilha protocolar *Bluetooth.*

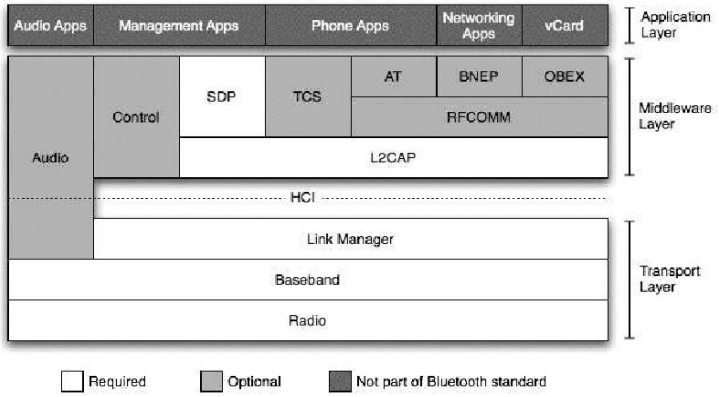

Figura 4.2: Pilha protocolar Bluetooth [27].

Perfis

Os perfis do protocolo *Bluetooth* definem a forma como a tecnologia é utilizada, isto é, como componentes distintos da especificação do protocolo podem ser combinados de forma a cumprirem os requisitos de um dispositivo *Bluetooth*. Um perfil pode ser visto como uma fatia vertical da pilha protocolar *Bluetooth*. Desta forma, são seleccionadas determinadas funcionalidades de cada camada, de acordo com as especificações da aplicação *Bluetooth* a ser desenvolvida. O conceito de perfil permite reduzir o risco de problemas de interoperabilidade entre produtos de diferentes fabricantes. Estes perfis não acrescentam novas especificações ao protocolo *Bluetooth.* É por este motivo que, quando necessário, novos perfis podem ser adicionados.

Na Figura 4.3 encontram-se diversos perfis de acordo com a listagem do grupo *SIG*. Como ilustrado, os perfis *Bluetooth* estão organizados em grupos. Cada grupo herda as funcionalidades do grupo abaixo. Este esquema permite a renovação de funcionalidades entre perfis, reduzindo deste modo os custos de desenvolvimento.

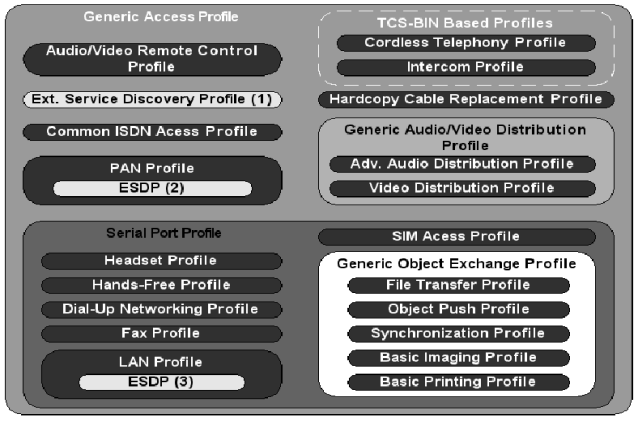

Figura 4.3: Perfis Bluetooth [26].

4.3 . Wifi

O protocolo *IEEE 802.11* [28] é actualmente o standard mais vulgarizado nas comunicações sem fios para redes locais. O objectivo inicial deste protocolo era especificar as camadas de Controlo de Acesso ao Meio (*MAC: Medium Access Control*) e Camada Física (*PHY: Physical)* para a conectividade sem fios de estações fixas, portáteis ou móveis numa área local.

Os dispositivos *Wifi* são essencialmente utilizados de forma a promover serviços de *broadband*, garantindo acesso a redes privadas ou públicas através de interface sem fios.

Após o seu lançamento em 1997, o protocolo *IEEE 802.11* foi rectificado em 1999, de forma a suportar taxas de transmissão acima da barreira dos 10 Mbps. Em 2003 foram introduzidas alterações de forma a alargar as taxas de transmissão para 54 Mbps na banda dos 2.4 GHz. Esta evolução deveu-se à crescente necessidade de largura de banda devido ao volume de informação crescente das aplicações.

4.3.1 Arquitectura

Como acima referido, a norma *IEEE 802.11* define a arquitectura das camadas *MAC* e *PHY.* A Figura 4.4 representa a correspondência entre o protocolo *802.11* e o modelo de referência OSI.

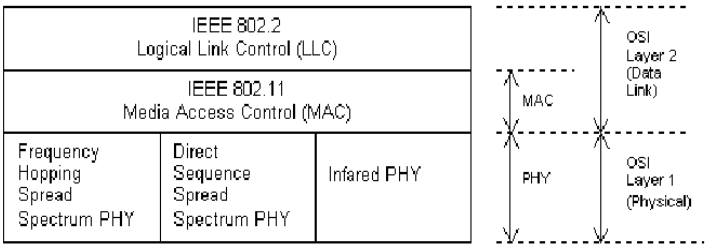

Figura 4.4: Arquitectura da pilha protocolar da tecnologia IEEE 802.11.

As redes *802.11* são constituídas por quatro componentes físicos: Sistema de Distribuição (*DS: Distribution System*), Pontos de Acesso (*AP: Access Point*), meio de comunicação sem fios e estações. Estes componentes estão relacionados como ilustrado na Figura 4.5.

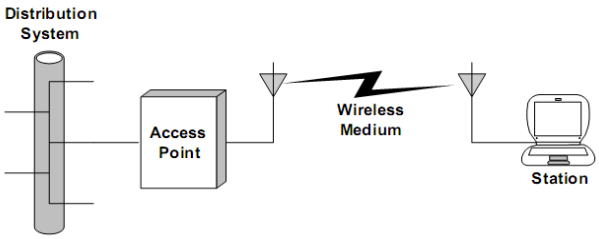

Figura 4.5: Dispositivos do protocolo IEEE 802.11 [26].

O *DS* é a interface que estabelece a ligação entre estações de uma rede WLAN para o exterior, reencaminhando os pacotes para os respectivos destinos. Os *APs* convertem os pacotes no formato *IEEE 802.11* para diferentes formatos, permitindo deste modo que estes sejam transmitidos em diferentes canais de comunicação (por exemplo a *Ethernet).*

O protocolo *IEEE 802.11* utiliza a atmosfera como canal de comunicações. Este meio é baseado em dois tipos de acesso *PHYs*: *Rádio Frequência* (*RF)* e infravermelhos. O *PHY RF* tornou-se no mais popular devido ao maior alcance e melhor rendimento, visto não ser necessário que os dispositivos estejam em linha de vista. A estação é um dispositivo que contém as funcionalidades do protocolo 802.11, nomeadamente *MAC, PHY* e uma ligação ao meio sem fios.

Tipicamente estas funcionalidades estão implementadas no *hardware* e *software* de uma placa de interface à rede (*NIC: Network Interface Card*). Estes dispositivos podem ser computadores portáteis, *PCs* ou *PDAs*.

Controlo de Acesso ao Meio

A camada *MAC (Medium Access Control)* do protocolo *IEEE 802.11* implementa diversos mecanismos que permitem controlar o acesso ao meio físico. A camada MAC usa os mecanismos da camada PHY para aceder ao canal físico, permitindo a troca de dados entre as camadas superiores de aplicação e o dispositivo com o qual a aplicação pretende trocar dados.

O envio de dados pela camada MAC baseia-se no método assíncrono, *best-effort* e comunicação sem ligação. A camada MAC implementa um mecanismo controlado de acesso ao meio partilhado, denominado *Carrier-Sense Multiple Access with Collision Avoidance* (CSMA/CA). Através deste mecanismo, um dispositivo *IEEE 802.11* apenas transmite um conjunto de dados após a verificação, por um período de tempo, que o canal se encontra livre para transmissão.

Outra funcionalidade desta camada é a de proteger os dados que são transmitidos através de serviços de segurança e privacidade. A segurança é disponibilizada pelos serviços de autenticação e um serviço de encriptação de dados, o *Wireless Equivalent Privacy* (*WEP*).

Camada física

A camada física do protocolo *IEEE 802.11* estabelece a interface entre a camada MAC e o meio físico. Esta camada disponibiliza três funcionalidades: interface para a troca de informação com a camada superior do MAC, transmissão de dados através de uma portadora e uma indicação para que a camada MAC verifique a actividade do meio. O protocolo *IEEE 802.11* define as seguintes vertentes da camada física PHY:

- ✔ Taxas de transmissão de 1 e 2 Mbps utilizando modulação *Frequency Hopping Spread Spectrum* (FHSS) e *Direct Sequence Spread Spectrum* (DSSS).
- ✔ Uma extensão ao protocolo inicial define taxas de transmissão de 5.5 e 11Mbps (802.11b), utilizando modulação *High Rate DSSS* (HR/DSSS)
- ✔ Outra extensão ao protocolo 802.11 (802.11a) define múltiplas técnicas de multiplexagem na banda dos 5 GHz de forma a atingir taxas de transmissão de 54 Mbps, utilizando modulação *Orthogonal Frequency-Division Multiplexing* (*OFDM).*

- ✔ A versão 802.11g (2.4 GHz) permite um ritmo de transmissão máximo de 54 Mbps, utilizando a mesma modulação utilizada na revisão 802.11b (*HR/DSSS).*

4.3.2 Topologia de rede

O Conjunto Básico de Serviços (*BSS: Basic Service Sets*) constitui o bloco básico de construção de uma rede sem fios, em que um grupo de estações comunica entre si. Tal como ilustrado na Figura 4.6, o BSS pode assumir duas formas: independente e infraestrutura.

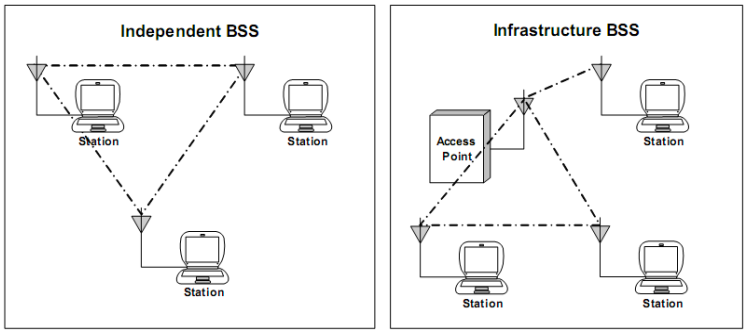

Figura 4.6: Topologias de rede suportados pelo protocolo IEEE 802.11.[26]

A topologia básica de uma rede *wifi* é constituída por um conjunto de estações que têm conhecimento dos componentes da rede, e que estão ligadas através do meio de comunicação sem fios de uma forma *peer-to-peer*. Este tipo de topologia de rede é conhecido por Conjunto Básico de Serviços Independente (*IBSS*: *Independent Basic Service Sets*) ou rede *Ad-hoc*. As redes *IBSSs* são estabelecidas de modo a permitir a conectividade em áreas de pequena dimensão, para um pequeno número de estações e durante curtos períodos de tempo. Redes com infraestruturas utilizam pontos de acesso (*AP: Access Point*) como intermediário nas comunicações. Quando uma estação pretende comunicar, esta tem de enviar a informação para o AP, mesmo que, a estação destino esteja dentro do raio de alcance da estação emissora. Posteriormente, a estação reencaminha a informação para a estação destino. Embora a comunicação seja efectuada em dois passos, existem duas vantagens neste processo:

- ✔ O alcance máximo de uma rede infra estrutura BSS depende da cobertura do AP. Deste modo é possível que duas estações que não estejam dentro do raio de alcance comuniquem entre si usando o AP como intermediário.
- ✔ As estações são normalmente equipamentos móveis alimentados por baterias. Caso os *APs* emitam tramas de reconhecimento às estações durante o modo de poupança energética, os *APs* armazenam toda a informação e enviam a mesma quando solicitado pelas estações. As estações não necessitam de permanecer à escuta de informação proveniente dos *APs.*

4.4 . UWB – Ultra Wide Band

A tecnologia *Ultra-Wide Band* (*UWB*) é conhecida e utilizada há vários anos em aplicações militares. Contudo, foi apenas nos anos 90, na Universidade da Califórnia do Sul que se iniciou o desenvolvimento do UWB como uma tecnologia de comunicações sem fios comercial [29]. Os primeiros sistemas UWB baseavam-se na tecnologia rádio, onde pequenos impulsos eram emitidos pelo ar [30]. Com base nesta técnica, em 1998, a empresa *Time Domain Inc* produziu o primeiro transmissor UWB baseado no circuito integrado *PulsOn 100*. Mais tarde, uma empresa recém formada, *XtremeSpectrum,* desenvolveu um circuito integrado denominado *Trinity* que suportava taxas de transmissão de 100 Mbps, usando o protocolo *IEEE 802.15.3.*

O crescente interesse nesta tecnologia em comunicações sem fios para aplicações não militares, deveu-se à alocação do *UWB* no espectro de frequências por parte da *Federal Communications*

Comission (*FCC*). Existem duas abordagens para a utilização de *UWB:* o *MB-OFDM* (*Multi-Band Orthogonal Frequency Division Multiplexing*) e o *DS-UWB* (*Direct Sequence UWB*). A Aliança *Wimedia* desenvolveu a proposta baseada em *MB-OFDM* e o *UWB Forum* a DS-UWB.

Em Março de 2005, o grupo *IEEE 802.15.4a* propôs a utilização de impulsos rádio na gama de operação UWB para aplicações de baixa taxa de transferência.

A FCC define a tecnologia UWB com sendo sinal RF que ocupe pelo menos 500 MHz dos 7.5 GHz do espectro, entre as frequências 3.1 GHz e 10.6 GHz (Figura 4.7). Cada canal de radio pode ocupar mais de 500MHz da largura de banda, dependendo da frequência central.

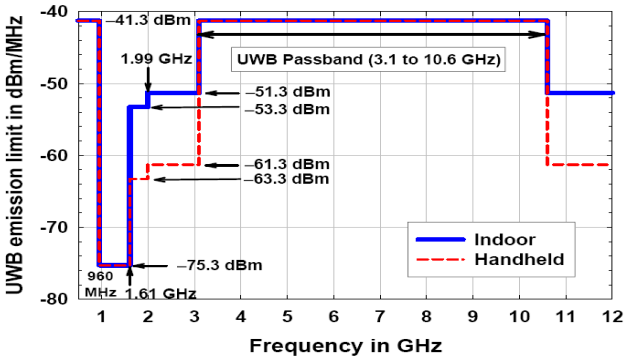

Figura 4.7: Largura de banda e potência de transmissão autorizadas pela FCC para a tecnologia UWB.

Para permitir uma largura de banda tão elevada, a *FCC* estabelece regras muito estritas na potência máxima emitida durante a transmissão de sinal. Deste modo, os dispositivos compatíveis com esta tecnologia podem utilizar uma largura de banda muito vasta sem o risco de ocorrência de interferência com outros dispositivos de comunicação rádio. Devido às limitações da potência do sinal emitido, os dispositivos compatíveis com a tecnologia *UWB* apresentam baixo consumo energético.

A aliança *WiMedia* aproveita as vantagens da tecnologia UWB (elevada taxa de transmissão e consumo energético reduzido) para definir uma plataforma de rádio comum que serve de suporte a outros protocolos. A plataforma de rádio comum *WiMedia UWB* define as especificações das camadas *MAC* e *PHY* com base na modulação *OFDM*. A plataforma *UWB* suporta novos protocolos de comunicação emergentes, tais como o *Wireless USB*, *Wireless IP* (*WiNET*), *Bluetooth* e *IEEE1394*.

A Figura 4.8 ilustra a arquitectura protocolar da plataforma definida pela aliança *WiMedia*.

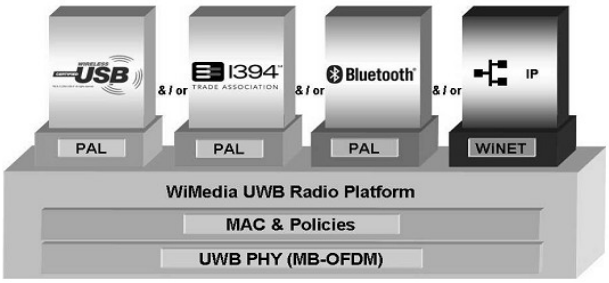

Figura 4.8: Plataforma UWB da Aliança WiMedia.[31]

As especificações MAC e PHY foram intencionalmente definidas de modo a adaptarem-se aos diversos requisitos definidos pelos organismos reguladores mundiais, nomeadamente, atingir reduzido nível de complexidade nos nós e suportar múltiplos modos de gestão de recursos energéticos e capacidade espacial elevada.

4.5 . ZigBee

A tecnologia *ZigBee* [34] permite a construção de redes de sensores sem fios (*WSN: Wireless Sensor Networks*) em ambientes domésticos e industriais. Os requisitos de consumo de energia e complexidade de implementação são a base do desenvolvimento da tecnologia *ZigBee*.

A empresa *Philips* foi a primeira promotora da tecnologia *ZigBee,* então designada por *HomeRF* Lite, no ano de 1998. A tecnologia evoluiu e a agregação de novos colaborados implicou a sucessiva alteração de nomenclatura desde *PURLnet*, *RF Lite*, *Firefly*, *RF Easy Link* até que, em 2001, adoptou o nome de *ZigBee*. O nome *ZigBee* é originário do princípio desta tecnologia, e deriva do movimento em *zig-zag* efectuado pelas abelhas de forma a informarem a sua colónia da localização, distância e direcção de novas fontes de comida [32].

Em 2000, o núcleo *ZigBee* associou-se ao grupo *IEEE 802.15* para combinarem esforços para a criação de um novo standard para redes de sensores com comunicações sem fios. Foi então criado o grupo 4 de forma a desenvolver um standard *Low Rate Wireless Personal Area Network* (*LR-WPAN*), o *IEEE 802.15.4* [33].

Posteriormente em 2002, foi formada a aliança *ZigBee* constituída pelas empresas *Philips*, *Motorola*, *Honeywell*, *Invensys* e *Mitsubishi Electric* com a intenção de promover a tecnologia *ZigBee*. O principal objecto desta aliança é a especificação das camadas superiores (*Network* e *Aplicação*) da pilha protocolar, desenvolvendo perfis de aplicação e execução de testes de conformidade e interoperacionalidade entre dispositivos de diferentes fabricantes.

As principais características de uma rede *ZigBee* são o baixo consumo de energia, baixa complexidade da pilha protocolar, baixa latência e a possibilidade de estabelecimento de múltiplas topologias de rede, tais como a ponto-a-ponto, ponto-multiponto, *cluster tree* e *mesh*.

Nas próximas secções é apresentada a pilha protocolar *ZigBee*.

4.5.1 Pilha Protocolar

A pilha protocolar *ZigBee* baseia-se nas camadas do modelo *OSI* (*Open Systems Interconnections*). O standard desenvolvido pelo grupo de trabalho *IEEE 802.15.4* define as camadas física e de controlo de acesso ao meio da tecnologia *ZigBee*. As restantes camadas (camada de rede e aplicação) são definidas pela Aliança *ZigBee*.

Cada camada da pilha protocolar produz um conjunto específico de serviços para a camada que se encontra imediatamente acima. Cada entidade de serviço possui uma interface para a camada acima através do *Service Access Point* (*SAP*).

A Figura 4.9 apresenta a arquitectura da pilha protocolar *ZigBee*.

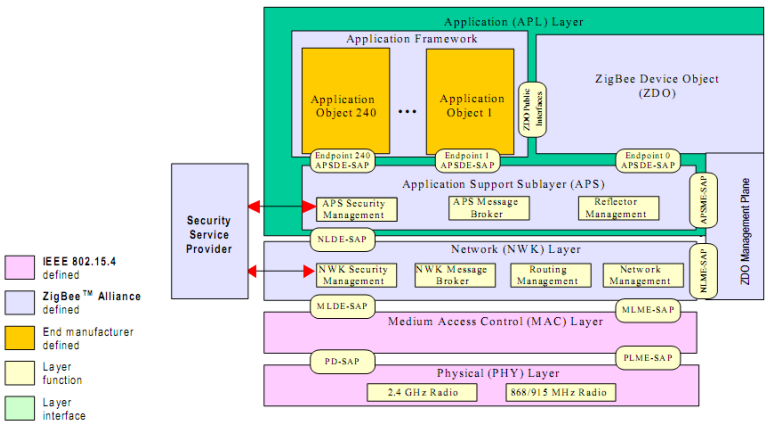

Figura 4.9: Pilha protocolar ZigBee [35].

Ao nível da camada física, existem duas bandas de frequências onde os dispositivos podem

operar, *868/915 MHz* e *2.4 GHz*. As bandas de baixa frequência são apenas licenciadas em determinadas partes do globo, na Europa (868 MHz) e Américas/Austrália (915 MHz). A banda frequências de 2,4 GHz é globalmente utilizada para aplicações industriais científicas e médicas (*ISM: Industrial, Scientific and Medical)* [35].

A camada de controlo de acesso ao meio (*MAC: Medium Access Control*) definida pela especificação *IEEE 802.15.4* controla o acesso ao canal utilizando o mecanismo de *CSMA-CA* (*Carrier Sense Multiple Access with Collision Avoidance*). As suas funcionalidades também incluem a sincronização entre dispositivos e garantia de fiabilidade nas transmissões. Ao nível da camada *MAC* definem-se dois dispositivos: *FFD (Full Function Device*) e *RFD (Reduced Function Device*).

A camada de rede (*NWK: Network*) implementa mecanismos de associação/dissociação de elementos na rede e executa encaminhamento de mensagens até ao destinatário. A descoberta e manutenção das tabelas de encaminhamento é efectuada ao nível desta camada. Existem diferenças entre as camadas de rede dos diferentes dispositivos de uma rede *ZigBee (Coordinator, Routers* e *End Devices).*

A camada de aplicação é responsável pela manutenção das tabelas de *binding,* definição da quantidade de serviço entre dispositivos, determinação dos serviços de aplicação que este disponibilizada e descrição do ambiente no qual os objectos das aplicações desenvolvidas são armazenadas nos dispositivos *ZigBee.*

4.5.2 Camada Física

A camada PHY executa dois tipos de serviços, o *PHY Data Service* e o *PHY Management Service.* O *PHY Data Service* permite a transmissão e recepção de dados através do canal físico rádio.

As funcionalidades da camada PHY são a activação/desactivação do transceptor rádio, verificação da energia do canal (*Energy Detection*), qualidade da ligação (*Link Quality Indication*), selecção do canal de operação e executar o mecanismo de *Clear Channel Assessment* (CCA). O CCA é o processo que determina o corrente estado do canal em determinado instante [36].

As diferentes bandas de frequência possuem diferentes números de canais físicos assim como taxas de transmissão de dados. As frequências mais baixas (868 e 915 MHz) são mais apropriadas para transmissões de maior alcance devido às menores perdas na propagação. Por outro lado, a frequência mais elevada (2,4 GHz) permite maior taxa de transmissão e menor latência. Todas as bandas de frequências são baseados na técnica de espalhamento *DSSS (Direct Sequence Spread Spectrum)*.

A utilização de diversos canais nas diferentes bandas de frequência permite a realocação do canal dentro do mesmo espectro. A técnica de modulação diverge nas duas bandas de frequência, para 868/915 MHz é utilizada modulação *Binary Phase-Shift Keying* (*BPSK)* enquanto para a banda de frequência de 2,4 GHz é usada a modulação *Offset Quadrature Phase-Shift Keying* (O-QPSK).

A Tabela 4.1 apresenta as especificações das bandas de operação do standard *IEEE 802.15.4*.

Tabela 4.1: Descrição das especificações técnicas da camada PHY do standard IEEE 802.15.4 [37].

	Banda	***Cobertura***	***Data Rate (kbps)***	***# de canais***	***Potência de tx (dBm)***	***Sensibilidade de Rx (dBm)***	***Link budget (dB)***
868 MHz	-	*America*	20	1	-3	- 92	89
915 MHz	-	*Europe*	40	10	- 3	- 92	89
2,4 GHz	ISM	*Worldwide*	250	16	- 3	- 85	82

O mecanismo de *DSSS* consiste na divisão prévia dos dados em pequenos pacotes, em que cada um destes é alocado numa frequência ao longo do espectro. Os dados, no ponto de transmissão, são combinados com uma sequência de elevada taxa de transmissão (*chipping code*) que divide os dados de acordo com a taxa de dispersão do canal. A redundância do *chipping code* ajuda o sinal a resistir a

interferências assim como permite que os dados originalmente transmitidos sejam recuperados mesmo que alguns bits tenham sido danificados.

A estrutura do *PHY Protocol Data Units (PPDU) (*Figura 4.10) possui um cabeçalho de sincronização (*SHR: Syncronization Header*), um cabeçalho da camada física (*PHR*: *physical header*) e o campo de dados *(PSDU: PHY Service Data Unit*). O *SHR* permite a sincronização do dispositivo de recepção e o *PHR* possui o restante tamanho da trama (*PSDU).*

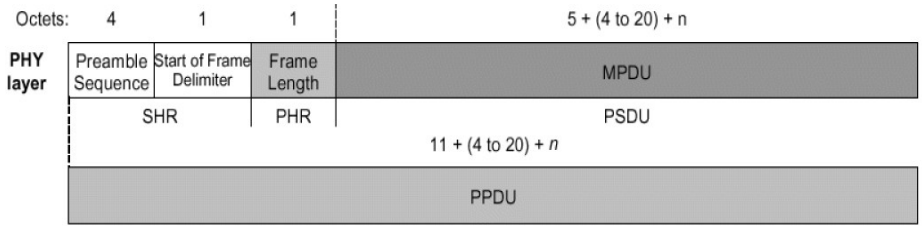

Figura 4.10: Estrutura de uma trama PPDU.

4.5.3 Controlo de Acesso ao Meio

A camada MAC é responsável pela execução dos mecanismos de gestão do modo *beacon*, acesso ao canal físico, alocação de *slots* de comunicação, validação de tramas, entrega de *acknowledges*, associação e dissociação. Nesta camada são definidos dois tipos de dispositivos, *FFD (Full Function Device*) e *RFD* (*Reduced Function Device*). Os dispositivos *FFD* possuem todos os mecanismos definidos pela norma, enquanto os dispositivos *RFD* possuem menor complexidade, estando maioritariamente em modo de poupança de energia.

Existem dois modos de comunicação suportados pela camada MAC: *beacon* e *non beacon*. No modo *non beacon* todos os dispositivos concorrem pelo acesso ao meio utilizando o mecanismo de *CSMA/CA*. No modo *beacon*, os diversos módulos encontram-se sincronizados com os *beacons* periódicos do *Coordinator*. O *modo beacon* permite a atribuição de *slots* temporais a diversos módulos, garantindo fiabilidade e baixa latência nas transmissões. O modo *beacon* utiliza uma estrutura de *superframe* de sincronismo de todos os elementos na rede.

Estrutura Superframe

O modo *beacon* é caracterizado pelo envio periódico de uma trama com estrutura específica, designada por *Superframe* (Figura 4.11). A inicialização desta estrutura é apenas efectuada pelo *Coordinator*. A estrutura é dividida em 16 *slots* temporais de igual período.

O *beacon* de sincronização é enviado em primeiro lugar para que todos os dispositivos na rede se sincronizem com este. A porção activa contém o período de acesso com contenção (*CAP: Contention Access Period*) e o período livre de contenção (*CFP: Contention Free Period*).

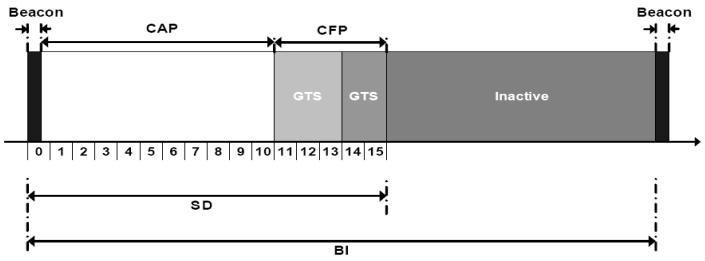

Figura 4.11: Estrutura Superframe [36].

Durante o *CAP*, cada dispositivo que pretende aceder ao meio disputa-o através do mecanismo

CSMA/CA. No período *CFP*, apenas os dispositivos que possuam um *Guaranteed Time Slots* (*GTSs)* alocado podem iniciar uma comunicação sem utilização de *CSMA/CA*. A atribuição de *GTSs* apenas pode ser efectuada pelo *Coordinator.* A utilização dos *GTSs* permite a diminuição da latência e atribuição de largura de banda dedicada.

Na porção inactiva os módulos entram em modo de poupança de energia.

Modelos de transferência de dados

A camada MAC define três modos de transferência de dados entre dispositivos: do *coordinator* para outro dispositivo, de um dispositivo para um *coordinator* e entre dois dispositivos. O fluxo de transmissões depende da utilização ou não de *beacons* [36].

A Figura 4.12 apresenta uma comunicação de um módulo para o *Coordinator* em modo *beacon.* O módulo aguarda a recepção do *beacon* e sincroniza-se com a estrutura *superframe,* enviando a trama de dados. Em modo *non beacon,* o *Network Device* não teria de aguardar a recepção do *beacon,* podendo efectuar a transmissão a qualquer instante.

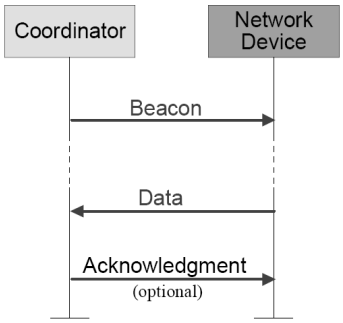

Figura 4.12: Comunicação para o Coordinator em modo beacon.

Quando o *Coordinator* pretende enviar dados em modo *beacon (Figura 4.13)*, este sinaliza a sua pretensão na mensagem de *beacon*. O dispositivo ao receber o *beacon* percebe que existem dados pendentes para lhe serem entregues. O dispositivo envia um *Data Request* ao *coordinator*. Os dados são então enviados para o dispositivo usando o mesmo mecanismo de acesso ao meio.

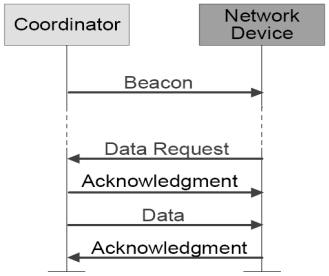

Figura 4.13: Comunicação do Coordinator para outro dispositivo.

Para redes em modo *non beacon*, o envio de dados do *coordinator* para um dispositivo é semelhante, sem que o dispositivo tenha de aguardar por sincronização.

Em redes *peer-to-peer,* cada dispositivo pode comunicar com qualquer outro na sua esfera de interferência sem que tenha de comunicar com o *coordinator*. Existem duas possibilidades de transmissão de dados: o dispositivo transmite os dados através de mecanismo *CSMA/CA* ou executam um processo de sincronismo um com o outro de forma a poupar energia.

Estrutura da trama MAC

O formato *MAC Protocol Data Unit (MPDU*) possui três campos, o *MAC Header* (*MHR), o MAC Service Data Unit* (*MSDU*) e o *MAC footer* (*MFR)*. Cada um dos referidos campos pode possuir outros sub campos, como ilustrado na Figura 4.14.

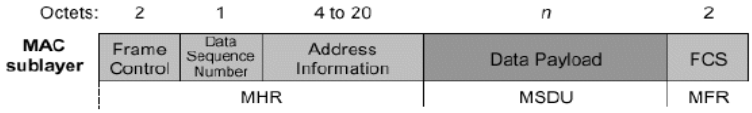

Figura 4.14: Formato de trama da camada MAC.

No *MHR* existe o campo *Frame control* que especifica o tipo de conteúdo da restante trama. Os tipos de trama são trama de dados, trama de *acknowledge,* trama de *beacon* e trama de comando. Os outros campos do *MHR* são o *Data Sequence Number* e o *Address Information*, estes permitem a identificação da mensagem com o respectivo *acknowledge* e o endereço do módulo de destino.

O campo *MSDU* define os campos de dados usados pelas camadas de mais alto nível. O *MAC footer* é composto pelo *Frame Check Sequence* (*FCS*) que valida a integridade da trama.

4.5.4 Camada de rede

Na camada *Network (NWK)* são implementadas as topologias de rede, os mecanismos de associação/dissociação e o encaminhamento de tramas.

Os dispositivos *FFD* e *RFD* definidos pelo protocolo *IEEE 802.15.4* permitem o desenvolvimento de três diferentes dispositivos *ZigBee,* o *Coordinator*, os *Routers* e os *End Devices*. As camadas *NWK* dos três possíveis dispositivos diferem entre si.

As funcionalidades da camada NWK de cada dispositivo *ZigBee* é apresentada na Tabela 4.2.

Tabela 4.2: Funcionalidades da camada NWK para diferentes dispositivos ZigBee [39].

Funcionalidades	***Coordinator***	***Router***	***End Device***
Estabelecimento de nova rede ZigBee	●		
Atribuição de endereços de rede (16 bit)	●	●	
Permissões para que outros dispositivos se associem à rede	●	●	
Manutenção de listas de vizinhos e rotas	●	●	
Reencaminhamento de pacotes de camada NWK	●	●	
Transferência de pacotes de camada NWK	●	●	●
Associação/Dissociação de uma rede	●	●	●

Topologias de rede

A camada de rede *ZigBee* suporte três topologias de rede: *star, cluster tree* e *mesh.* As diferentes topologias disponibilizam diferentes serviços para diferentes tipos de aplicação. Uma rede *ZigBee* pode porém possuir as três topologias integradas.

A topologia *star* consiste num grupo de nós (tipicamente *End Devices*) que apenas comunicam com o seu parente (*Router* ou *Coordinator*). A topologia *star* possui vantagens em aplicações de baixa latência e consumo, pois os *End Devices* podem encontrar-se maioritariamente em modo de poupança de energia. A desvantagem da utilização da topologia *star* deve-se à limitação da extensão máxima da rede ser de dois saltos (*hops*) entre dois *End Devices*. Para além disso, nesta topologia a fiabilidade é baixa, pois não podem existir caminhos alternativos em caso de falha do parente.

A topologia de rede *cluster tree* é constituída por uma árvore de múltiplos saltos entre comunicações de diferentes dispositivos.

Uma rede do tipo *mesh* permite a existência de múltiplos caminhos entre dois dispositivos *ZigBee*, aumentando a fiabilidade da comunicação. Os *routers* na topologia *mesh* podem proceder à descoberta e caracterização de caminhos alternativos disponíveis e seleccionar o melhor. A desvantagem da utilização desta topologia relaciona-se com o elevado consumo de energia dos módulos, pois os *routers* têm de estar constantemente ligados. Nesta topologia, a latência é difícil de estimar.

A Figura 4.15 apresenta exemplos das diferentes topologias de rede da camada *NWK ZigBee*.

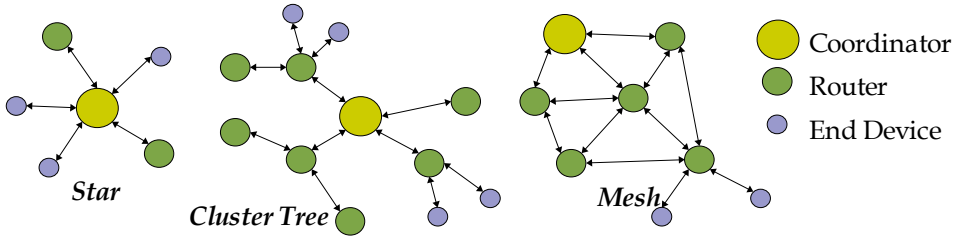

Figura 4.15: Topologias de rede ZigBee.

Arquitectura

A arquitectura da camada NWK executa dois tipos de serviços: *NWK Data Service* (*NLDE: Network Layer Data Entity)* e *NWK Management Service* (*NLME: Network Layer Menagement Entity)* acedidos através de dois *SAPs* (*Service Access Points*) pelas camadas superiores.

O *NDLE* executa os serviços de dados que permitem a transferência de dados entre dois ou mais dispositivos. Este bloco cria o *NPDU* (*Network Packet Data Unit*) e o protocolo de *routing* especifico da topologia, permitindo a transmissão do NPDU ao seu destinatário. O *NLDE* assegura a autenticidade e confidencialidade da transmissão.

A gestão dos serviços da camada *NWK* permitem a uma aplicação interagir com a pilha protocolar *ZigBee,* assegurada pelo bloco *NLME*. Este bloco pode inicializar nova rede, associar ou dissociar-se de uma rede existente, atribuir endereços de rede, descobrir, registar e partilhar informações dos módulos vizinhos e descobrir/manter informações acerca dos caminhos de rede.

Atribuição de endereços de rede

Durante o processo de associação de um dispositivo a uma rede *ZigBee,* é atribuído ao novo dispositivo um endereço de rede lógico.

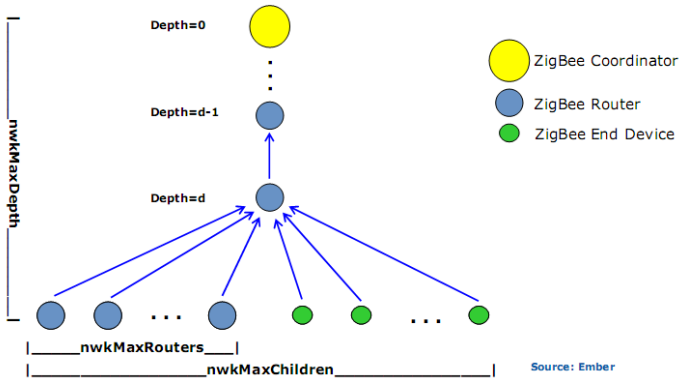

Figura 4.16: Parâmetros máximos do número de nós numa rede ZigBee.

Os endereços de rede são atribuídos pelo *Coordinator* ou pelos *Routers* usando um algoritmo estruturado em árvore. A estrutura da rede é definida por uma entidade designada por *stack profile*.

A *stack profile* inclui a definição da profundidade máxima da rede (*maximum network depth)*, número máximo de filhos *routers* (*maximum number of child routers)* e número máximo de filhos (*maximum number of children*). Estes parâmetros definem a forma da rede (Figura 4.16).

O *maximum network depth* define o número máximo de saltos entre o *Coordinator* e qualquer outro dispositivo. O *maximum number of child routers* e *children* definem o número máximo de *routers* e filhos em geral (*Routers* ou *End Devices*) que se podem associar a um *Router* ou ao *Coordinator.*

Protocolos de Encaminhamento

A camada *NWK ZigBee* possui dois mecanismos de encaminhamento de pacotes, o encaminhamento hierárquico usando o algoritmo de *tree-routing* e o *AODV* (*Ad hoc On-Demand Distance Vector Routing*), baseado em tabelas de encaminhamento [40]. Ambos os dispositivos *Coordinator* e *Routers* possuem um ou mais mecanismos de encaminhamento.

No algoritmo de *tree-routing (*Figura 4.17) os pacotes passam para cima e para baixo na árvore lógica de dispositivos, usando os endereçamentos lógicos de rede previamente atribuídos. A atribuição dos endereços define a localização lógica dos elementos de rede.

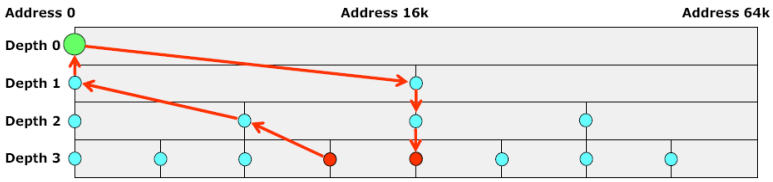

Figura 4.17: Protocolo de endereçamento baseado no algoritmo de tree-routing.

O mecanismo de descoberta de rotas é usado para actualização das tabelas de encaminhamento e para manutenção de informação acerca dos nós vizinhos. Um vizinho é um nó com o qual se pode comunicar apenas com um salto na rede. Este mecanismo usa algoritmo *AODV*. Neste encaminhamento, caso o dispositivo destino possa ser atingido directamente, o pacote é encaminhado directamente, tal como ilustrado na Figura 4.18.

Figura 4.18: Exemplo de encaminhamento por vizinho (Neightbour-routing).

No encaminhamento *mesh,* o *coordinator* e os *routers* mantêm uma tabela do endereço destino do próximo salto do melhor caminho para atingir o dispositivo alvo. A Figura 4.19 ilustra o mecanismo de encaminhamento *mesh*.

Figura 4.19: Exemplo de encaminhamento mesh (Mesh-routing).

4.5.5 Camada de Aplicação

A tecnologia *ZigBee* implementa um conjunto de serviços definidos pelos perfis de aplicação.

Estes perfis permitem a interoperacionalidade entre aplicações *ZigBee* de diferentes fabricantes [39]. Os perfis de aplicação são geridos ao nível da camada Aplicação (*AL: Application*).

A camada de aplicação da tecnologia *ZigBee* é constituída internamente por três blocos, o *Application Support Sublayer* (*APS*), o *ZigBee Device Object* (*ZDO*) e o *Application framework (AF)*. A disposição lógica destes blocos foi apresentada na Figura 4.9.

O bloco *APS* define uma interface entre a camada *NWK* e a restante camada *AL* garantindo um conjunto de serviços usados pelo *ZDO* e pela *AF*. O bloco *APS* mantém as tabelas de *binding*. As tabelas de *binding* definem a capacidade de combinação de dois dispositivos baseados nos mesmos serviços: encaminhar pacotes entre dispositivos associados, definir grupos de endereços e filtrar pacotes de grupos de endereços.

O ambiente onde os objectos da aplicação são alojados na pilha protocolar *ZigBee* é na *Application Framework*. Na *AF,* os objectos definidos pelos fabricantes executam as funções de controlo e gestão das camadas do protocolo *ZigBee* assim como inicialização das funções de rede através das interfaces públicas do *ZDO*. O *ZDO* representa a classe básica de funcionamento que permite a interface entre os objectos da aplicação, o perfil de utilização e a *APS*. O *ZDO* é responsável pela inicialização do APS, da camada *NWK* e o provedor de serviços de segurança (*Security Service Provider*) assim como agrega as informações de configuração da aplicação final de forma a determinar e implementar descoberta, gestão de segurança, gestão da rede e gestão de *binding*.

Perfis

Para descrever os serviços gerados por um dispositivo *ZigBee,* a tecnologia *ZigBee* define o conceito de perfil. Um perfil é um objecto de aplicação da camada AL. Os dispositivos *ZigBee* são modelados utilizando objectos de aplicação que comunicam com outros dispositivos trocando os objectos e atributos do perfil em que estão inseridos, garantindo a interoperacionalidade entre iguais perfis de aplicação de diferentes fabricantes.

A Tabela 4.3 descreve alguns dos perfis actualmente em desenvolvimento pela aliança *ZigBee.*

Tabela 4.3: Lista de perfis em desenvolvimento [41].

Nome	***Descrição***
Infra-estrutura de metrologia avançada	Aplicações de medição de dados e gestão de energia de forma a garantir mais eficiente utilização de energia.
Automação comercial para edifícios	Aplicações no domínio comercial, industrial e institucional para controlo, gestão e monitorização de edifícios.
Cuidados pessoais, de habitações e hospitais	Aplicações de exercício físico pessoal, equipamentos médicos ou hospitalares para monitorização da saúde e bem-estar.
Aplicações de telecomunicações	Aplicações para serviços de valor acrescentado em telecomunicações WAN (*Wide Area Network*). Inclui entrega de dados, pagamentos móveis e partilha de dados.
Aplicações de redes de sensores sem fios	Permite ambiente de monitorização, *tracking* de produtos e monitorização de estruturas.

Existem diversos perfis públicos que podem ser definidos e certificados pela Aliança *ZigBee*, que podem ser utilizados pelos membros da aliança no desenvolvimento de soluções interoperacionais. Cada diferente perfil possui um diferente identificador atribuído pela aliança *ZigBee.* Existem ainda perfis privados cuja utilização pretende ser exclusiva dos fabricantes.

Actualmente, os perfis públicos existentes definem aplicações para domótica (*HA: Home Automation*). O perfil HA é focalizado no controlo de aplicações de forma esporádica e com restrições temporais. São incluídos neste perfil dispositivos genéricos de controlo de iluminação, aplicações para *HVAC* (*Heating, Ventilating and Air Conditioning*) e sistemas de alarme.

4.5.6 Serviços de segurança

A pilha protocolar *ZigBee* permite diversos serviços de segurança (*security*) que são um benefício maior para a tecnologia *ZigBee*. A segurança *ZigBee* utiliza o modelo de segurança do IEEE 802.15.4 que especifica os mecanismos de *Advanced Encryption Standard* (*AES*) e o *Counter mode and Cipher block chaining Message authentication code* (*CCM*). Nas camadas de NWK e AL são configurados as definições de segurança, nomeadamente os tipos de chave (mestre, ligação ou rede) e modo de operação *CCM*.

Os serviços de segurança *ZigBee* garantem segurança ao nível da infra-estrutura assim como dos dados da aplicação. A segurança da infra-estrutura executa o controlo de acesso à rede, mantém uma lista de dispositivos de confiança, integridade dos pacotes encaminhados e prevenção de transporte não autorizado. A segurança dos dados da aplicação executa quatro mecanismos fundamentais de segurança: *freshness*, *integridade da mensagem*, *autenticação* e *encriptação*.

O mecanismo de *freshness* consiste na rejeição de pacotes de dados que tenham sido replicados, o dispositivo compara o valor de *freshness* com o último valor conhecido do mesmo dispositivo e rejeita a trama recebida caso o valor de *freshness* não tenha sido actualizado deste a última transmissão. A *integridade da mensagem* assegura que uma mensagem não foi alterada durante o transporte. A *autenticação* promove a confirmação segura do emissor da mensagem. A autenticação pode ser implementada ao nível da rede (para ataques externos à rede) ou ao nível do dispositivo (para ataques internos à rede). Ao nível da rede existe uma chave comum a todos os dispositivos da rede *ZigBee*. Ao nível do dispositivo, são usadas chaves únicas entre pares de dispositivos. A *encriptação* evita a interpretação das mensagens por qualquer outro dispositivo na rede *ZigBee* a estes não destinados. Tal como a *autenticação*, existe encriptação ao nível da rede e do dispositivo.

4.6 . Soluções Comerciais ZigBee

A tecnologia *ZigBee* pode ser implementada em redes de comunicação sem fios sob diversas formas. Nesta secção serão abordadas diversos transceptores comerciais que implementas as camadas *PHY* e *MAC* da tecnologia *ZigBee* assim como soluções de módulos integrados.

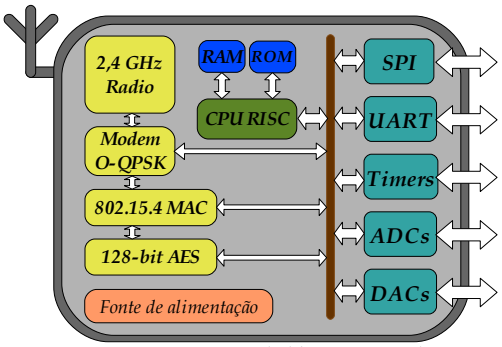

Figura 4.20: Diagrama de blocos tipico de um módulo ZigBee.

A Figura 4.20 apresenta os componentes físicos típicos de um módulo de comunicações sem fios *ZigBee*. O transceptor (*2,4GHz Radio, Modem O-QPSK, 802.15.4 MAC e 128-bit AES*) implementa as camadas *IEEE 802.15.4 PHY* e *MAC*, o *CPU* implementa as restantes camadas da pilha *ZigBee*. Tipicamente, existem diversos periféricos associados ao CPU que podem ser utilizados pelas aplicações, tais como *ADC (Analogue to Digital Converter)*, *DAC (Digital to Analogue Converter)*, portas de comunicação série (*USART, SPI, I2C, etc*) e pinos digitais de I/O.

Diversos fabricantes implementam, na saída rádio, um amplificador (*PA: Power Amplification*) de forma a aumentar a potência máxima de transmissão e amplificadores para ruído baixo (*LNA: Low Noise Amplifier*) para aumentar a sensibilidade de recepção de dados

4.6.1 Transceptores IEEE 802.15.4

Os transceptores de tecnologia *ZigBee* consistem num circuito integrado que implementa as camadas *PHY* e *MAC* da norma *IEEE802.15.4* fazendo a ponte entre a antena e o *CPU* onde da restante pilha protocolar é armazenada.

Cada transceptor pode operar como *Full Function Device* (*FFD*) ou como *Reduced Function Device* (*RFD*), suportar as topologias de *peer-to-peer*, ponto-a-ponto, ponto-multiponto e *mesh* assim como implementar os diversos mecanismos de acesso ao meio e de segurança da camada *MAC.*

A Tabela 4.4 apresenta as características de diversos transceptores comerciais.

Tabela 4.4: Características técnicas de diversos transceptores IEEE 802.15.4 comerciais. (X – Não especificado)

Características	***Microchip[43] MRF24J40***	***Freescale [44] MC1320x***	***Texas CC2420 [45]***	***Atmel [47] AT86RF230***	***UBEC UZ2400 [48]***	***ZMD [49] ZMD44102***
Frequência	2,4 GHz	2,4 GHz	2,4 GHz	2,4 GHz	2,4 GHz	868/915 MHz
Package	QFN 40pins	QFN 32 pins	QLP 48 pins	QFN 32 pins	QFN 40 pins	QFN 48 pins
Interface	4-wire SPI	4-wire SPI	4-wire SPI	4-wire SPI	4 wire SPI	4 wire SPI
Buffering de dados	4 FIFOS de tx,1 de rx	On-chip RAM	Rx: 128 bytes, Tx: 128 bytes	128 bytes SRAM	Tx-512 bytes Rx-144 bytes	Tx-128 bytes Rx-256 bytes
Consumo	Rx: 22mA. Tx:18 mA. Sleep: 2µA	Rx: 37 mA Tx: 30 mA Sleep: 1µA	Rx:18,8 mA Tx:17,4 mA	Tx: 17 mA, Rx: 16 mA, Sleep:0,1µA	Tx: 23 mA Rx: 19 mA, Sleep: 2 µA	Tx: 28 mA Rx: 29 mA, Sleep: 3 µA
Tensão de alimentação	2,4 a 3,6 V	2,0 – 3,4 V	1,6 a 3,6 V	1,8 – 3,6 V	2,4V a 3,6V	2,2V a 3,6V
Dimensões	6 mm x 6 mm	5 mm x 5 mm	7 mm x 7 mm	5 mm x 5 mm	6 mm x 6 mm	7mm x 7mm
Indicação RSSI	- 50 a 0 dBm	X	-100 a 0 dBm	-91 a +10dBm	-35 a – 100dBm	-20 a –100 dBm
Sensibilidade min. de Rx	-91 dBm	-92 dBm	-95 dBm	- 101 dBm	- 95 dBm	-98 dBm
Potência de Tx	0 dBm	-27 a +3dBm	24 a 0 dBm	-17 a +3 dBm	0 dBm	0 dBm
Alcance máximo	100 m LOS	X	100m LOS	700 m LOS	100 m LOS	100m LOS
Preço	1,94€ / un [43]	[MC13202]: 4,26 €/un[42] [MC13203]: 4,71€/un.[42]	8,30€ / un [42]	5,15€ / un [42]	X	X

4.6.2 Soluções embebidas

O tempo de implementação de soluções baseadas na tecnologia *ZigBee* pode ser reduzido recorrendo-se a módulos *OEM*. A arquitectura típica deste tipo de módulos foi apresentada na Figura 4.20. O microcontrolador possui a pilha *ZigBee* assim como uma *API (Application Programming Interface)* de comunicação com um possível *host.*

Para além dos módulos integrados, diversas pastilhas de silício integram o microcontrolador e o transceptor. Estes sistemas são designados de *System on chip (SoC)* ou *System in Package (SiP)*. Este tipo de circuitos diminui o custo de implementação e tamanho do circuito. A desvantagem do uso deste tipo de módulos reflecte-se na necessidade de implementação de circuito de integração da

antena RF, tal como nas soluções baseadas em transceptores.

A Tabela 4.5 descreve alguns dos referidos circuitos comerciais.

Tabela 4.5: Características técnicas de sistemas integrados ZigBee.

Características	***Texas CC2430/31 [45]***	***Feeescale MC13214 [44]***	***Jennic JN5139 [53]***	***Ember EM260 [51]***
Frequência	2,4 GHz	2,4 GHz	2,4 GHz	2,4 GHz
Package	QLP de 48 pinos	LGA de 71 pinos	QFN 56 pinos	QFN 40 pinos
CPU Flash	[CC2430]:32,64,128kB [CC2431]: 128 kB	60 kB	[ROM]: 192kB	128 kB
CPU RAM	8 kB	4 kB	8, 16, 32 ou 96kB	5 kB
Interfaces I/O	1xADC, 2xUSART, 21 pinos I/O	8xADC, 2xUSART, 32 pinos I/O	4xADC, 2xDAC, 2xUSART, 2 timers, 21 pinos I/O	3 pinos I/O, 1xUSART, 1 SPI
Consumo	Tx: 27mA, Rx: 27mA, Sleep: 0,5µA	Tx: 30mA, Rx: 327mA, Sleep: 0,2µA	Tx: 34mA, Rx: 34mA, Sleep: 0,2µA	Tx: 28mA, Rx: 28mA, Sleep: 1µA
Tensão	2,0 – 3,6 V	2,0 – 3,4 V	2,2 – 3,6 V	2,1 – 3,6 V
Dimensões	7mm x 7mm	9mm x 9mm	8mm x 8mm	6mm x 6mm
Sensibilidade min. de Rx	-92 dBm	-92 dBm	-97 dBm	-99 dBm
Potência de tx	0 dBm	De -27 a +3 dBm	+3 dBm	+2,5 dBm
Preço	[CC2430]: $6,80 (USD) (+100) [*45*] [CC2431]: $8,10 (USD) (+100) [*45*]	$4.61 (USD) (+1000) [*44*	5,92 € (+100) [42]	$5,83 (USD) [51]

O *SoC CC2431* difere do *CC2430* por possuir uma ferramenta de localização por *hardware* baseada em medições de *RSSI* (*Received Strength Signal Indication*).

Tipicamente, nas soluções integradas, os fabricantes produzem um perfil próprio privado que implementa uma estrutura de comunicação série, para que os módulos sejam utilizados em diversas aplicações como protocolo de comunicações *wireless*.

Nas próximas secções serão apresentados diversos módulos comerciais integrados.

ZigBit da Meshnetics

Existem dois módulos *OEM* da *Meshnetics* que se diferenciam pela presença de uma antena dupla do tipo *chip* (*ZDM-A1281-A2 – Figura 4.21*) ou um conector *RF (ZDM-A1281–B0*) para ligação de antena externa. Ambos os modelos são baseados na tecnologia da *Atmel*. O transceptor é o *AT86RF230* e o microcontrolador o *Atmega1281*.

A *Meshnetics* disponibiliza duas pilhas de protocolos: *ZigBeeNet* e *eZeeNet*. A stack *ZigBeeNet* é conforme com a especificação *ZigBee* enquanto a pilha *eZeeNet* implementa um perfil privado (*ZigBee*) para a recolha de dados de sensores.

A Tabela 4.6 descreve as principais características dos módulos *ZigBit*.

Figura 4.21: Módulo ZigBit da Meshnetics (ZDMA1281 – A2).

Tabela 4.6: Características técnicas dos módulos ZigBit [52].
(XX - Informação não disponível.)

Características	***Descrição***
Transceptor	AT86RF230
Antena	Chip ou conector RF
Consumo	*RX*: 19 mA ,*TX*: 18 mA ,*Sleep*: 6 µA
Tensão de alimentação	1,8V – 3,6V
Dimensões	[ZDMA1281 – A2] : 24 mm x 13,50 mm
	[ZDMA1281 – B0] : 18,8 mm x 13,5 mm
Memória	[FLASH] : 128 kB
	[RAM] : 8 kB
	[EEPROM] : 4 kB
Potência de transmissão	3 dBm
I/O	*I2C, SPI/USART, USART* com controlo *CTS/RTS*, 4 linhas de *ADC*, 10 linhas de I/O (podem ser 30)
Preço	[ZDMA1281 – A2]: 34,08 € [42]
	[ZDMA1281 – B0]: 30,98 € [42]

IP-Link da Helicomm

A *helicomm* possui diversos módulos *OEM* que diferem pelo tipo de antena que possuem e pela potência máxima de transmissão (máx.: 18 dBm). De entre a gama de cinco versões de módulos *ZigBee* da *helicomm*, são apresentados na Tabela 4.7 os módulos *IP-Link 1221-2034 e 1221-2134*.

A Figura 4.22 ilustra os referidos módulos da *Helicomm*.

Figura 4.22: Módulo IP-Link da Helicomm [46].

Tabela 4.7: Características técnicas dos módulos da helicomm [46.
(X – Informação não disponível.)

Características	***IP-Link 1221-2034***	***IP-Link 1221-2134***
Transceptor	X	X
CPU	C8051F133 (*Silicon Labs*)	C8051F133 (*Silicon Labs*)
Antena	Chip	Externa
Consumo	Tx:37mA, Rx:43mA, Sleep: 40µA	Tx:100mA, Rx:43mA, Sleep: 40µA
Tensão	3,3 V	3,3 V
Dimensões	41 mm x 19 mm	46 mm x 19 mm
Memória	RAM: 8 kB, ROM: 64kB	RAM: 8 kB, ROM 64kB
Potência de transmissão	-25 a +0 dBm	-15 a +10 dBm (Máx: 350m LOS)
Interfaces I/O	2xUSART, 2xADCs, 2 Comparadores, 11 pinos I/O	2xUSART, 2xADCs, 2 Comparadores, 11 pinos I/O
Preço	X	X

JN5139 Jennic

A empresa *Jennic* utiliza o seu *SoC (System on Chip)* para produção de módulos integrados. A Tabela 4.8 apresenta as características técnicas dos módulos OEM da *Jennic* e a Figura 4.23 ilustra o módulo *JN5139*.

Tabela 4.8: Características técnicas dos módulos JN5139 da Jennic [53].

Características	***JN5139-xxx-M00/01/03***	***JN5139-xxx-M02/04***
Transceptor + CPU	SoC JN5139	SoC JN5139
Antena	M00: on board	M02: Conector SMA
	M01: Conector SMA	M04: Conector uFI
	M03: Conector uFI	-
Consumo	Tx:37mA, Rx:37mA, Sleep: 2,8µA	Tx:120mA, Rx:45mA, Sleep: 2,8µA
Tensão	2,7 – 3,6 V	2,7 – 3,6 V
Dimensões	18 mm x 30 mm	18 mm x 41 mm
Memória	RAM: 96kB, ROM: 192kB	RAM: 96kB, ROM: 192kB
Potência de transmissão	+2,5 dBm	+ 19 dBm
Interfaces I/O	4xADCs, 2xDACs, 2xtimers, 2xUSARTs, 21 pinos I/O	4xADCs, 2xDACs, 2xtimers, 2xUSARTs, 21 pinos I/O
Preço	***M00:***19,03€; ***M01:***21,62€; ***M03:***21,92 €[42]	***M02:*** *27,59*€ [42]

Figura 4.23: Módulo integrado JN5139 da Jennic [53].

4.6.3 XBee/XBee-PRO da MaxStream

Os módulos *XBee/XBee-PRO* (Figura 4.24) da *MaxStream* permitem a implementação de redes *IEEE 802.15.4* ou *ZigBee.* A Tabela 4.9 apresenta as características técnicas destes módulos.

Figura 4.24: Módulo XBee-PRO com antena chip.

Tabela 4.9: Características técnicas dos módulos XBee [54].

Características	***XBee***	***XBee-PRO***
Transceptor	MC13193 (freescale)	MC13193 (freescale)
CPU	MC9S08GT60 (freescale)	MC9S08GT60 (freescale)
Antena	Chip, whip ou conector RF	Chip, whip ou conector RF
Consumo @ 3.3V	Tx: 45 mA, Rx: 50 mA, Sleep: 83 µA	Tx: 215 mA, Rx: 55 mA, Sleep: 115 µA
Tensão	2,8 – 3,4 V	2,8 – 3,4 V
Dimensões	24,4 mm x 27,6 mm	24,4 mm x 32,9 mm
Memória	ROM: 60kB	ROM: 60kB
Potência de transmissão	0 dBm	18 dBm
Interfaces I/O	8 pinos I/O, 6 ADCs, 1 USART, 2 PWMs	8 pinos I/O, 6 ADCs, 1 USART, 2 PWMs
Preço	$19 (USD)	$32 (USD)

Existem dois tipos de tecnologia complementares que podem operar nos módulos *XBee,* a *IEEE 802.15.4* e a *ZigBee.* O *IEEE 802.15.4* possui maior número de parâmetros configuráveis embora não permite o reencaminhamento de pacotes.

Existem dois tipos de módulo *ZigBee* disponibilizados pela *Maxstream,* o *XBee* e o *XBee-PRO*. Os dois módulos diferem essencialmente na performance *RF* (*Radio Frequency*) entre eles. O *XBee-PRO* permite o envio de tramas *ZigBee* com potência de saída máxima de 18 dBm e os módulos *XBee* possuem potência de saída de 0 dBm.

Arquitectura

Os módulos *XBee/XBee-PRO* recorrem aos dispositivos da *freescale* (transceptor e microcontrolador). A arquitectura dos módulos *XBee* é ilustrada na Figura 4.25.

Os módulos *XBee* são constituídos internamente por três blocos, o *processador*, o transceptor e um *switch RF*. O processador (*MC9S08GT60)* efectua a interface com um *host*, sendo o meio de efectuar configurações, receber e enviar dados. O transceptor *MC13193* efectua a interface rádio a *2.4 GHz*. Por fim, existe um interruptor *RF* que alterna entre os modos *receive* e *transmit*. Sempre que o módulo pretende transmitir direcciona a ligação da antena para o *transmit* do *transceptor*. Após transmitir o *transceptor* volta a colocar a antena conectada ao *receive*, aguardando a recepção de pacotes *ZigBee.*

Para além da arquitectura da Figura 4.25 os módulos *XBee-PRO* possuem, após o *RF switch*, um mecanismo de amplificação de sinal *RF* para a transmissão e um *LNA (Low Noise Amplifier*) para a

recepção. O *LNA* permite que a sensibilidade de recepção dos módulos *XBee-PRO* seja de -100 dBm.

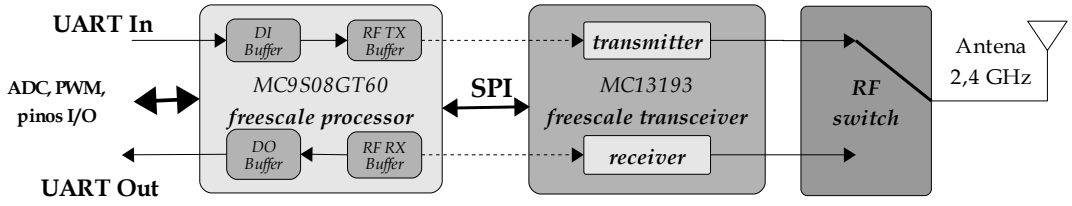

Figura 4.25: Arquitectura dos módulos XBee da Maxstream.

Modos de Operação

Os módulos *XBee* suportam dois modos de operação: *modo transparente* e o *modo API.* Os possíveis modos são seleccionados previamente.

No *modo transparente* os módulos comportam-se como uma linha série, ou seja, os dados recebidos na *UART* são transmitidos sem qualquer interpretação dos dados. O modo *transparente* opera da mesma forma na recepção de dados, tudo que recebe por RF envia para porta série. No modo transparente as configurações são efectuadas através de comandos AT (*Attention).*

A Tabela 4.10 exemplifica uma configuração de um registo através de comandos AT.

Tabela 4.10: Exemplos de comandos AT.

Configuração	Comando AT	Descrição	Resposta AT
Alteração do registo de endereço destino	+++	Entra em modo de comando	OK<CR>
	ATDL1F3E<CR>	Altera endereço destino *low*	OK<CR>
	ATWR<CR>	Salva configuração em memória	OK<CR>
	ATCN<CR>	Sai do modo de comando	OK<CR>

O *modo API* permite efectuar operações de configuração dos módulos, monitorização do estado das mensagens transmitidas e validação das mensagens recebidas. Neste modo, os dados transmitidos são interpretados e verificados. Existe uma estrutura de tramas que permitem efectuar configurações, enviar e receber dados. Na Figura 4.26 é apresentada a estrutura de uma mensagem em modo *API*.

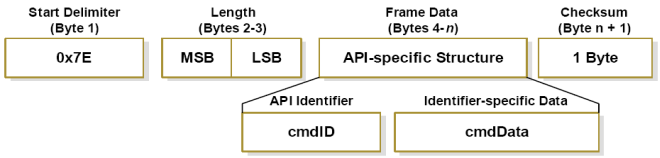

Figura 4.26: Estrutura das mensagens em modo API [54].

Uma trama em modo *API* inicia-se sempre com o caracter 0x7E (*Start Delimiter*). Os dois bytes seguintes (*Length*) indicam o tamanho do campo de dados (*API-specific Structure*). O *CheckSum* completa a trama *API,* permitindo a confirmação de mensagem bem recebida por parte *do módulo receptor.* O campo *cmdID* identifica o tipo de trama (*Modem Status, AT Command, ZigBee Transmit Request, ZigBee Transmit Status* ou *ZigBee Received Packet*) e a composição do campo *cmdData*.

Capítulo 5

Arquitectura, operação e caracterização técnica do sistema Wireless Temp I/O

5.1 . Introdução

Na proposta da arquitectura do sistema *Wireless Temp I/O* existem múltiplas estações de validação com comunicações sem fios a operar em simultâneo (Figura 5.1). Em relação ao produto *Temp I/O,* apresentado no capítulo 2, são introduzidas novas funcionalidades, enumeradas nos seguintes pontos:

- ✔ Comunicação sem fios entre o PC e os terminais de registo de ponto;
- ✔ Possibilidade de existência de múltiplos terminais de registos;
- ✔ Gestão de acesso a locais reservados. Cada funcionário possui diferentes permissões para diferentes locais de acesso reservados;
- ✔ Diminuição da carga computacional do PC para execução de outras tarefas enquanto o sistema de controlo de assiduidade opera em *background* (aplicação no PC mais leve pois a identificação biométrica é efectuada nas estações remotas);
- ✔ Diferentes períodos de marcação por defeito para diferentes estações de registo;
- ✔ Interface com o utilizador simplificada e de maior robustez;
- ✔ Flexibilidade de instalação e mobilidade de operação.

A conectividade *wireless* aliada à flexibilidade de utilização das estações remotas permite a existência de períodos de tempo em que estas não possuem conectividade com o módulo central, quer pela presença de um obstáculo, degradação de sinal devido a ruído externo ou simplesmente pela aplicação do módulo central estar inactiva. Para este modo de operação foram definidos mecanismos que permitem a continuidade do registo dos tempos de trabalho e do controlo de acesso. As estações remotas operaram então em modo *stand alone*.

A intuitividade da interacção homem-máquina é outro dos requisitos fundamentais na nova

arquitectura do sistema *Temp I/O*.

A utilização de comunicações sem fios permite a existência de múltiplas estações de registo com a respectiva flexibilidade associada. A mobilidade é então outra das novas funcionalidades do sistema de controlo de assiduidade.

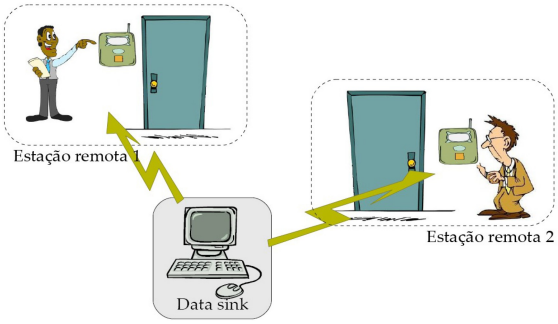

Figura 5.1: Ilustração da nova proposta do sistema Wireless Temp I/O.

No presente capítulo apresenta-se a arquitectura e modo de operação da versão *wireless* para o sistema *Temp I/O*. Na secção seguinte é definida a arquitectura do sistema assim como dos módulos que o constituem. O modo de interacção com o utilizador e o funcionamento interno dos módulos remotos serão também apresentados. O protocolo de comunicações desenvolvido para troca de dados entre os elementos do sistema é introduzido na secção *Comunicações sem fios*. Por último, será efectuada uma caracterização técnica dos módulos implementados no protótipo desenvolvido.

5.2 . Arquitectura do sistema Wireless Temp I/O

O sistema *wireless Temp I/O* é constituído por um módulo central (*data sink*) e por diversos módulos de validação remotos (estações remotas). O *data sink* regista os dados relativos a todas as operações executadas em cada *módulo de validação sem fios* (*WVM*: *Wireless Validation Module*) [1].

A Figura 5.2 ilustra o diagrama de blocos simplificado do sistema de controlo de assiduidade com multiposto e comunicações *wireless.*

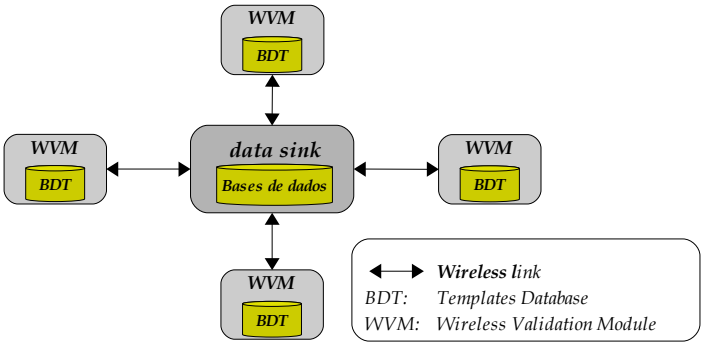

Figura 5.2: Diagrama de blocos generalizado do sistema.

As estações remotas (*WVM)* identificam os funcionários através de análise da sua impressão digital. Os dados são transmitidos para o *data sink* através da interface sem fios. Para proceder à identificação em cada *WVM*, é necessária a existência de uma *Base de Dados de Templates* (*BDT)* em cada *WVM*. Um *template* é um conjunto de dados digitalmente codificados que definem as características biométricas únicas de um indivíduo.

A distribuição da *BDT* por todos os módulos *WVM* da rede, aumenta os níveis de segurança do

sistema e reduz o tráfego na rede sem fios. Sendo as *BDTs* coerentes, quando um funcionário executa uma operação, apenas o seu identificador é enviado pela rede *wireless*. O processo de registo de um novo funcionário é o único procedimento no qual o *template* é transmitido pela rede sem fios. A transferência do *template* pela rede é, no entanto, um processo seguro pois os dados usam encriptação na comunicação. A referida encriptação é suportada pela tecnologia *ZigBee*.

No *data sink*, uma operação é registada em *base de dados de operações (BDO)* para posterior criação de relatórios pela aplicação. Cada registo de operação contém dados como a data, hora, identificador de funcionário, operação executada (*Entrada ou Saída)* e a informação relativa ao acesso (cedido ou negado).

5.2.1 Data sink

O *data sink* funciona como base de dados e gestor de restante sistema. O *data sink* executa diversas configurações tais como: registo de novos utilizadores, sincronização de data/hora, atribuição de permissões e configuração de períodos de marcação por defeito.

A Tabela 5.1 descreve os campos das três bases de dados armazenadas no *data sink*.

Tabela 5.1: Descrição das base de dados presentes no data sink.

Nome	***Descrição***	***Campos***
BDF (Base de Dados de Funcionários)	A *base de dados* referente aos funcionários possui o identificador deste assim com as suas informações pessoais, por exemplo, primeiro e último nome e os *templates* biométricos.	*- User ID* *- Primeiro nome* *- Último nome* *- Templates*
BDW (Base de Dados de WVMs)	A base de dados *WVM* possui o seu identificador, os *IDs* dos funcionários com permissões de acesso, o nome lógico da interface (por exemplo: "*Armazém*") e a data da última trama recebida.	*- WVM ID* *- User IDs (permissões)* *- Nome lógico* *- Data de última trama.*
BDO (Base de Dados de Operações)	A base de dados de registo de operações possui registo de todas as operações executadas por todos os funcionários. Regista a data e hora do momento do registo, quem e em que WVM foi executado, qual a operação e se o acesso foi cedido ao utilizador.	*- User ID* *- WVM ID* *- Data (Dia, Mês, Ano)* *- Tempo (Hora, Min., Seg)* *- Operação/Acesso*

Quando o *data sink* recebe um pedido de registo, extrai da *BDF* o primeiro e último nome do funcionário, e regista a operação na *BDO*. Após este registo, o *data sink* verifica na *BDW* se o utilizador possui permissões de acesso naquela *WVM*. Por fim, é enviada uma mensagem de confirmação do sucesso de registo da operação. A mensagem de confirmação é constituída pelo primeiro e último nome do funcionário, operação registada e tipo de permissão de acesso do funcionário que efectuou o registo, se tal for o caso.

O registo de novas *WVMs* é também uma tarefa efectuada pelo *data sink*. O registo de uma nova interface é um processo efectuado de forma automática. Os módulos WVM possuem um endereço de produção, o qual quando detectado na rede gera o evento de registo de nova WVM. Durante o registo da nova estação são enviados os dados biométricos dos funcionários registados após confirmação de um administrador do sistema.

O *data sink* é constituído por um sistema computacional de elevado desempenho (memória e velocidade de processamento) e uma interface de comunicação que opera como *gateway* das comunicações *wireless*. O *gateway* é conectado ao sistema computacional através da interface *USB (Universal Serie Bus)*.

5.2.2 Estações remotas

Os módulos *WVM (Wireless Validation Module)* procedem à identificação do utilizador através da análise da sua impressão digital, actuam sobre os mecanismos de abertura de acesso e promovem a interacção com os funcionários.

Cada *WVM* é constituído por um conjunto de módulos controlados pelo *MCU* (*MicroController Unit*). A Figura 5.3 ilustra a arquitectura e interfaces de ligação das estações remotas.

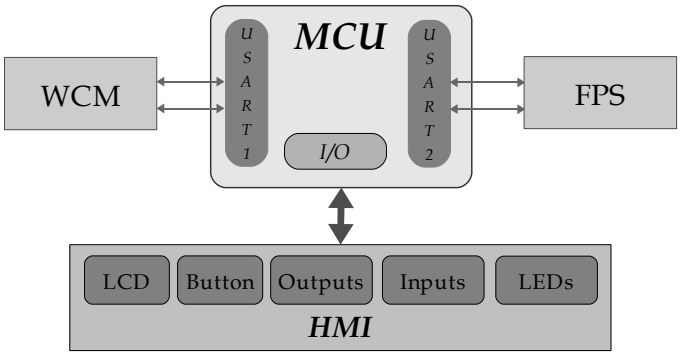

Figura 5.3: Arquitectura e ligações entre os periféricos internos à WVM.

A *HMI (Human Machine Interface)* integra os mecanismos de interacção com o utilizador. Este bloco possui um *LCD*, um botão, entradas e saídas digitais e alguns *LEDs*. O *FPS (Fingerprint Sensor)* identifica os funcionários através da análise da sua impressão digital. O *WCM (Wireless Communication Module)* efectua a conectividade *wireless* com o *data sink*. A unidade de processamento *(MCU)* interliga os restantes componentes do bloco *WVM*, recebendo informações do *FPS* e *WCM* através de protocolo série (*UART: Universal Asynchronous Receiver Transmitter*).

Os periféricos da *HMI* comunicam com o *MCU* através dos pinos de I/O. A interface do LCD usa um protocolo paralelo de comunicação através de barramento de dados e alguns sinais de controlo.

A *Human Machine Interface (HMI*) é constituída por um *display LCD*, um botão de selecção de operação, por um conjunto de entradas e saídas digitais e por alguns LEDs de sinalização.

As entradas e saídas digitais são parte integrante da funcionalidade de controlo de acessos. Estes sinais digitais permitem o accionamento e monitorização do sistema electromecânico de abertura do acesso. O *LCD* permite o envio de mensagens ao utilizador. O botão presente na *HMI* tem como finalidade permitir que o utilizador seleccione a operação que pretende efectuar, *Entrada* ou *Saída*. O botão desenvolvido possui a vantagem de ser accionado sem contacto físico. O botão usa tecnologia de infravermelhos para detecção da mão do utilizador a curta distância.

O sensor de impressões digitais (*FPS: Fingerprint Sensor*) é o dispositivo de extracção de impressões digitais usado para determinar a identificação de um utilizador. O processo de identificação consiste na atribuição de um *User ID* a uma impressão digital extraída do sensor de impressões digitais. A *base de dados de templates* local a cada módulo *WVM* encontra-se armazenada neste dispositivo.

O módulo *FPS* é constituído internamente por um sensor de impressões digitais e por uma unidade de processamento. O sensor é o *hardware* onde cada funcionário deve colocar o dedo para extracção do *template*. A unidade de processamento efectua a leitura do *template* no sensor e executa um algoritmo que verifica (*matching*) se o *template* extraído corresponde a algum utilizador previamente registado. O *FPS* comunica com o *MCU* informando-o dos eventos ocorridos neste módulo.

O módulo de comunicações sem fios (*WCM)* é o módulo responsável pela troca de dados com o *data sink*. Este módulo é o *gateway* das comunicações *wireless* para as estações remotas. O *WCM* é responsável pela conectividade da *WVM* ao sistema global de controlo de assiduidade. A tecnologia usada no protótipo desenvolvido é a tecnologia *ZigBee*.

A unidade de controlo (*MCU: Microcontroller Unit*) processa todas as mensagens emitidas pelo *data sink* e pelo *FPS*, efectuando todas as configurações pedidas pelos comandos recebidos. O *MCU* efectua ainda, periodicamente, diversos procedimentos de gestão da interface *WVM*. O módulo *MCU* é implementado recorrendo a um controlador *RISC* de baixa complexidade.

5.3 . Modo de utilização das estações remotas

Durante o processo de registo de uma operação, o utilizador apenas tem de seleccionar a operação que pretende efectuar e introduzir o seu dedo no leitor de impressões digitais. Na primeira linha do *LCD* são apresentadas duas informações alternadamente: a data/hora actualizada e o nome da interface. A segunda linha contém a operação seleccionada *(Entrada* ou *Saída)*, como ilustrado na Figura 5.4.

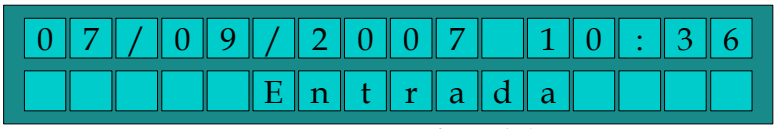

Figura 5.4: Mensagem no LCD referente à data e operação.

Caso a operação seleccionada no LCD seja concordante com a que o funcionário pretende executar, o funcionário apenas tem de colocar o dedo no leitor de impressões digitais. Para alteração da operação seleccionada basta accionar o botão. Os dois modos de operação possíveis, *Entrada e Saída* aparecem alternadamente cada vez que o botão é accionado.

Quando uma impressão digital é extraída com sucesso pelo leitor, o LED amarelo acende indicando que o utilizador pode retirar o dedo do leitor. Caso o utilizador seja identificado, é exibida uma mensagem no *LCD* com o nome do utilizador, a operação executada e a hora. A Figura 5.5 é um exemplo de uma mensagem de confirmação de registo de uma operação.

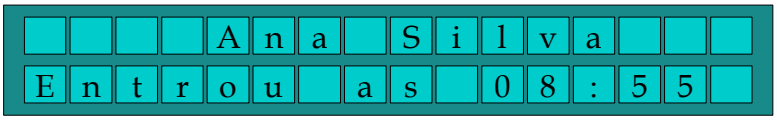

Figura 5.5: Mensagem de LCD para confirmação de operação.

Caso um utilizador possua permissões de acesso, o mecanismo automático de abertura da porta é accionado e o LED verde acende.

Caso a interface remota opere em modo *stand alone*, a mensagem que aparece no *LCD* difere da anterior, é então exibida mensagem da Figura 5.6, em que *XXX* é o identificador do utilizador na rede (já que o nome não está armazenado no módulo local). Neste modo de operação, o LED vermelho fica constantemente ligado, indicando que não existe conectividade com o *data sink*. Caso contrário, o LED deve permanecer intermitente.

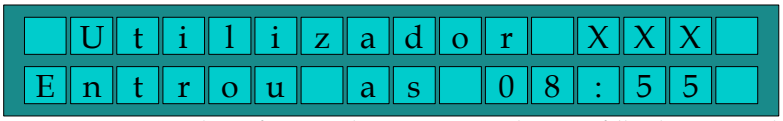

Figura 5.6: Mensagem de confirmação de operação quando existe falha de conectividade.

5.4 . Máquina de estados dos WVMs

Existem três estados essenciais em que cada *WVM* pode operar: *Inicialização*, *Identificação* e *Configuração*. A Figura 5.7 apresenta uma máquina de estados das estações remotas.

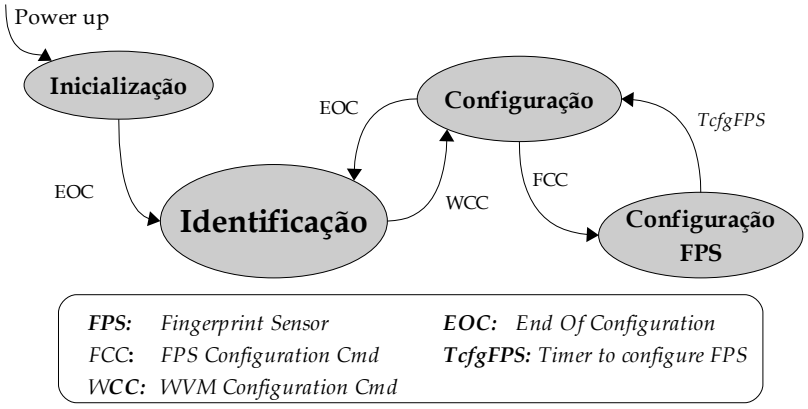

Figura 5.7: Diagrama de estados de operação para uma WVM.

5.4.1 Inicialização

O estado de *Inicialização* é executado sempre que o *WVM* é colocado em funcionamento (*Power Up*). Para além de executar a inicialização de todo o *hardware* periférico, este estado verifica se os diversos módulos se encontram a operar conforme previsto.

O processo de *Inicialização* inclui a actualização da estação remota (novos funcionários, alteração das permissões, actualização de data e hora).

5.4.2 Identificação

O modo de *Identificação* é o estado por defeito dos módulos remotos do sistema *Wireless Temp I/O*. O modo de operação do estado de identificação pode ser executado segundo dois processos algo distintos. O primeiro, para condições normais de funcionamento, denominado de *Modo de Registo Normal (MRN)*, e o segundo para operação em modo *stand-alone*, denominado de *Modo de Registo Degradado (MRD)*. Os dois referidos processos diferenciam-se pela forma como o registo da operação é armazenado. No segundo modo os registos de operações são armazenados localmente em memória não volátil. No modo *MRN,* o registo das operações é efectuado no *data sink*. Os dados são transmitidos ao *data sink* através de interface *wireless*, e é neste dispositivo que a operação deve ser registada (por motivos de recursos e centralização da informação). O *modo MRD* é apenas activado quando não existe conectividade com o *data sink*.

Cada *WVM* possui uma base de dados local de utilizadores com permissões de acesso. Os utilizadores que possuem a referida permissão devem ser previamente configurados através da aplicação no *data sink.* Assim, apenas aos utilizadores referenciados nesta base de dados local é garantido acesso. Os restantes utilizadores podem porém registar as operações de assiduidade. Ambas as opções são limitadas ao espaço de memória disponibilizado para o efeito.

Tabela 5.2: Campos da base de dados local para registo de operações.

Campos	***Espaço de memória necessário***
User ID	2 bytes
Hora	3 bytes (Hora, Minutos, Segundos)
Data	3 bytes (Dia, Mês, Ano)
Operação	1 bit
Acesso	1 bit

Existe uma tarefa que verifica a existência de conectividade com o *data sink* periodicamente. Esta

tarefa consiste num envio de comando e aguarda pela recepção do respectivo *acknowledge*. Em caso de a conectividade ser retomada, as informações dos registos entretanto executados são actualizadas para o *data sink.* Para o modo *MRD*, cada registo contem os campos referenciados na Tabela 5.2.

A Figura 5.8 descreve a forma como o espaço de memória destinado ao armazenamento de registos é mapeado. Cada registo de uma operação contém 9 bytes de dados. O ponteiro *reg_ptr* indica o endereço do bloco de memória livre para o próximo registo. Este é incrementado de bloco em bloco e aponta para o primeiro *byte* do bloco. O ponteiro *reg_alr_sent* indica os blocos de memória que já foram actualizados com sucesso para o *data sink*. O *reg_alr_sent* apenas é incrementado quando é recebido o *acknowledge* da trama de envio do registo. Os parâmetros *START_REG_MEM* e *END_REG_MEM* definem o inicio e terminação do espaço de memória destinado ao registo de operação na WVM. Estes parâmetros definem o máximo número de registos permitidos (*MAX_NBR_REG*).

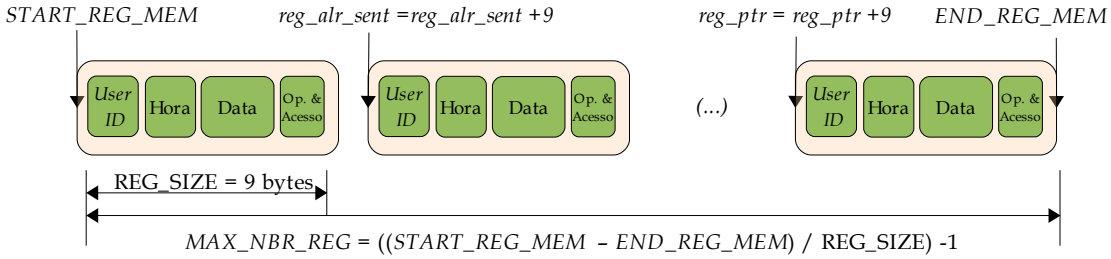

Figura 5.8: Processo de registo e actualizações para data sink de operações guardadas localmente.

5.4.3 Configuração

Durante a operação do sistema, existem sucessivas trocas de informação com o *data sink* de forma a executar configurações nas *WVMs.* Este processo é executado no estado de *Configuração*. O estado *Configuração* é desactivado quando a configuração é executada com sucesso. A alteração dos períodos de marcação por defeito e da tabela de permissões locais à *WVM* são duas das possíveis configurações deste estado.

Quando um comando de *Configuração* indica que o *data sink* pretende configurar o módulo de impressões digitais (*FPS: Fingerprint Sensor*) o estado de *Configuração FPS* é activado. Este estado é activado por um comando específico onde é incluído um *timeout TcfgFPS (Time to configure FPS*) durante o qual este estado permanece activo. Quando esse intervalo de tempo termina, o sistema transita para o estado *Configuração.* O estado *Configuração FPS* permite que o *data sink* comunique directamente com o *FPS* de forma a executar diversas operações, tais como registar novo utilizador, registar novo *template* para mesmo utilizador, apagar *template* de utilizador, apagar utilizador, verificar coerência das base de dados de *templates.*

Períodos de marcação por defeito

Os períodos de marcação por defeito permitem maior fluidez de utilização do sistema em períodos de elevada entrada ou saída de funcionários. Com os períodos de marcação por defeito pode definir-se um tipo de operação, *Entrada* ou *Saída,* para um período de tempo.

A Figura 5.9 ilustra o mapeamento da memória não volátil (*EEPROM)* para armazenamento dos períodos de marcação por defeito. Cada período de marcação por defeito usa 5 bytes (Hora de Inicio (2 bytes), Hora de terminação (2 bytes) e operação (1 byte)).

Para aceder aos registos são usados índices de selecção do espaço de memória para cada registo. Para alterar, apagar ou inserir um período de marcação por defeito é necessário o envio de um comando pelo *data sink,* em que num dos campos, é definido o índice de memória onde se pretende efectuar a operação em memória não volátil.

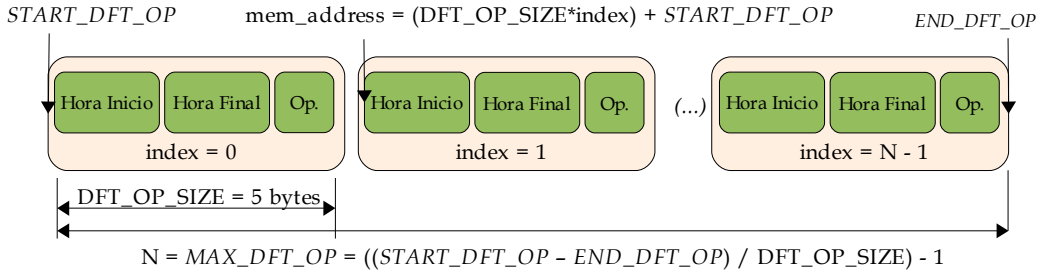

Figura 5.9: Mapeamento de memória não volátil para registo de períodos de marcação por defeito.

Permissões locais

Para que em modo *stand-alone* (*MRD)* o controlo de acesso permaneça em operação, os identificadores (*User ID)* dos funcionários com permissões de acesso são armazenados localmente. Os *User IDs* são registados em memória não volátil e acedidos através de índices. A abordagem de mapeamento da memória é semelhante ao método utilizado para os períodos de marcação por defeito, com a diferença de o número de bytes de um registo ser 2 (*User ID*). Para se alterar, registar ou apagar uma permissão de um funcionário é necessário envio de um comando pelo *data sink.*

5.5 . Comunicações sem fios

A tecnologia *ZigBee* implementa as comunicações sem fios para a troca de dados entre as estações remotas e o *data sink*. A referida tecnologia possui mecanismos de garantia de entrega de dados, baixa complexidade da pilha protocolar, baixo custo e consumo energético, preenchendo por isso os requisitos do sistema *wireless Temp I/O*.

O planeamento de rede do sistema de comunicações é baseado na topologia *mesh.* Esta topologia permite a extensão da dimensão da rede através da adição de *Routers*. A topologia *mesh* possui mecanismos de *self-routing* e *self-healing* que possibilitam multicaminho no encaminhamento dos pacotes em caso de falha de um dos módulos de transmissão (Figura 5.10). Caso a comunicação directa entre o *data sink* e uma *WVM* não seja possível, são usados *routers* para o encaminhamento de dados entre os dois pontos de comunicação. O planeamento da rede sem fios deve considerar pelo menos um caminho alternativo entre cada *WVM* e o *data sink.* Devem ser considerados os alcances máximos de cada módulo *wireless* e a distância física entre cada um dos módulos.

Os dispositivos *ZigBee* que integram a aplicação operam em modo *non-beacon*. No *modo non beacon,* os diversos módulos podem iniciar a comunicação de uma trama sempre que entendam sendo o acesso ao meio efectuado através de mecanismo *CSMA/CA*.

Os módulos *ZigBee* das estações remotas operam como *Routers,* permitindo o encaminhamento de dados das restantes estações da rede *ZigBee.*

As diferentes tramas da aplicação são endereçadas sob duas formas distintas: *broadcast* ou *unicast.* As tramas geradas pelas *WVMs* usam endereçamento *unicast*. O *data sink* utiliza endereçamento *unicast* para as configurações com requisitos de fiabilidade, tais como a configuração da base de dados de *templates*, alteração do identificador único da estação, edição das permissões locais de acesso ou escrita de mensagens no *LCD*.

As configurações de menor nível de relevância são endereçadas através de abordagem *broadcast* (exemplo: sincronizar data/hora). As tramas de endereçamento *broadcast* não geram *acknowledges* nas *WVMs* evitando a ocorrência de colisões no meio [1].

Além da utilização da tecnologia *ZigBee* para a troca de dados entre dispositivos do sistema, foi desenvolvido um protocolo que define a estrutura das tramas usadas pela aplicação. O referido protocolo opera acima da camada Aplicação definida pela tecnologia *ZigBee.*

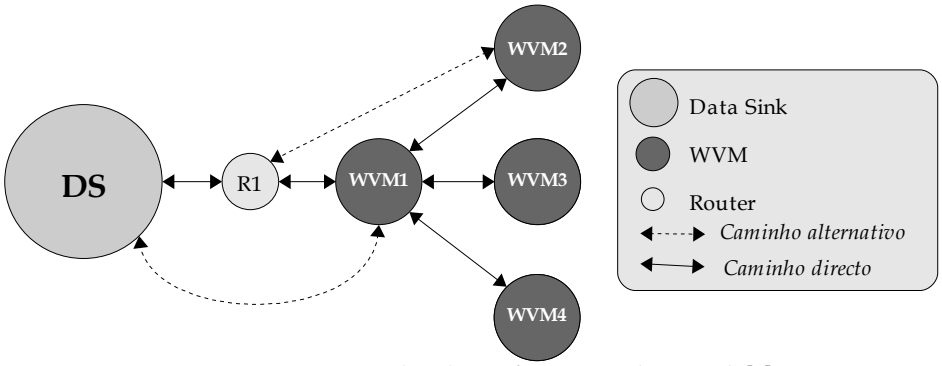

Figura 5.10: Diagrama de rede sem fios com topologia mesh [1].

O *data sink* comunica com dois distintos módulos internos às estações remotas, o *MCU* e o *FPS*. Por defeito, todas as mensagens são processadas pelo *MCU* e possuem a estrutura da aplicação *wireless Temp I/O*. Para que o *data sink* comunique com o *FPS* este deve enviar previamente uma mensagem de estrutura *wireless Temp I/O* para que as comunicações série sejam direccionadas para este dispositivo. A referida trama é designada por *COM2FPS Request*. O *data sink* fica então a comunicar virtualmente com o *FPS*, pelo que deve usar a estrutura de mensagem do módulo comercial *Suprema*, o *Unifinger SFM Packet Protocol* apresentado no capítulo 3.

A Figura 5.11 ilustra o processo de comunicação entre os diversos componentes do sistema.

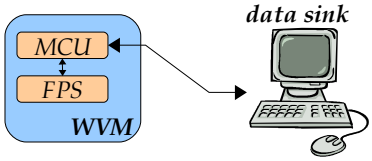

Figura 5.11: Diagrama das comunicações entre o data sink e uma WVM.

5.5.1 Protocolo wireless Temp I/O

O protocolo *wireless Temp I/O* define uma estrutura de tramas que permite a troca de dados na aplicação. As tramas desta estrutura são codificadas em *ASCII* e possuem tamanho variável (de 9 a 50 bytes). A cada trama transmitida é gerada no receptor uma trama de *acknowledge*, de forma a sinalizar a recepção da mensagem. A Figura 5.12 ilustra a estrutura base das mensagens do protocolo *wireless Temp I/O*.

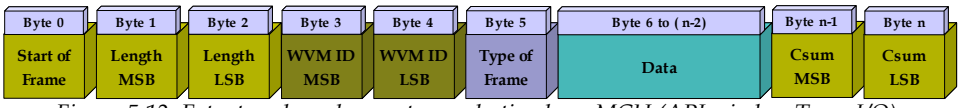

Figura 5.12: Estrutura base de uma trama destinada ao MCU (API wireless Temp I/O).

O campo *Start of Frame* (*SOF*) define a chegada de uma nova trama. Este caracter é exclusivo a esta função, caso seja usado noutro campo gera o inicio de leitura de uma nova trama descartando a anterior. O *SOF* é preenchido com o caracter *ASCII* '#'.

O campo *Length* determina o restante tamanho da mensagem e possui tamanho fixo de 2 bytes. Este campo deriva do tamanho dos campos *WVM ID*, *Type of Frame* e *Data*.

Cada *WVM* possui um identificador (*WVM ID*) único na rede de módulos de validação sem fios. As tramas *wireless Temp I/O* possuem sempre no campo *WVM ID* o identificador do *WVM*, quer este seja o emissor ou o *data sink*. Caso o *data sink* pretenda enviar uma trama para todos os *WVMs* de sistema, este usa o endereço de *broadcast* (*'0'*, *'0'*).

O campo *Data* possui os dados que se pretendem transmitir, dependendo a sua estrutura de cada tipo de trama definido no campo *Type of frame*. Na Tabela 5.3 são resumidas as tramas do sistema *Wireless Temp I/O*.

Tabela 5.3: Tipos de tramas possíveis do protocolo de comunicações wireless Temp I/O.

Nome	***Descrição***
Do data sink para o WVM (Download)	
Update Lcd	Introduz uma *string* de tamanho variável no *LCD*. Pode funcionar como confirmação de registo e alteração de nome lógico da interface.
Update Date	Actualização da Data (Dia, Mês e Ano).
Update Hour	Actualização da Hora (Hora, Minutos e Segundos).
Assert Output Pins	Actualização do estado dos pinos digitais de saída
Status Input Pins Request	Pedido de envio do estado dos pinos digitais de entrada
Change WVM ID	Alteração do identificador (WVM ID) de uma estação remota.
Erase EEPROM	Permite apagar todos os registos da *EEPROM*, registos de operações, período de marcação por defeito, permissões de utilizador.
Setup Local Permissions	Adiciona, apaga ou edita uma permissão de acesso de um utilizador.
Setup Default Operation	Adiciona, apaga ou edita um período de marcação por defeito.
COM2FPS Request	Direcciona as comunicações do *WCM* para o *FPS*.
Do WVM para o data sink (Upload)	
Status Input Pins Response	Responde à trama de *Status Input Pins Request* com o valor das saídas digitais no presente instante.
Upload reg NIM	Envia registo de operação em modo *MRN*.
Upload reg BIM	Envia registos de operações efectuados em modo *MRD*.
I am alive	Verifica conectividade com o *data sink*.

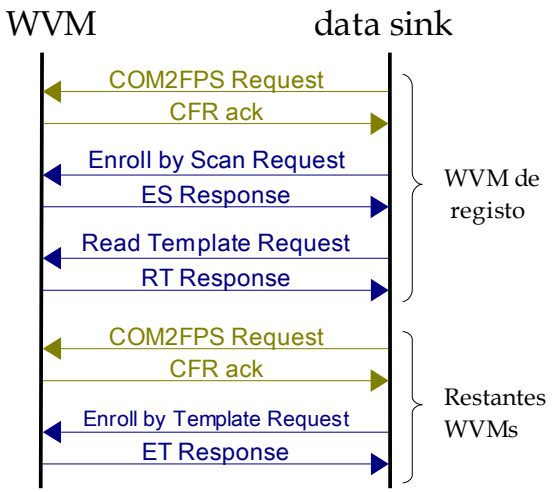

Figura 5.13: Fluxo de mensagens para processo de registo de novo utilizador.

O último campo de cada trama é um *checksum (Csum)*, que verifica a ocorrência de erros de

transmissão. Para calcular o valor a colocar neste campo, todos os valores dos campos *WVM ID, Type of frame e Data* devem ser somados. O resto da divisão hexadecimal da referida soma anterior por 0xFF é o valor a colocar nos campos *Csum* em codificação *ASCII.*

A trama de *acknowledge* possui o mesmo valor para *Type of Frame* que a mensagem recebida e o campo *Data* possui valor zero ('0').

A Figura 5.13 exemplifica um fluxo de mensagens que integram tramas do protocolo *Wireless Temp I/O* (verde) e do protocolo *Unifinger* (azul). O fluxo de mensagens refere-se ao processo de registo de um novo funcionário no sistema. Este processo divide-se em duas secções: registo do funcionário numa estação remota (*WVM de registo*) e partilha dos seus *templates* biométricos pelas restantes estações do sistema (*restantes WVMs*).

5.6 . Caracterização técnica

Na presente secção são identificadas as características técnicas dos módulos que integram a nova proposta para o sistema *Temp I/O*. O modo de operação e os parâmetros configurados nos módulos comerciais *XBee* e *Unifinger* utilizados na implementação do protótipo serão apresentados.

5.6.1 Data sink

O *gateway* associado ao sistema computacional permite a conectividade sem fios do *data sink* com os restantes módulos. O *gateway* é constituído por um módulo *XBee* e por um conversor *USB (Universal Serial Bus)* para *UART.*

O módulo *XBee,* descrito no Capítulo 4, efectua a conversão da tecnologia *ZigBee* para comunicação série (*UART*). De forma a garantir maior facilidade de conectividade, é usado um módulo de conversão do protocolo série (*UART)* para *USB.* Esta conversão é executada pelo circuito integrado da *FTDI, o FT232R.* Este circuito integrado possui a *stack USB* para operar com *device* do referido protocolo de comunicações série. A Figura 5.14 esquematiza as ligações internas ao módulo *data sink.* A Figura 5.15 ilustra o *hardware* adicional desenvolvido para o *gateway wireless*.

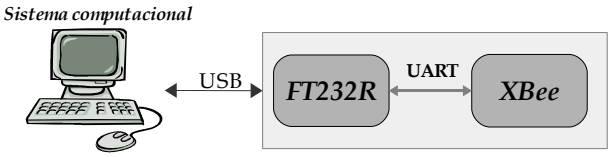

Figura 5.14: Módulos que compõem a interface com o data sink.

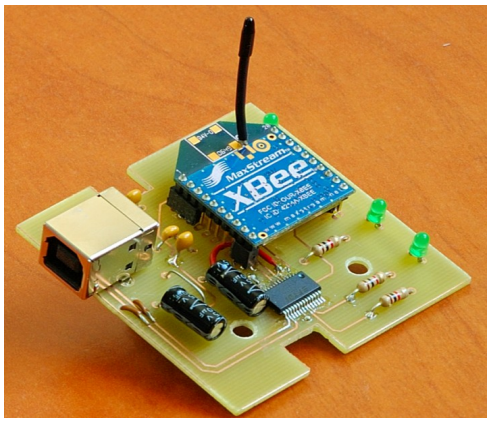

Figura 5.15: Protótipo do gateway

FT232R

O circuito integrado *FT232R* efectua a conversão do protocolo série (*UART)* para *USB*. Este dispositivo opera sem mais periféricos externos ao circuito integrado.

No *host USB* (PC) é instalado um *driver USB* para o circuito integrado da *FTDI*. A *FTDI* disponibiliza no seu portal *online* [56] diversos *drivers* para diferentes tipos de aplicação, sistemas operativos e arquitectura de processadores. De entre os tipos de *drivers* disponíveis, existem o *VCP* (*Virtual COM Port*) e os *D2XX* (*Direct Drivers*). O *VCP* cria uma porta série (*COM)* virtual no sistema operativo, pelo que as diversas aplicações consideram o periférico como uma porta COM vulgar. Este tipo de *driver* é preferencialmente usado em cenários de migração de uma aplicação com interface *COM* para um de interface *USB*, sem alterar a aplicação previamente desenvolvida. O driver *D2XX* permite a comunicação directa com o periférico sem qualquer emulação adicional.

XBee

O módulo *wireless XBee* é configurado no *data sink* como *Coordinator* da rede *ZigBee.* A escolha do módulo *ZigBee Coordinator* como o módulo presente no *data sink* prende-se com a centralização da aplicação numa módulo único e sempre presente no sistema, o *data sink.*

Os parâmetros *DH* (*Destination Address High*) e *DL* (*Destination Address Low*) são configurados pela aplicação no *data sink* sempre que esta pretende alterar o módulo destino da informação a enviar. A Tabela 5.4 descreve alguns dos parâmetros configurados no módulo *XBee* que opera como *Coordinator.*

Tabela 5.4: Configurações do módulo XBee para a interface do data sink [54].

Parâmetro	***Valor***	***Observações***
Versão firmware	*8017*	*ZigBee Coordinator (Modo transparente AT)*
ID (PAN ID)	*2233*	*Personal Area Network Identifier*
DH (Destination Address High)	*0x00*	*O conjunto dos registos DH e DL configurados como endereço de broadcast. São alterados sempre que se pretende comunicar com uma interface.*
DL (Destination Address Low)	*0xFFFF*	
NJ (Node Join Time)	*FF*	*Permite que outros dispositivos se associem a este em qualquer instante.*
PL (Power Level)	*4*	*Potência de transmissão RF, 0dBm.*
BD (Baud Rate)	*4*	*Taxa de transferência de dados pela UART (19200 bps).*
D7 (DIO7 Configuration)	*1*	*Activo CTS Flow Control*
D5 (DIO5 Configuration)	*1*	*Led de Associação activo.*

Software

O registo de operações em base de dados e a gestão das configurações nos módulos *WVM* são efectuadas a partir de uma aplicação no *data sink*. No âmbito desta dissertação foi desenvolvida uma aplicação de ensaio do sistema. A aplicação foi desenvolvida para sistema operativo *Windows* da *Microsoft,* usando os paradigmas da programação por objectos. Foram utilizadas as plataformas *C#* e *.Net Framework 2.0*.

O acesso ao módulo de comunicações sem fios é efectuado através de interface *USB* e *driver* específico (*VCP*) disponibilizado pelo fabricante *FTDI*.

O bloco *classe COM_Manager* efectua o acesso à porta de comunicação série e implementa a descodificação e construção de tramas com a estrutura do protocolo desenvolvido. Sempre que um conjunto de dados é recebido na porta série é gerado um evento que permite a descodificação da trama recebida.

A *Classe WTIO_API* utiliza os *buffers* e mecanismos da *classe COM_Manager* para construir o restante conteúdo das tramas do protocolo *Wireless Temp I/O*. As referidas tramas foram apresentadas na secção 5.5.1. A *Classe WTIO_API* utiliza a livraria (*DLL: Dynamic Link Library*) disponibilizada pelo fornecedor *Suprema Inc.* para efectuar configurações diversas no módulo de impressões digitais (Registar/Apagar funcionário, alterar dados biométricos de funcionário, parâmetros de operação, etc.).

Dependendo do tipo de configuração, a classe *WTIO_API* selecciona a estrutura de tramas a utilizar (protocolo *Wireless Temp I/O* ou o protocolo *Unifinger*)

A Figura 5.17 apresenta a arquitectura do *software* desenvolvido.

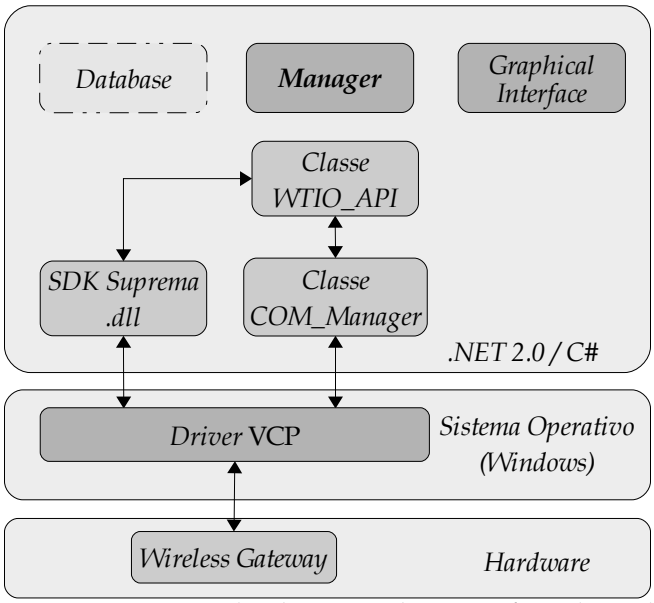

Figura 5.16: Diagrama da aplicação Wireless Temp I/O no data sink.

A classe *Manager* efectua a gestão dos blocos da aplicação, permitindo a interacção entre as restantes classes. Como exemplo, sempre que existe um registo numa estação remota, este é comunicado à classe *Main* através da classe *WTIO_API* e a informação de registo é enviada para a base de dados e para a interface gráfica.

A interface gráfica (*Graphical Interface*) permite a interacção da aplicação com um administrador de sistema. Nesta interface é possível aceder aos relatórios de tempos e editar os dados dos funcionários assim como efectuar configurações diversas. A Figura 5.17 apresenta a interface gráfica da aplicação de ensaio.

O bloco *Database* permite o armazenamento de informações dos funcionários (nome e dados biométricos), dos tempos de trabalho dos funcionários e das estações remotas. As bases de dados necessárias para o sistema não foram implementadas na aplicação de ensaio desenvolvida.

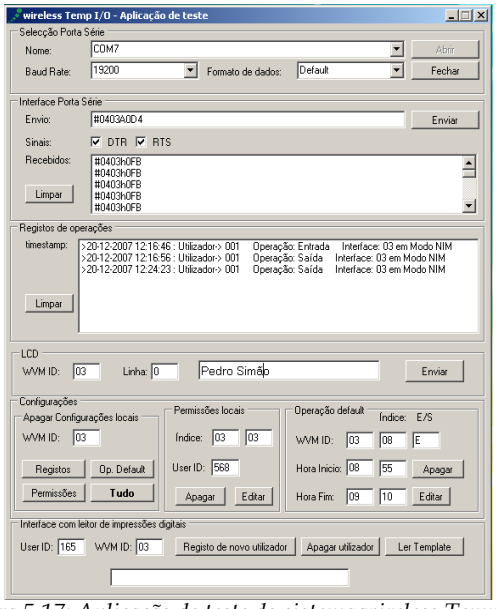

Figura 5.17: Aplicação de teste do sistema wireless Temp I/O.

5.6.2 Módulos locais WVM

O módulo de validação sem fios integra diversos sub módulos internos, *FPS, MCU, HMI* e o *WCM* (Figura 5.3). Todos os componentes referidos encontram-se dispostos numa única placa de circuito impresso. As unidades de processamento, *MCU, SFM3000 (*módulo de processamento do módulo *Unifinger)* e o *XBee* estão localizados na parte de trás da placa. Na parte frontal, ilustrada na Figura 5.18, apenas aparecem os elementos de interacção com o utilizador.

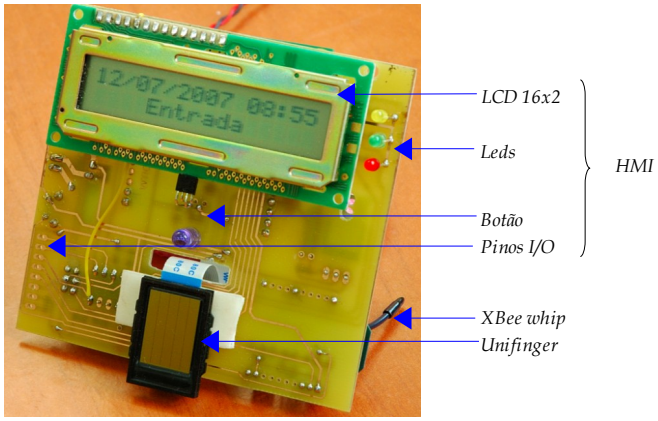

Figura 5.18: Protótipo do módulo WVM.

O módulo comercial que executa as funções de *FPS* é o *Unifinger* da *Suprema Inc*. Este módulo é composto por uma unidade de processamento que efectua a identificação (*SFM3000)* e um sensor de extracção da impressão digital, o *TouchChip* capacitivo de tipo 1 da *UPEK* [57].

O módulo *WCM* é também implementado usando um módulo comercial, o *XBee.* Este módulo opera no sistema em modo transparente e como *Router* de rede *ZigBee.* O *MCU* é também implementado por um dispositivo comercial, o *PIC18F* da *Microchip.*

O *LCD* usado no protótipo é o *LM052L*, um LCD monocromático e alfanumérico. Este *LCD* possui 16 colunas e 2 linhas e é baseada no circuito integrado *HD44780 da Hitachi* [58]. A interface com o *LCD* é executada através de interface paralelo de 4 linhas de dados e 3 de controlo.

XBee

A Tabela 5.5 descreve os parâmetros de configuração do módulo *XBee* que opera como *Router* na rede de módulos de validação *ZigBee*. Os campos *DH* e *DL* são preenchidos com o endereço *MAC* do módulo *Coordinator* da rede *ZigBee,* nesta aplicação, o *data sink*.

Tabela 5.5: Configurações do módulo XBee para a WVM [54].

Parâmetro	***Valor***	***Observações***
Versão firmware	*8217*	*ZigBee Router (Modo transparente AT)*
ID (PAN ID)	*2233*	*Personal Area Network Identifier*
DH (Destination Address High)	*0013A200*	*O conjunto dos registos DH e DL configurados para apenas comunicarem com o coordinator da rede.*
DL (Destination Address Low)	*40089E98*	
NJ (Node Join Time)	*FF*	*Permite que outros dispositivos se associem.*
PL (Power Level)	*4*	*Potência de transmissão RF, 0dBm.*
BD (Baud Rate)	*4*	*Taxa de transferência de dados pela UART (19200).*
RO (Packetization Timeout)	*3*	*Número de espaços de caracteres de silêncio na linha de Data in da UART até envio dos dados por RF.*
D5 (DIO5 Configuration)	*1*	*Led de Associação activo.*

SFM3050TC1

A unidade de processamento *SFM3000* possui diversos parâmetros que permitem a adaptação do seu modo de operação. No sistema em desenvolvimento pretende-se que o sistema funcione em *free scan* ou seja, sem que seja preciso o *host* enviar nenhum pedido de leitura ao sistema. A configuração do modo de comunicação em rede é outro dos importantes parâmetros configurados. A Tabela 5.6 descreve a lista de parâmetros do módulo *FPS*.

Tabela 5.6: Parâmetros configurados no módulo SFM3000 para operar nas WVM do wireless Temp I/O.

Parâmetro	***Valor***	***Observações***
Network Mode	Half Duplex	Estrutura de rede. Endereçamento no campo *Terminal ID*.
Security Level	Auto (1/10000)	
Fast Mode	Normal	
Free Scan	On	Não necessita de *polling* por parte do *host*.
Enroll Mode	2 Templates I	Registo de 2 templates por utilizador.
Template Size	384	Tamanho fixo de um *template,* em bytes.
Send scan success	On	Envia trama informativa acerca do utilizador identificado.
Timeout	10 sec	*Timeout* de operação (exemplo: registo de novo utilizador).
Matching Timeout	4 sec	Ignora processo de *matching* após duração máxima.
Auto Response	*Host*	Envia informação de eventos para o *host (MCU)*, através de comunicação série.

Ligações internas na WVM

O botão de selecção de operação na interface sem fios, possui a característica de ser activado sem

contacto ou seja, para o pressionar o utilizador não precisa de lhe tocar fisicamente. Este usa um *LED* de radiação infravermelha emissor e um receptor da mesma radiação para a detecção de movimento na sua frente, a presença de movimento significa que existe um utilizador que pretende accionar o botão.

O botão detecta a presença de uma mão a uma curta distância (5 cm). Este botão usa um circuito integrado da *Sharp* (*IS471F)* que efectua a detecção da luz infravermelha. Este coloca um LED emissor (*SFH486)* a conduzir e detecta a presença de obstáculos na sua proximidade.

Os diversos periféricos internos ao *WVM* estão conectados por diferentes interfaces ao *MCU*. Os módulos *XBee* e *Unifinger* são conectados à *USART* do *PIC18F (MCU)*. O pino *Sleep* do *XBee* é conectado ao *PIC* para que este possa entrar em modo de baixo consumo.

Software

A arquitectura do *software* do *MCU* é constituída por diferentes blocos que partilham os diversos recursos entre si. A partilha de recursos pode ser efectuada através da chamada de funções de blocos de menor nível de abstracção ao *hardware*, assim como o uso de memórias partilhadas. A Figura 5.19 define a arquitectura do *firmware* do *MCU* de cada estação remota.

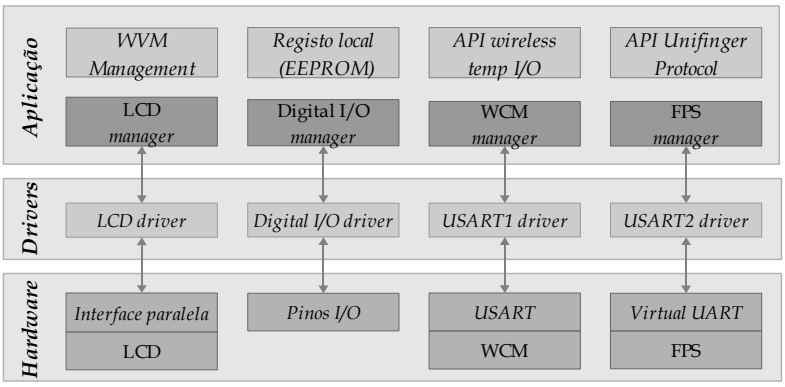

Figura 5.19: Arquitectura do software dos módulos WVM.

Os blocos do tipo *driver* definem o acesso ao *hardware*. Os blocos acima, *manager*, usam as funções do *driver* mas de forma abstracta ao tipo de ligação ou protocolo usado.

No bloco *Aplicação* são implementadas as diversas funcionalidades do sistema *wireless Temp I/O*. Os blocos *API (Application Programmable Interface)* permitem a transmissão e descodificação de tramas com os periféricos *FPS* e *data sink*. O bloco *Registo Local* permite registar dados nas bases de dados locais. O bloco *WVM Management* permite a execução de determinadas tarefas de gestão da estação remota, permitindo a gestão dos demais blocos consoante os eventos gerados pela interface do utilizador.

Capítulo 6

Ensaio e avaliação do desempenho

6.1 . Introdução

No presente capítulo apresentam-se os resultados dos ensaios realizados ao protótipo do sistema de controlo de assiduidade. Os ensaios preliminares referem-se aos módulos comerciais que operam no sistema: o módulo de impressões digitais (*Unifinger)* e módulo de comunicações *ZigBee (XBee)*. Nos ensaios seguintes verifica-se o desempenho do protótipo desenvolvido, quer em termos de tempo de execução de tarefas quer relacionado com as comunicações sem fios. Para as comunicações sem fios foram realizados ensaios em diferentes cenários da rede de comunicações sem fios.

6.2 . Módulo de impressões digitais

O processo de identificação por análise da impressão digital consiste nos processos de extracção da impressão digital, codificação da informação digitalmente e determinação (*matching*) do utilizador com os registos armazenados em memória.

Ao módulo em avaliação (*Unifinger SFM3050*) foi determinado o tempo de *matching* de utilizadores em diferentes condições de operação. Os resultados são apresentados na Tabela 6.1.

Tabela 6.1: Tempos de matching medidos no leitor Unifinger SFM3000.

		2 templates (1 utilizador)			***80 templates (40 utilizadores)***		
		Médio	***Desvio padrão***	***#amostras***	***Médio***	***Desvio padrão***	***#amostras***
Normal	Dedo conhecido	**586 ms**	13,29	10	**589 ms**	32,98	10
	Dedo desconhecido	**593 ms**	14,45	10	**791 ms**	19,50	10
Fast 5	Dedo conhecido	**590 ms**	11,75	10	**590 ms**	10,16	10
	Dedo desconhecido	**595 ms**	13,57	10	**689 ms**	25,16	10

Tal como apresentado na tabela, os tempos de *matching* foram determinados para uma base de dados para 80 e 2 *templates* e para um dedo conhecido e desconhecido. Foi também avaliado o modo de identificação *Fast*.

Da análise dos resultados verifica-se que, para um maior número de utilizadores registados, o modo *Fast* permite maior rapidez de *matching* caso se tente uma verificação de um utilizador não registado. Para um utilizador conhecido verifica-se que os dois modos (*Normal* e *Fast*) se comportam de forma semelhante.

6.3 . Ensaio dos módulos de comunicação wireless

O ensaio dos módulos *XBee* consistiu na verificação das características *ZigBee* implementadas nos módulos *XBee*. Após a construção de uma rede *ZigBee* e verificação dos mecanismos de *routing* e *self-healing*, foram medidas as intensidades de sinal recebido em ambientes *indoor* ou *outdoor*. Os testes de alcance foram executados de forma a determinar o alcance máximo dos módulos *ZigBee* da *MaxStream* sem a diminuição da qualidade de serviço.

A realização dos testes *indoor* considera as perdas de sinal provocadas pelos diversos obstáculos presentes num ambiente deste tipo, tais como paredes de cimento, ocas, armários e obstáculos móveis. Os testes *outdoor* tiveram a finalidade de avaliar o desempenho dos módulos *XBee* em ambientes sem obstáculos.

Para além dos testes de alcance, foram determinados os tempos de latência dos módulos *XBee.*

6.3.1 Indoor

Para o teste de alcance *indoor* foi extraído o valor de *RSSI* (*Received Strength Signal Indication*) de dois módulos em comunicação através do *software X-CTU* da *Maxstream*. O *software X-CTU,* através da opção *Range Test,* envia um conjunto de 32 bytes de dados endereçados ao módulo remoto. O módulo remoto possui uma ficha de *loopback* na comunicação série, permitindo que os dados recebidos no módulo remoto sejam reencaminhados para o módulo base. Ao receber os dados, o *X-CTU* verifica se estes coincidem com os dados previamente enviados e calcula o valor de RSSI correspondente. A Figura 6.1 ilustra a localização dos módulos remotos para as diferentes posições de medição realizadas. O módulo base foi colocado na posição POS 0 durante todos os ensaios.

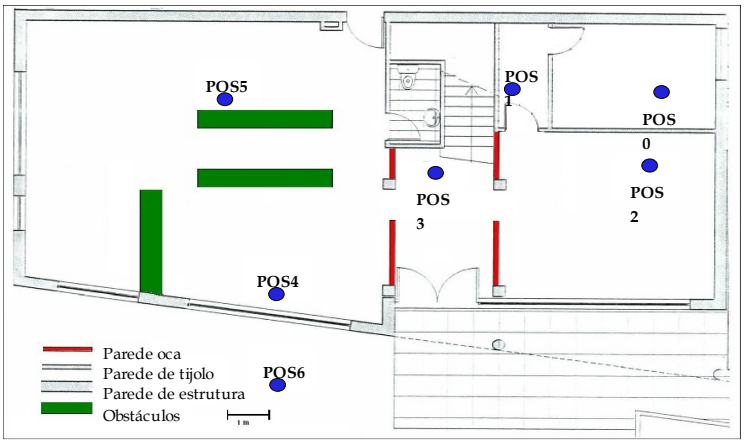

Figura 6.1: Localização geográfica dos módulos XBee para o teste Indoor.

Os resultados de força de sinal recebido para as diversas posições consideradas na Figura 6.1 e para os diferentes módulos *XBee* usados, encontram-se na Tabela 6.2.

De acordo com as especificações técnicas dos módulos *XBee* e *XBee-PRO [54]*, este possuem valores de sensibilidade de recepção de -92 dBm e -100 dBm respectivamente. Nas medições

executadas, verifica-se a concordância com os valores de sensibilidade de recepção referenciados, a partir dos quais se verifica a diminuição da qualidade de serviço.

Tabela 6.2: Força de sinal recebido para diferentes módulos e distâncias em ambiente Indoor.
** Cerca de 50 % de sucesso na entrega de dados **Cerca de 80 % de sucesso na entrega de dados*

Módulo	Antena	Força de sinal recebido (dBm)						
		POS1	POS2	POS3	POS4	POS5	POS6	2º Andar
XBee	chip	-73	-79	-86	-101**	-105**	-96	-98*
	whip	-53	-61	-79	-98**	-93**	-85	-95**
	RF connector	-55	-60	-79	-88	-96	-86	-98**
XBee-PRO	whip	-40	-40	-61	-69	-73	-63	-75

Da análise da Tabela 6.2, podemos concluir que uma simples parede oca introduz perdas de força de sinal recebido significativas. Por exemplo, os caminhos entre a posição *POS 0* e *POS 2* e o caminho entre *POS 0* e *POS 3*, apenas diferem por o segundo ter uma parede oca no caminho directo. Para os módulos *XBee,* com antena *whip* e *RF connector*, obtiveram-se diferenças de força de sinal de cerca de 19 dBm.

Para a posição em que o módulo foi colocado no segundo andar do edifico, apenas o módulo *XBee-PRO* conseguiu efectuar a conectividade com sucesso.

Como seria espectável, o módulo *XBee-PRO* apresenta maior desempenho, pois possui uma potência de transmissão de 18 dBm enquanto o módulo *XBee* transmite a 0 dBm.

6.3.2 Outdoor

Os testes realizados em ambiente *outdoor,* tiveram como principal motivação a avaliação das distâncias a que os módulos *XBee* conseguem transmitir na ausência de obstáculos.

Os factores que afectam o desempenho do valor de RSSI para este tipo de ambiente são a orientação da antena, período do dia, humidade, temperatura e distância [59]. Para os referidos testes pretende-se apenas avaliar a dependência da distância entre o emissor e o receptor no valor de *RSSI* obtido. Assim, os restantes factores foram considerados constantes. A temperatura na altura das medições era de 22ºC, a humidade do ar de 87% e a pressão de 120 kPa [62].

A realização do teste *outdoor* seguiram a mesma montagem de *hardware* que o teste *indoor,* com a diferença de que o valor de *RSSI* foi extraído usando um analisador de redes *ZigBee,* o *ZENA Analyzer* da *Microchip.*

A Tabela 6.3 possui a média de valor de *RSSI* para os 40 pacotes recebidos em cada medição. Foram consideradas medições entre 0 e 60 metros intercaladas de 5 metros para os dois tipos de módulos *ZigBee* da *Maxstream,* o *XBee* e o *XBee-PRO.*

Tabela 6.3: Valores de RSSI para diferentes distâncias no teste Outdoor.

Distância (m)	***0***	***5***	***10***	***15***	***20***	***25***	***30***	***35***	***40***	***45***	***50***	***55***	***60***
XBee whip	10,10	-24,61	-20,00	-38,49	-30,73	-31,24	-34,90	-41,56	-40,24	-42,51	-39,44	-44,02	-42,95
XBeePRO RF	21,61	-3,88	-5,61	-16,2	-16,44	-15,32	-20,20	-15,15	-15,37	-19,20	-17,76	-23,54	-33,83

Para os módulos *XBee* verifica-se que, para distâncias superiores a 30 metros, a qualidade de ligação é fraca. Dos valores obtidos verifica-se que os módulos *XBee-PRO* possuem desempenho constante, em termos de alcance *outdoor,* até aos 50 metros. A partir deste valor, nota-se um decréscimo na força de sinal recebido mas sem a detecção de perda de pacotes.

6.3.3 Medição da latência

A latência dos módulos *XBee* determina o tempo de comunicação entre os módulos. A latência dos módulos *XBee* inclui o tempo de comunicação série com o *host,* a latência *ZigBee* e os tempos de processamento dos dispositivos integrantes na rede.

A latência dos módulos *XBee* varia com o *baudrate* seleccionado para a comunicação com um *host.* A Tabela 6.4 apresenta os tempo de latência médios dos módulos *XBee* quando enviada uma trama por *unicast* com 21 bytes (*TXbytes*) nos dois sentidos da comunicação. A Figura 5.2 apresenta a fórmula de cálculo do tempo de comunicação para diferentes *baudrates*. O *NCOMbits* indica o número de bits da comunicação série utilizada (*10 = 1 Start bit + 1 Stop bit + 8 Data bits*).

Tabela 6.4: Latência obtida em função do baud rate para comunicação unicast.

Baud rate (b/s)	***9600***	***19200***	***57600***	***115200***
Latência XBee para dois saltos (ms)	61,20	34,60	17,60	13,60
Tempo de comunicação (ms)	43,75	21,88	7,29	3,65
Latência ZigBee para 2 saltos (ms)	17,45	12,72	10,31	9,95

$$Com_{time}(s) = \frac{(TXbytes)}{(baudrate / NCOMbits)}$$

Figura 6.2: Cálculo do tempo de comunicação.

A latência *ZigBee* é determinada pela subtracção da latência dos módulos *XBee* pelo tempo de comunicação para cada *baudrate*. Os tempos de processamento são desprezáveis.

Com o aumento do *baudrate* verifica-se uma diminuição da latência *ZigBee*. Este facto deve-se ao tempo que cada módulo aguarda por dados na porta série até enviar um pacote *ZigBee*. Para um menor *baudrate*, existe um maior número de tramas *ZigBee* enviadas com menos carga em cada trama.

Para *baudrate* de *19200 bps,* foi determinada a latência dos módulos *XBee* para diversos saltos na rede para transmissão de um byte nos dois sentidos de comunicação. Os resultados do referido ensaio são apresentados, em valores médios, na Tabela 6.5.

Tabela 6.5: Latência XBee para diversos saltos.

Latência XBee	***Baud rate***	***19200 bits/s***
	2 saltos	39,04 ms
	4 saltos	56,20 ms
	6 saltos	72,80 ms

6.4 . *Overhead* computacional dos módulos WVM

O tempo de execução de diversas tarefas nas interfaces *WVM* assim como as taxas de utilização do *MCU* com o aumento de tráfego na rede foram determinados. A taxa de utilização do MCU refere-se à percentagem de processamento disponibilizada pelo controlador para executar os comandos recebidos do *data sink*.

A taxa de utilização de *MCU* pretende verificar de que modo o aumento de tráfego na rede influencia a taxa de utilização deste controlador. A execução desta medição pressupõe a medição de um valor referencial de utilização do *MCU* sem tráfego na rede. Para medição do valor referencial mediu-se o incremento de uma variável em *background.* A referida variável foi colocada a

incrementar durante 20 segundos. Para diferentes taxas de envio de mensagens foi medida a taxa de utilização do *MCU* da mesma forma que o valor referencial.

A Tabela 6.6 apresenta os resultados do referido ensaio.

Tabela 6.6: Resultados da taxa de utilização do processador.

Referência de incremento: 6415		***Com endereço da WVM ID***		***Com endereço diferente do WVM ID.***	
		%	***incremento***	***%***	***incremento***
Taxa	***100 ms***	*5,39 %*	*6069*	*0,02 %*	*6414*
	10 ms	*41,7 %*	*3740*	*0,03 %*	*6413*
	5 ms	*41,98 %*	*3722*	*0,03 %*	*6413*

Da análise da Tabela 6.6 conclui-se que o aumento de tráfego de tramas não destinadas ao *WVM* introduz um aumento na taxa de utilização desprezável, verificando-se que o *MCU* suporta uma abordagem *broadcast*. A mensagem é descartada assim que é verificado o endereço de destino da mensagem recebida. Quando a mensagem é destinada ao *WVM*, a taxa de utilização do processador depende do comando enviado. Neste caso foi enviada a trama de confirmação de uma operação.

As restantes taxas de utilização das restantes tarefas são apresentadas na Tabela 6.7. Para além das taxas de utilização, a tabela apresenta também os tempos de execução das diferentes tarefas. Para as tarefas da referida tabela foi usada uma taxa de amostragem de 100 ms.

Tabela 6.7: Tempo de execução e taxa de utilização das diferentes tarefas para baudrate de 19200 bps.

Tarefa	***Tempo de execução***		***Tempo de comunicação***		***Taxa de utilização (Periodicidade de 100 ms)***
			Comando	***Acknowledge***	
Update LCD (Máx: 26 bytes)	OP = 0	13,20 ms	13,54 ms	4,70 ms	4,75 %
	OP = 1/2	17,40 ms			5,64 %
	OP = 3	18,02 ms			4,29 %
Update Date (19 bytes)	26,20 ms		9,90 ms	4,70 ms	14,19 %
Update Hour	16,80 ms		7,29 ms	4,70 ms	9,13 %
Assert Output Pins (11 bytes)	19,20 ms		5,73 ms	4,70 ms	4,29 %
Status Input Pins Request (9 bytes)	8,80 ms		4,70 ms	4,70 ms	5,18 %
Change WVM ID (10 bytes)	12,10 ms		5,21 ms	4,70 ms	6,69 %
Erase EEPROM (9 bytes)	*Tudo*	118 ms	4,70 ms	4,70 ms	78,10 %
	Permissões	80 ms			68,93 %
	Registos	19,40 ms			14,15 %
	Períodos	36 ms			29,17 %
Setup Local Permissions (14 bytes)	*OP = 0*	12, 40 ms	7,29 ms	4,70 ms	6,69 %
	OP = 1	19,60 ms			11,71 %
Setup Default Operation (19 bytes)	*OP = 0*	12,50 ms	9,90 ms	4,70 ms	6,69 %
	OP = 1	27,80 ms			16,77 %
COM2FPS Request (11 bytes)	-		5,73 ms	4,70	-

Os tempos de execução apresentados na Tabela 6.7 são relativos ao pior cenário de utilização de cada tarefa. O pior cenário é definido pelas instruções pedidas por cada comando que introduzem

um maior tempo de processamento. Para cada opção de execução dos comandos foram medidos os tempos de execução e apenas são apresentados os que apresentam maior tempo de processamento. O tempo de execução das diferentes tarefas é determinado pelo tempo de envio da mensagem de comando, execução da tarefa e posterior tempo de envio de mensagem de *acknowledge* em sentido contrário. O tempo de execução inclui o tempo de comunicação. O tempo de comunicação é determinado através da expressão da Figura 6.2.

6.5 . Ensaio do sistema com ligação ponto-a-ponto

O ensaio realizado com comunicação ponto-a-ponto permite determinar a taxa de sucesso nas comunicações sem fios no sistema *wireless Temp I/O*. O ensaio refere-se à comunicação com apenas uma interface *WVM*. Considera-se uma rede ponto-a-ponto uma ligação entre dois dispositivos (*data sink* e terminal *WVM)* com endereçamento *unicast*. O presente ensaio utiliza a aplicação de ensaio, introduzida no capítulo 5, para gestão das tramas no *data sink*.

O ensaio consiste na determinação da taxa de sucesso de registo de uma operação. O referido processo consiste no envio de uma trama da *WVM* para o *data sink*, e respectivo *acknowledge* em sentido contrário. Para além destas tramas é emitido uma confirmação de registo da operação para o terminal, que consiste na escrita do nome do funcionário no LCD das estações remotas. Este processo é executado com periodicidade de 2 segundos.

Para a totalidade das tramas transmitidas neste ensaio obteve-se uma confirmação de recepção das tramas, assim podemos concluir que com ligação ponto-a-ponto *ZigBee*, a taxa de sucesso foi de 100%.

6.6 . Ensaio do sistema com ligação ponto-multiponto

No presente ensaio é usada uma abordagem ponto-multiponto em que o *data sink* comunica com vários terminais remotos. Os terminais apenas comunicam com o *data sink*, daí se designar uma rede ponto-multiponto. A rede ponto-multiponto é suportada pela tecnologia *ZigBee*. Como os terminais geram tramas por eventos do utilizador, o *data sink* não consegue gerir a carga na rede sem fios de forma a diminuir o número de colisões na rede. Este ensaio permite avaliar a capacidade da rede *ZigBee* para gerir as colisões na rede através dos mecanismo de *CSMA/CA*.

Os módulos *ZigBee* utilizados agrupam os conjuntos de dados emitidos sequencialmente, permitindo a construção de uma rede ponto-multiponto sem destruição da integridade das tramas emitidas por diferentes terminais. A Figura 6.3 ilustra este processo. Durante a emissão de uma trama do módulo *ZED A* o terminal *ZED B* emite outra trama sem que o *ZED A* tenha terminado o envio da primeira. No módulo central (ZC Out), as duas tramas são recebidas tal como foram emitidas por cada dispositivo.

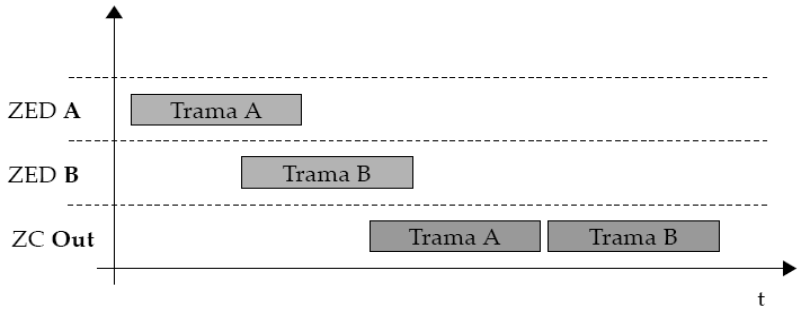

Figura 6.3: Processo de agrupamento de tramas ZigBee.

As comunicações entre os diferentes módulos usam endereçamento *unicast*. Para envio de tramas *unicast*, os módulos *XBee* necessitam da alteração do endereço de 64-bit do módulo *XBee* associado a

cada módulo WVM. A aplicação no *data sink* utiliza os comandos *AT* para alteração do endereço de destino da trama.

Tal como para o ensaio ponto-a-ponto, foram utilizados diversos cenários de rede com diferentes saltos na rede ZigBee. Sempre que se introduz um novo salto na rede de comunicações sem fios existe a adição de um *router ZigBee* na rede.

A Figura 6.4 apresenta a estrutura da rede sem fios para o ensaio de três saltos.

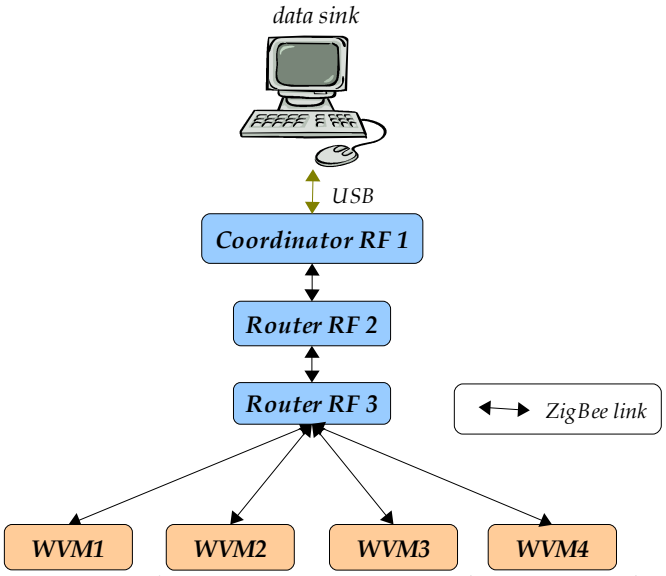

Figura 6.4: Rede ZigBee ipara ensaio ponto-multiponto com 3 saltos.

Neste ensaio foram determinadas as taxas de sucesso de identificações de quatro módulos *WVM*. Em cada um dos módulos simulou-se a execução de 300 pedidos de registo de operação com periodicidade de 5 segundos. Cada registo de operação contém a troca dos mesmos comandos que os apresentados para o ensaio ponto-a-ponto. Sempre que, após um timeout, uma trama de confirmação do envio de outra não é recebida, os dados eram reenviados. Este processo de reenvio de dados é independente da pilha protocolar ZigBee e são uma implementação acima da camada aplicação. A Tabela 6.8 apresenta os resultados obtidos neste ensaio.

Tabela 6.8: Taxa de identificações com sucesso para periodicidade de 5 segundos.

Casos	***Pacotes Enviados (1x)***	***Pacotes Reenviados (2x)***	***Pacotes Reenviados (3x)***	***Pacotes Perdidos***	***Taxa de Sucesso***
1 Salto ZigBee	1200	2	1	1	99,92 %
2 Saltos ZigBee	1200	7	6	5	99,59 %
3 Saltos ZigBee	1200	46	9	7	99,42 %

A diminuição da taxa de sucesso em relação ao ensaio ponto-a-ponto deve-se ao facto do módulo XBee entrar em modo de comando para alteração dos endereços de destino. Durante este período de configuração o módulo não processa possíveis tramas recebidas pela interface sem fios. A alteração do endereço de destino dos dados no módulo *ZigBee Coordinator* introduz um atraso de 30 ms.

Capítulo 7

Conclusões e trabalhos futuros

Do estudo realizado no âmbito desta dissertação, conclui-se que a integração de tecnologias biométricas suportadas por comunicações sem fios de baixa taxa de transferência, permite desenvolver aplicações de elevada fiabilidade, desempenho e segurança.

A tecnologia biométrica emergiu nos últimos anos sendo agora integrada em diversos produtos comerciais permitindo fiabilidade na identificação de pessoas. A vulgarização das tecnologias sem fios determinou a redução de custos e complexidade como em protocolos como o *ZigBee*. Este tipo de protocolo permite o desenvolvimento de aplicações de custo reduzido e de desempenho semelhante às soluções cabladas.

O desenvolvimento de uma solução de controlo de assiduidade e controlo de acessos baseada nas duas referidas tecnologias garante fiabilidade na identificação, devido à dificuldade em ludibriar o mecanismo de identificação biométrica e garante também fiabilidade e segurança na comunicação devido aos mecanismos existentes nos protocolos de comunicações sem fios.

Os principais objectivos da dissertação consistiam em avaliar as tecnologias biométricas e de comunicações sem fios, propor uma arquitectura para um sistema de controlo de assiduidade com interface sem fios e implementar um protótipo do sistema. Por fim, era requierida a definição e realização de ensaios ao protótipo desenvolvido. Todos estes objectivos foram cumpridos no âmbito desta dissertação.

A arquitectura proposta permitiu o desenvolvimento de um sistema de elevado desempenho, quer em termos de rapidez na realização de um registo de ponto quer na fiabilidade da identificação dos funcionários.

Os ensaios apresentados no capítulo 6 comprovam a eficiência do módulo *Unifinger* de identificação por impressões digitais, sendo este rápido na identificação e facilmente adaptável a diferentes modos de operação. Os módulos de comunicações sem fios *ZigBee* (*XBee*) permitem a construção de uma rede *ZigBee* facilmente adaptável aos requisitos da aplicação. Os módulos *XBee-PRO* possuem maior potência de transmissão, o que lhes permite efectuar comunicações a maiores distâncias. Para ambiente *indoor,* verifica-se que a presença de obstáculos impõe diminuição

significativa do alcance máximo dos módulos.

Um sistema de controlo de assiduidade nem sempre é bem recebido pelos funcionários que o utilizam. Considerando este facto, o sistema propõe uma interface amigável permitindo que os funcionários interpretem o *Wireless Temp I/O* como uma ferramenta fiável de cálculo dos seus tempos de trabalho e que garante a segurança no seu espaço laboral e não como uma forma automática de os supervisionar.

Como trabalho futuro, existem diversos passos a serem realizados tendo em vista a comercialização da solução final, nomeadamente, aumentar o grau de integração dos circuitos de electrónica de forma a diminuir os custos de produção. O módulo de comunicações *ZigBee* é o exemplo disso mesmo. A integração do módulo *ZigBee* pode ser implementada através de um dos referidos transceptores apresentados no capítulo 4, em que a aplicação *Wireless Temp I/O* é integrada num microcontrolador juntamente com a pilha protocolar *ZigBee.*

A classe de comunicações desenvolvida nesta dissertação deve integrar a aplicação *BackOffice* do produto *Temp I/O*, de forma a avaliar o desempenho do sistema em condições reais. A base de dados de registos necessita de introdução de novos campos, tais como o identificador da estação de registo e informação acerca do acesso.

As entradas e saídas digitais devem possuir isolamento óptico de forma a isolar o circuito de baixa potência dos módulos mecânicos de abertura e fecho de acesso automático, de forma a proteger ambos os circuitos de eventuais erros de manuseamento.

De forma a aumentar a flexibilidade do sistem,a poderá ser desenvolvido um modo de baixo consumo de energia. Durante a operação neste modo, as estações remotas seriam alimentadas por baterias.

Bibliografia

[1] Simão P., Fonseca J.A, Santos V., "Time attendance system with multistation and wireless communications", ISCE 2008 - 12th Annual IEEE International Symposium on Consumer Electronics, Vilamoura – Portugal, Abril de 2008.

[2] Manual de Utilizador – *Temp I/O*, versão 1.1, *Micro I/O*, Novembro de 2006

[3] "Speaker recognition", National Science and Technology Council (NSTC), *Subcommittee on Biometrics, August 2006*

[4] Douglas A. Reynolds (M.I.T. Lincoln Laboratory) and Larry P. Heck (Nuance Communications), "Automatic Speaker Recognition: Recent Progress, Current Applications and Future Trends", AAAS 2000 Meetings: Humans, Computers and Speech Symposium, Fevereiro de 2000.

[5] Qinghan Xiao, "Biometrics – Technology, Application, Challenge, and Computational Intelligence Solutions", IEEE *Computational Intelligence Magazine, Maio 2007*

[6] International Biometric Group, http://www.biometricgroup.com/reports/public/market_report.html, Dezembro de 2007

[7] Bio ID, http://www.bioid.com/sdk/docs/About_EER.htm, Dezembro de 2007

[8] Peter Bishop, "Atmel's FingerChip™ Technology for Biometric Security", Atmel *Corporation, 2002*

[9] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, "Handbook of Fingerprint Recognition", *Springer, New York, 2003*

[10] "Fingerprint Recognition", National Science and Technology Council (NSTC), Subcommittee on Biometrics, August 2006

[11] Michael J. Riezenman, "Cellular Security: better, but foes still lurk", IEEE Spectrum, June 2000.

[12] MIT Media Lab: VisMod Group, *http://vismod.media.mit.edu/vismod/demos/facerec/basic.html*, *(Dezembro de 2007)*

[13] Face recognition, NIST (National Science and Technology Council), Subcommittee on Biometrics, August 2006

[14] Institut für Neuroinformatik, *http://www.neuroinformatik.ruhr-uni-bochum.de*, Dezembro de 2007

[15] John Makhoul and Richard Schwartz, State of the art in continuos speech recognition. BBN Systems and Technologies, Cambridge, MA 02138, 1995.

[16] "Iris recognition", NIST (National Science and Technology Council), Subcommittee on Biometrics, August 2006

[17] Harvey & Bernice Jones Eye Institute, *http://www.uams.edu/jei/patients/retina_services/maculardegen.asp*, Dezembro de 2007

[18] University of Cambridge, Computer Laboratory, *http://www.cl.cam.ac.uk/~jgd1000/iris_recognition.html*, Dezembro de 2007

[19] "Hand Geometry", NIST (National Science and Technology Council), Subcommittee on Biometrics, August 2006

[20] Michigan State University, *http://biometrics.cse.msu.edu/hand_proto.html, Dezembro de 2007*

[21] Nitgen, *http://www.nitgen.com/, Novembro de 2007*

[22] Suprema Inc., *http://www.supremainc.com, Dezembro de 2007*

[23] Specification for the Bluetooth System 1.1, Technical Report Specification Volume 1, Bluetooth Special Interest Group (SIG), 2001.

[24] IEEE Std 802.15.1 - IEEE Standard for Information technology – Telecommunications and information exchange between systems - Local and metropolitan area networks – Specific requirements Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). Technical report, IEEE Computer Society, 2002.

[25] J. Kardach. "Bluetooth Architecture Overview", Intel Technology Journal, 2000.

[26] Paulo Bartolomeu, "Evaluating Bluetooth® for the wireless transmission of MIDI", Universidade de Aveiro, Dissertação de Mestrado, 2005

[27] Vasco Santos, "Comunicações em Aplicações de Domótica para Apoio a Pessoas com Limitação Funcional", Universidade de Aveiro, Dissertação de Mestrado, 2007

[28] "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", Technical Report ISO/IEC 8802-11:1999(E), International Standard ISO/IEC, 1999.

[29] UltRa Lab, University of Southern California, 2006, *http://ultra.usc.edu/*, Dezembro de 2007

[30] M. P. Wylie-Green, P. A. Ranta, and J. Salokannel, "Multi-band OFDM UWB Solution for IEEE 802.15.3a WPANs. In Advances in Wired and Wireless Communication", IEEE/Sarnoff Symposium on, 2005.

[31] Nokia Reserach Center, *http://research.nokia.com/research/programs/uwb/index.html*, Dezembro 2007

[32] Evans-Pughe, C., "Bzzzz zzz [ZigBee wireless standard]", IEEE Review, March 2003

[33] "Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks", IEEE Communications Magazine p.70-77, August 2002, Ed Callaway, Paul Gorday, and Lance Hester, Motorola Laboratories, Jose A. Gutierrez and Marco Naeve, Eaton Corporation, Bob Heile, Appairent Technologies, Venkat Bahl, Philips Semiconductors

[34] Aliança ZigBee, *www.zigbee.org*, Dezembro de 2007

[35] "ZigBee Specification", Document 053474r13, ZigBee Alliance, Dezembro 2006

[36] IEEE 802.15.4 - 2003 Specification, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), October 2003

[37] Safaric, S, Malaric, K., "ZigBee wireless standard", p.259 to 261, 48th International Symposium ELMAR 2006, Zadar, Croatia, Junho 2006

[38] "ZigBee/IEEE 802.15.4 Summary", Sinem Coleri Ergen, September, 2004

[39] Forbes, H., "ZigBee in a Nutshell: Suited for Industrial Applications?", ARC Advisory Group, August 2005

[40] Oehen, P., "ZigBee: An Overview of the upcoming standard", Distribute Computing Seminar – ZigBee.

[41] Phil Jamieson, "ZigBee Application Profiles", ZigBee Open House, França, Maio de 2007

[42] Farnell, *http://pt.farnell.com*, Novembro de 2007

[43] Microchip, *www.microchip.com,* Dezembro de 2007

[44] Freescale, *www.freescale.com,* Dezembro de 2007

[45] Texas Instruments, *www.ti.com/zigbee,* Dezembro de 2007

[46] *IP-Link 122X - Embedded Wireless Module*, User Manual, Version 2.1.00, Junho de 2007

[47] *ZigBee IEEE 802.15.4 Radio transceptor – AT86RF230*, 5131C-ZIGB-05/22/07, Atmel, 2007

[48] Ubec, *www.ubec.com.tw,* Dezembro de 2007

[49] ZMD, *www.zdma.com*, Dezembro de 2007

[50] Helicomm, *www.helicomm.com*, Dezembro de 2007

[51] Ember, *www.ember.com/* , Dezembro de 2007

[52] Meshnetics, *www.meshnetics.com*, Dezembro de 2007

[53] Jennic, *www.jennic.com*, Dezembro de 2007)

[54] *XBee / XBee-PRO OEM RF Modules – Product Manual v8.x17 Beta – ZigBee Protocol* (2007)

[55] *UniFinger SFM Series, Packet Protocol Manual*, version 2.6, *Suprema Inc* 2006

[56] FTDI, *www.ftdichip.com,* Novembro de 2007

[57] UniFinger SFM3050-TC Datasheet, Version 1.0, Suprema, Dezembro 2004

[58] *HD44780U (LCD-II), "Dot Matrix Liquid Crystal Display Controller/Driver", Hitachi, Revision 0.0, 1998*

[59] *T*adakamadla, *Shashank,* Indoor Local Positioning System For ZigBee, Based On RSSI, The Department of Information Technology and Media (ITM), Mid Sweden University, 2006

[60] Liahren, *http://www.liahren.com/,* Dezembro de 2007

[61] Secugen, *http://www.secugen.com,* Dezembro de 2007

[62] Accuweather, *http://www.accuweather.com/*, Novembro de 2007