Universidade do Minho

Tópicos de Comunicações sem Fios

José Augusto Afonso

Guimarães, 11 de maio de 2016

Índice de Conteúdos

Lista de Abreviaturas

3GPP	3rd Generation Partnership Project
AAL	ATM Adaptation Layer
ABR	Available Bit Rate
AC	Access Category
ACL	Asynchronous Connection-Less
ADPCM	Adaptive Differential Pulse Code Modulation
AIFS	Arbitration InterFrame Space
AP	Access Point
API	Application Programming Interface
APS	Application Support Sublayer
ARQ	Automatic Repeat reQuest
ATM	Asynchronous Transfer Mode
BAN	Body Area Network
BER	Bit Error Rate
BRAN	Broadband Radio Access Networks
BS	Base Station
BSN	Body Sensor Network
BSS	Basic Service Set
BWA	Broadband Wireless Access
CBR	Constant Bit Rate

CC	Central Controller
CCA	Clear Channel Assessment
CCK	Complementary Code Keying
CDMA	Code Division Multiple Access
CDV	Cell Delay Variation
CDVT	Cell Delay Variation Tolerance
CEPT	European Conference of Postal and Telecommunications Administrations
CER	Cell Error Rate
CFB	Contention Free Burst
CFP	Contention Free Period
CLR	Cell Loss Ratio
CP	Contention Period
CMR	Cell Misinsertion Rate
CRA	Contention Resolution Algorithm
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CT	Cordless Telephony
CTD	Cell Transfer Delay
CTS	Clear To Send
CW	Contention Window
DCF	Distributed Coordination Function
DECT	Digital Enhanced Cordless Telecommunication
DFIR	Diffuse Infrared

DFS	Dynamic Frequency Selection
DIFS	DCF InterFrame Space
DLC	Data Link Control
DLP	Direct Link Protocol
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
DS-CDMA	Direct Sequence Code Division Multiple Access
EC	Error Control
EDCA	Enhanced Distributed Channel Access
EDCF	Enhanced Distributed Coordination Function
EDD	Earliest Due Date
EDF	Earliest Deadline First
eLPRT	Enhanced Low Power Real Time
ERC	European Radiocommunications Committee
ETSI	European Telecommunications Standards Institute
ESS	Extended Service Set
FCC	Federal Communications Commission
FCFS	First Come First Served
FCS	Frame Check Sequence
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FFD	Full Function Device
FFQ	Fluid Fair Queuing
FHSS	Frequency Hopping Spread Spectrum

FH-CDMA	Frequency Hopping Code Division Multiple Access
FIFO	First In First Out
FP	Fixed Part
FSK	Frequency Shift Keying
FWA	Fixed Wireless Access
GFSK	Gaussian Frequency Shift Keying
GMSK	Gaussian Minimum Shift Keying
GPS	Generalized Processor Sharing
GSM	Global System for Mobile Communications
GTS	Guaranteed Time Slot
HARQ	Hybrid ARQ
HC	Hybrid Coordinator
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HEC	Header Error Check
HIPERLAN	High Performance Radio Local Area Network
HTTP	Hypertext Transfer Protocol
IBSS	Independent BSS
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IrDA	Infrared Data Association
ISI	InterSymbol Interference
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization

ITU	International Telecommunications Union
LAN	Local Area Network
LEACH	Low-Energy Adaptive Clustering Hierarchy
LLC	Logical Link Control
LOS	Line Of Sight
LQI	Link Quality Indication
LR-WPAN	Low Rate Wireless Personal Area Network
MAC	Medium Access Control
MASCARA	Mobile Access Scheme based on Contention and Reservation for ATM
MBS	Maximum Burst Size
MCR	Minimum Cell Rate
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
MTE	Minimum Transmission Energy
NAV	Network Allocation Vector
nrt-VBR	Non-Real-Time Variable Bit Rate
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PAN	Personal Area Network
PCF	Point Coordination Function
PCR	Peak Cell Rate
PDU	Protocol Data Unit
PER	Packet Error Rate
PIFS	PCF InterFrame Space

PLCP	Physical Layer Convergence Procedure
PLR	Packet Loss Ratio
PMD	Physical Medium Dependent
PRMA	Packet Reservation Multiple Access
QAM	Quadrature Amplitude Modulation
QBSS	QoS Basic Service Set
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RF	Radiofrequência
RFD	Reduced Function Device
RTS	Request To Send
rt-VBR	Real-Time Variable Bit Rate
SCO	Synchronous Connection-Oriented
SCR	Sustained Cell Rate
SDMA	Space Division Multiple Access
SDU	Service Data Unit
SIFS	Short InterFrame Space
SMTP	Simple Mail Transfer Protocol
STA	Station
TBTT	Target Beacon Transmission Time
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TG	Task Group
TIM	Traffic Indication Map

TPC	Transmission Power Control
TSPEC	Traffic Specification
TXOP	Transmission Opportunity
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
U-NII	Unlicensed National Information Infrastructure
VBR	Variable Bit Rate
WATM	Wireless ATM
WEP	Wired Equivalent Privacy
WFQ	Weighted Fair Queueing
WLAN	Wireless Local Area Network
WLL	Wireless Local Loop
WPAN	Wireless Personal Area Network
WRR	Weighted Round-Robin
WSN	Wireless Sensor Network
ZC	ZigBee Coordinator
ZDO	ZigBee Device Object
ZED	ZigBee End Device
ZR	ZigBee Router

1. Introdução

Este capítulo começa por apresentar uma revisão de conceitos associados às redes de comunicação que são relevantes para a aprendizagem nesta unidade curricular.

1.1 Revisão de redes de comunicação

Devido à multidisciplinaridade e complexidade associada à tarefa de implementar o conjunto completo de funcionalidades oferecidas por uma rede de comunicação, essas funcionalidades são tipicamente repartidas em várias camadas mais simples, ficando assim cada camada responsável pela implementação de um subconjunto particular das funcionalidades da rede.

As camadas são modulares e hierárquicas, como mostra a Figura 1.1. Em termos lógicos, cada camada comunica horizontalmente com a respetiva camada de outra máquina (também chamada, dependendo do contexto, de estação, nó, equipamento ou dispositivo) utilizando um protocolo específico da camada. Em termos reais, as camadas na mesma máquina comunicam com as camadas adjacentes na vertical. Como mostra a Figura 1.2, a camada superior (k+1) utiliza os serviços oferecidos pela camada inferior (k), por intermédio da API (*Application Programming Interface*) desta. A modularidade e independência entre camadas têm a vantagem de tornar possível substituir uma implementação de uma camada por outra implementação, porventura mais eficiente.

Os dados que uma camada recebe da camada imediatamente superior para serem transportados para outra máquina, no emissor, recebem o nome de *payload* ou SDU (*Service Data Unit*) da camada. A esses dados, a camada anexa o respetivo cabeçalho, ou *header* (H), no início. No caso da camada 2, também é anexada uma cauda, ou *trailer* (T), no fim. O pacote assim formado recebe a denominação técnica de PDU (*Protocol Data Unit*) da camada. Esse

processo é denominado encapsulamento. No recetor efetua-se o processo inverso.

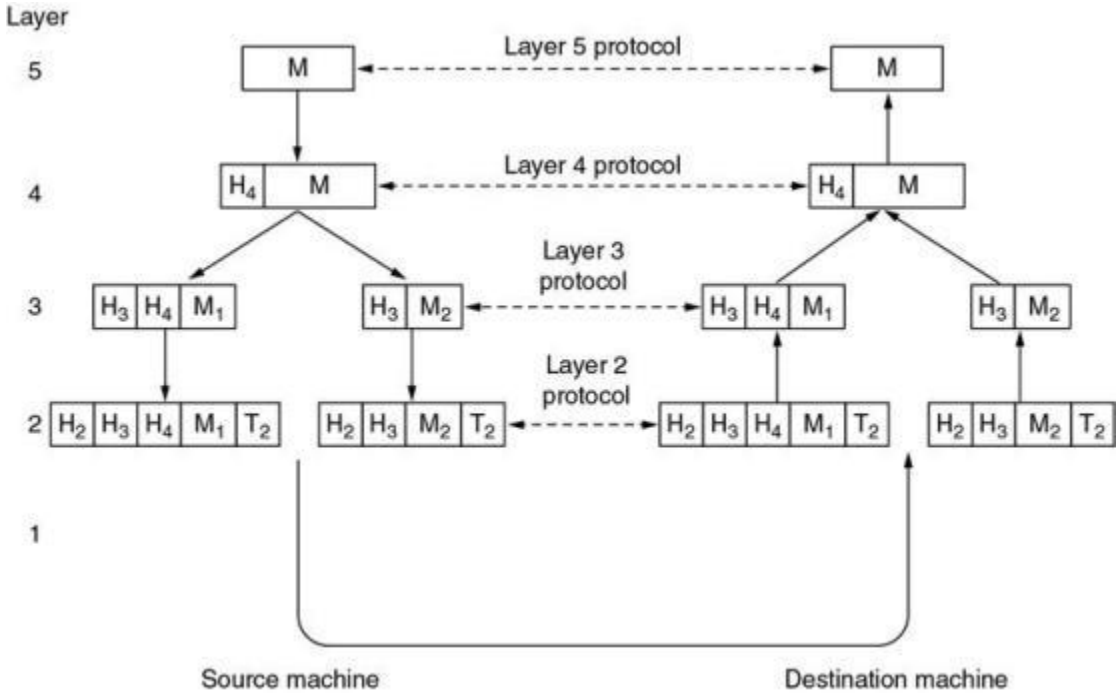

Figura 1.1 - Hierarquia de protocolos e encapsulamento [Tan03].

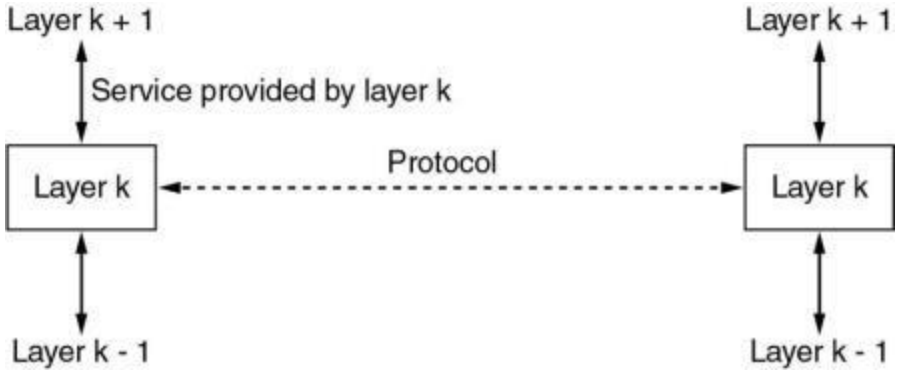

Figura 1.2 - Conceitos de serviço e protocolo da camada [Tan03].

A Figura 1.3 apresenta o modelo OSI (*Open Systems Interconnection*), que é usado como referência para a conceção de redes de comunicação, que é composto pelas 7 camadas apresentadas. Por cima da camada de aplicação situa-se a aplicação (programa) propriamente dita. Por exemplo, um *browser* da World Wide Web (WWW) é um programa que utiliza os serviços do protocolo da camada de aplicação HTTP (*Hypertext Transfer Protocol*).

Ao contrário do que indica a figura, nas redes de comunicação sem fios, o termo PPDU normalmente significa PHY PDU, ou seja, PDU da camada física. O pacote da camada 2 costuma receber a denominação particular de trama (*frame*), embora essa palavra também seja utilizada com outros significados. Nas redes cabladas, a camada de ligação de dados por vezes é dividida em duas subcamadas: a subcamada de controlo de acesso ao meio (MAC - *Medium Access Control*), por baixo, e a subcamada de controlo da ligação lógica (LLC - *Logical Link Control*), por cima. No caso das redes de comunicação sem fios, devido à importância do controlo de acesso ao meio, a camada 2 costuma ser conhecida simplesmente por camada MAC, e o pacote desta camada é conhecido como MPDU (MAC PDU).

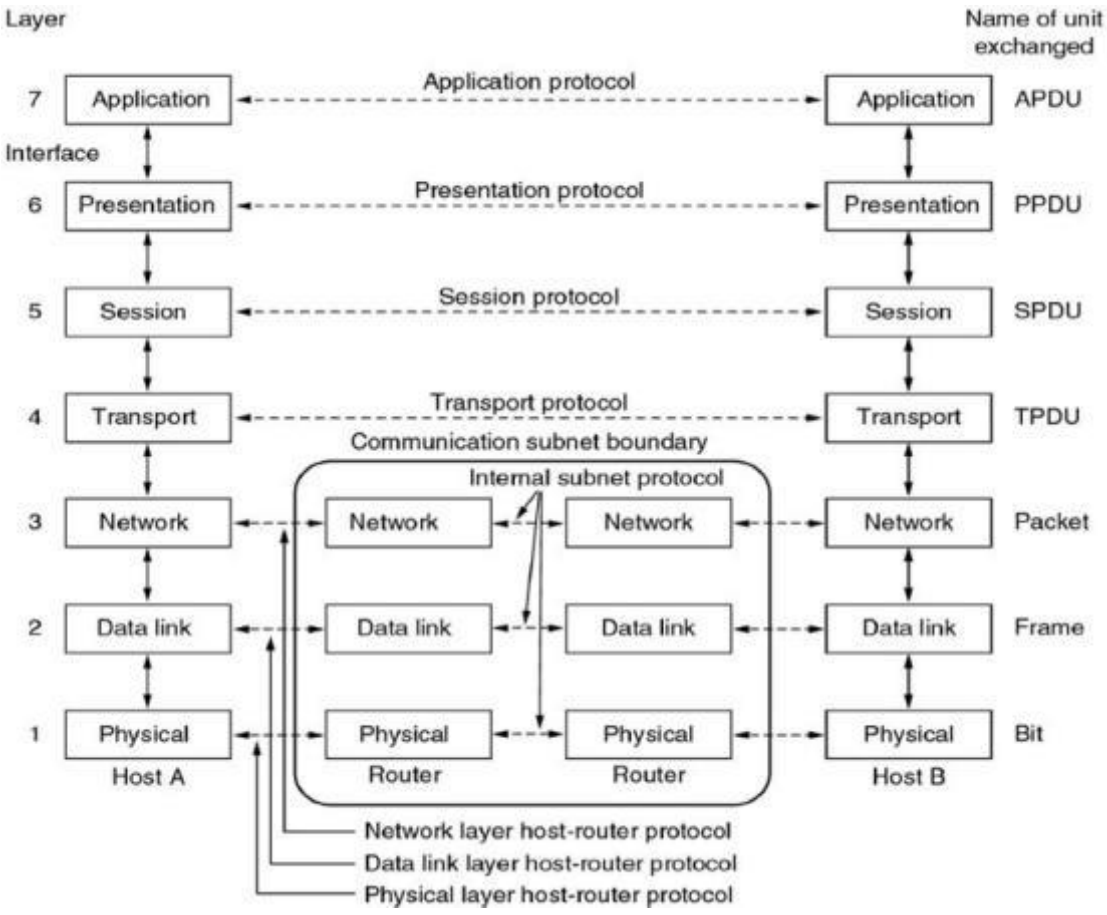

Figura 1.3 - Modelo OSI [Tan03].

Como mostra a Figura 1.3, entre os equipamentos terminais (*hosts* A e B) podem existir equipamentos de rede. Um *router* é um equipamento de rede que opera a nível das três camadas inferiores (até à camada de rede). Já um

comutador, ou *switch*, opera a nível das duas camadas inferiores, enquanto *hub* opera somente a nível da camada física.

Na prática, as camadas de apresentação e de sessão do modelo OSI são raramente usadas, sendo mais comumente usado o modelo de cinco camadas apresentado na Figura 1.4. Neste exemplo, o equipamento de rede implementa a funcionalidade de *internetworking*, funciona como um *gateway*, entre uma rede sem fios e uma rede cablada, que utilizam diferentes protocolos nas camadas inferiores.

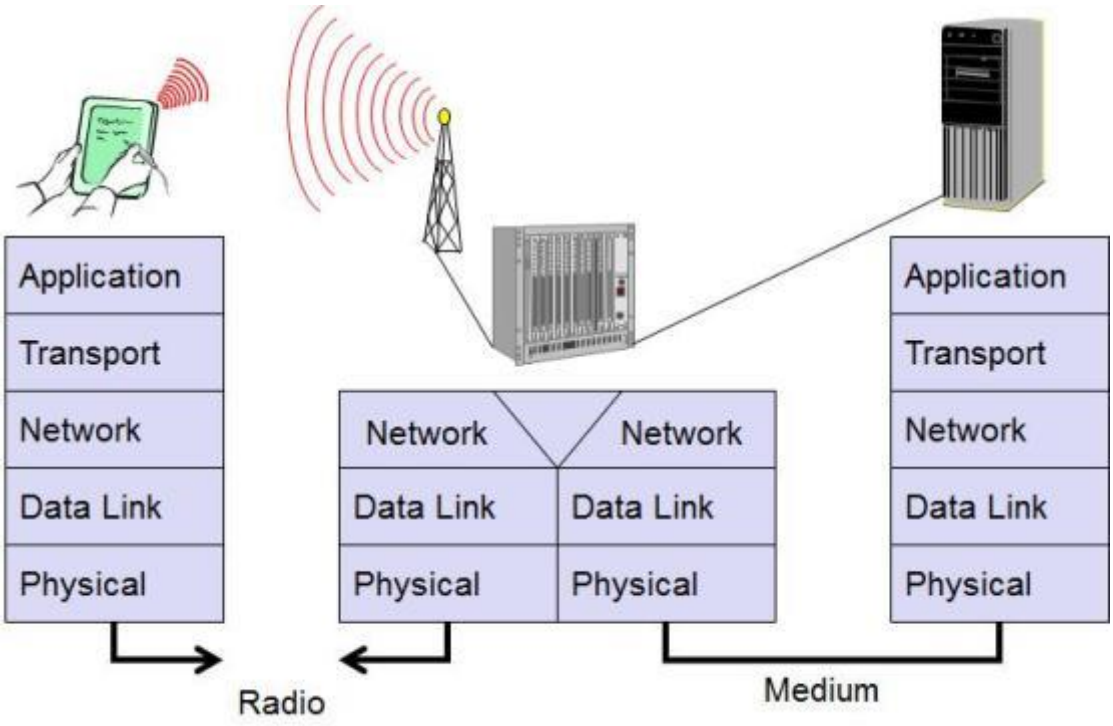

Figura 1.4 - Modelo de camadas tipicamente usado [Schi08].

Segue abaixo um resumo das principais funcionalidades oferecidas por cada uma dessas cinco camadas:

- **Camada física:** Esta camada é responsável pelos aspetos associados à transmissão do fluxo de bits a nível elétrico e mecânico, englobando funcionalidades como a modulação e desmodulação do sinal, sincronização dos bits e correção de erros.
- **Camada de ligação de dados:** É responsável pelo controlo de acesso ao meio e pela delimitação das tramas (*framing*), ou seja, pela tarefa de

identificar quando começa e quando termina uma trama. Esta camada também oferece funcionalidades de controlo de erros e controlo de fluxo.

- **Camada de rede:** Implementa as funcionalidades de encaminhamento de pacotes, endereçamento de rede, *internetworking* e controlo de congestionamento.
- **Camada de transporte:** Esta camada implementa controlo de erros e controlo de fluxo fim-a-fim (entre a origem e o destino), bem como multiplexagem de diferentes fluxos.
- **Camada de aplicação:** Proporciona serviços específicos para o utilizador final por intermédio da aplicação.

1.2 Atividade de normalização de redes

Para que os equipamentos de uma determinada rede possam comunicar entre si, é necessário que todos sigam os mesmos conjuntos de regras, ou seja, os mesmos protocolos. Existem diversas organizações responsáveis pela atividade de normalização de redes, ou seja, pela elaboração de normas (*standards*) que especificam as características de uma dada rede e dos respetivos protocolos. Algumas organizações de normalização estão associadas a governos, outras são criadas por membros da indústria, podendo contar também com a presença de membros de universidades e centros de investigação.

Uma das organizações mais influentes a nível mundial é o Comité 802 do IEEE. Este comité desenvolve e mantém normas de redes e recomendações de práticas no domínio das redes locais, redes metropolitanas e outras redes de comunicação. Algumas destas normas estão disponíveis para download gratuito em [IEEEGet]. Os grupos de trabalho (*working groups*) ativos em dezembro de 2012 são apresentados abaixo [IEEE802]:

- 802.1 - Higher Layer LAN Protocols Working Group.
- 802.3 - Ethernet Working Group.
- 802.11 - Wireless LAN Working Group.
- 802.15 - Wireless Personal Area Network (WPAN) Working Group.

- 802.16 - Broadband Wireless Access Working Group.
- 802.18 - Radio Regulatory TAG (Technical Advisory Group).
- 802.19 - Wireless Coexistence Working Group.
- 802.21 - Media Independent Handover Services Working Group.
- 802.22 - Wireless Regional Area Networks.
- 802.24 - Smart Grid TAG.
- OmniRAN EC Study Group.

Os seguintes grupos encontravam-se inativos nessa data:

- 802.17 - Resilient Packet Ring Working Group.
- 802.20 - Mobile Broadband Wireless Access (MBWA) Working Group.

Os grupos de trabalho listados abaixo foram encerrados:

- 802.2 - Logical Link Control Working Group.
- 802.4 - Token Bus Working Group.
- 802.5 - Token Ring Working Group.
- 802.6 - Metropolitan Area Network Working Group.
- 802.7 - Broadband TAG.
- 802.8 - Fiber Optic TAG.
- 802.9 - Integrated Services LAN Working.
- 802.10 - Security Working Group.
- 802.12 - Demand Priority Working Group.
- 802.14 - Cable Modem Working Group.
- 802.23 - Emergency Services Working Group.
- QOS/FC Executive Committee Study Group.
- ECSG TVWS TV Whitespace study group.
- ES-ECSG Emergency Services Executive Committee Study Group.

A análise da área de atuação destes grupos permite verificar que a maior parte dos grupos de trabalho ativos está relacionado a redes de comunicação sem fios, enquanto nenhum dos grupos inativos ou encerrados está associado a este tipo de redes.

Outra organização de normalização relevante na área dos sistemas de comunicação é o ETSI (*European Telecommunications Standards Institute*). O

ETSI é uma organização independente sem fins lucrativos europeia, com projeção global, que inclui membros da indústria das telecomunicações, nomeadamente fabricantes de equipamentos e operadoras de rede. O ETSI atuou na normalização de sistemas como a sistema celular móvel GSM (*Global System for Mobile Communications*) e o sistema de rádio móvel profissional TETRA (*Terrestrial Trunked Radio*). As normas do ETSI estão disponíveis para download gratuito em [ETSIPub].

O projecto BRAN (*Broadband Radio Access Networks*), do ETSI desenvolveu normas para as novas gerações de redes de comunicação sem fios de banda larga. Para sistemas com licença de operação, a principal aplicação visa o fornecimento de serviços para residências e empresas através da cobrança de subscrição. Por outro lado, os sistemas sem licença que foram desenvolvidos têm como objetivo a utilização maioritariamente dentro das instalações de empresas e em indústrias.

As redes de área local de alto débito HIPERLAN/1 e HIPERLAN/2, foram desenvolvidas no ambito deste projecto. Além destas redes, o projecto BRAN foi responsável pela normalização dos seguintes sistemas.

- **HIPERACCESS**: Visa proporcionar acesso fixo sem fios de banda larga (cerca de 25 Mbit/s) até às instalações do subscritor, sendo capaz de suportar aplicações multimédia. Apresenta um alcance de até 5 km e pode ou não requerer licença para operação, sendo vocacionado para o acesso por parte de residências e empresas de pequeno e médio porte, com operação em bandas entre 11 e 66 GHz.
- **HIPERLINK**: Destina-se a fornecer ligações de rádio de alto débito (até 155 Mbit/s) para interconexão estática de curta distância (até 150 m) entre redes HIPERACCESS ou HIPERLAN, sem necessidade de licença, com operação na banda de 17 GHz.

Alguns exemplos de organizações criadas por membros da indústria são referidos abaixo. Essas organizações são formadas para especificar ou promover normas associadas a um determinado sistema de comunicação e

para certificar a compatibilidade e interoperabilidade de produtos de diferentes fabricantes.

- Wi-Fi Alliance.
- Bluetooth SIG (*Special Interest Group*).
- ZigBee Alliance.
- WiMAX Forum.
- WiMedia Alliance.
- HART Communication Foundation.

1.3 Redes de comunicação sem fios

As redes de comunicação sem fios, de que são exemplos as redes celulares móveis e as redes de área local e pessoal sem fios, tem sido objeto de cresceste interesse e disseminação nas últimas décadas junto ao utilizador final. Este crescimento deriva da evolução da tecnologia combinada com as diversas vantagens proporcionadas pela não existência de cabos, como por exemplo:

- Maior mobilidade;
- Rápida instalação e reestruturação da rede;
- Redução dos custos e inconvenientes associados à instalação de cabos.

No seu início, as redes celulares móveis surgiram tendo em vista a transmissão de tráfego de voz em alternativa à rede telefónica fixa, enquanto as redes locais sem fios foram concebidas para substituir, ou complementar, as redes locais cabladas convencionais, como a Ethernet, criadas para transmissão de dados. O tráfego de voz (e vídeo) interativo possui requisitos de tempo real, impondo, por isso, limitações nos atrasos de transmissão, mas é relativamente tolerante a erros resultantes da perda de pacotes. Já o tráfego de dados normalmente não tolera erros, mas, por outro lado, não impõe restrições temporais, sendo por isso denominado tráfego assíncrono. Com a

evolução dessas redes e a popularização da Internet, caminhou-se no sentido da convergência quanto ao tráfego transportado por essas redes, dito multimédia, por abranger voz, vídeo e dados.

Como foi referido acima, cada tipo de tráfego impõe os seus requisitos de qualidade de serviço à rede de comunicação, pelo que a conceção de uma rede de comunicação deve ter em consideração a existência de mecanismos adequados para satisfazer esses requisitos do tráfego que a rede visa transportar. O tópico da qualidade de serviço é abordado com maior detalhe no capítulo 3.

Embora as redes sem fios apresentem diversas vantagens em relação às redes cabladas, o desenvolvimento destas redes também introduz desafios, associados à propagação em meio livre, dentre os quais se destacam os seguintes:

- A largura de banda disponível para a operação de um sistema sem fios é limitada, pois o espectro de frequências tem que ser dividido pelos diferentes serviços que partilham o mesmo meio, para possibilitar a sua coexistência.
- Nas redes sem fios normalmente não é possível transmitir e monitorar o canal ao mesmo tempo, pois o sinal transmitido sobrecarregaria os circuitos de receção. Isto tem repercussão a nível do protocolo de controlo de acesso ao meio.
- As redes cabladas podem ser organizadas em diferentes topologias de acordo com as ligações físicas entre as estações. Nas redes sem fios o sinal de uma estação propaga-se para todas as outras como num barramento.
- As redes sem fios estão sujeitas a taxas de erros no canal muito mais elevadas e variáveis no tempo, devido a fatores como interferências, obstrução e efeitos da propagação multipercurso.

1.4 Classificação das redes sem fios

Existem diversas formas de se implementar uma rede de comunicação sem fios. Esta secção apresenta três critérios de classificação deste tipo de redes:

- Tipo de estrutura.
- Forma de comunicação entre as estações.
- Tipo de coordenação do acesso ao meio.

As soluções associadas a cada um desses critérios são descritas abaixo. A escolha da solução mais apropriada em cada caso depende dos requisitos particulares da aplicação na qual se pretende utilizar a rede.

1.4.1 Estruturas de redes sem fios

No que concerne à estrutura, as redes de comunicação sem fios podem ser classificadas em duas categorias básicas: redes *ad hoc* e redes baseadas em infraestrutura, como mostra a Figura 1.5.

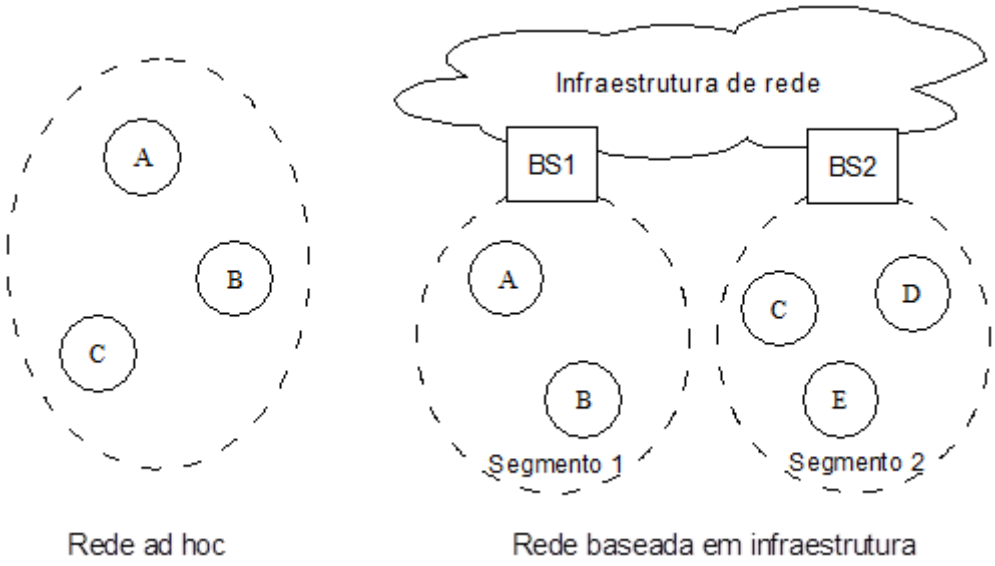

Figura 1.5 - Estruturas de redes sem fios.

- **Rede *ad hoc*:** O principal propósito de uma rede *ad hoc* é possibilitar a comunicação entre as estações que formam a rede. As redes *ad hoc* costumam operar durante períodos relativamente curtos, pelo que

geralmente são concebidas de forma a tornar simples e rápido o processo de estabelecimento e dissolução da rede. Um exemplo de aplicação deste tipo de rede é uma reunião de negócios, durante a qual os participantes podem utilizar os seus dispositivos portáteis para partilhar informações entre si.

- **Rede baseada em infraestrutura:** Estas redes são segmentos sem fios de uma rede mais extensa, cujo núcleo é normalmente uma rede cablada. As redes baseadas em infraestrutura possuem uma estação especial, denominada de ponto de acesso (AP - *Access Point*) ou estação base (BS - *Base Station*), que serve de interface entre o segmento sem fios e o resto da rede. Exemplos de infraestruturas de rede junto às quais são utilizadas estas redes sem fios são o *backbone* da rede telefónica e a rede local de uma organização.

1.4.2 Modos de comunicação entre as estações

O meio de transmissão sem fios é um meio de difusão por natureza, ou seja, a princípio a transmissão de uma estação poderia ser recebida diretamente por qualquer outra estação na sua vizinhança[1]. Apesar disso, a rede pode ser concebida de forma que as estações não possam comunicar diretamente entre si, mas apenas por intermédio de uma estação central. Tendo isso em consideração, as redes sem fios podem operar utilizando comunicação direta entre as estações ou comunicação centralizada, como é representado na Figura 1.6. Estas configurações correspondem, em termos lógicos, às topologias em barramento (*bus*) e em estrela (*star*) das redes cabladas, respetivamente.

[1] Desde que não haja estações ocultas na rede.

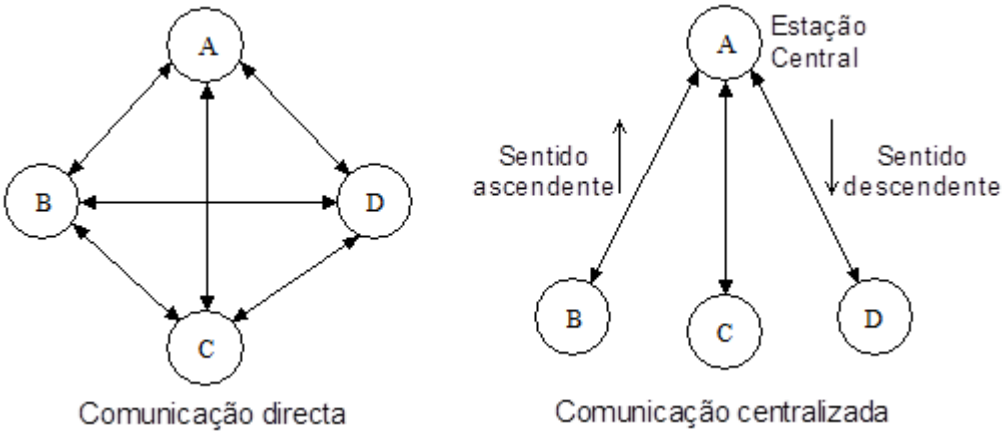

Figura 1.6: Modos de comunicação entre as estações numa rede sem fios.

- **Comunicação direta:** Nesta configuração, as estações que pertencem à rede sem fios comunicam diretamente entre si. Nas redes baseadas em infraestrutura que usam esta configuração, apenas as mensagens que têm como origem ou destino o exterior da rede é que precisam passar pela estação base. Este modo de operação é apropriado para aplicações em que a maior parte do tráfego é trocado entre as estações situadas dentro de uma mesma célula.
- **Comunicação centralizada:** Nesta configuração, todas as mensagens que circulam na rede passam por uma estação central[2]. Estas redes admitem apenas dois sentidos de transmissão: o sentido descendente (*downlink*), da estação central para as outras estações; e o sentido ascendente (*uplink*), destas estações para a estação central. A ligação ascendente é do tipo ponto a ponto. Já a ligação descendente geralmente é do tipo ponto-multiponto, permitindo a transmissão simultânea de informação para um grupo de estações na célula (*multicast*) ou para todas as estações (*broadcast*). Para que duas estações terminais da mesma célula possam comunicar, a estação de origem tem que transmitir a sua mensagem para a estação central, que depois retransmite a mensagem

[2] A estação central é tipicamente a estação base de uma rede baseada em infraestrutura, embora esta configuração também seja usada em algumas redes *ad hoc*.

para a estação de destino. Isso implica a duplicação da largura de banda necessária em relação ao modo de comunicação direta, pelo que a comunicação centralizada é mais apropriada quando a maior parte do tráfego das estações é trocado com a estação central ou com unidades situadas no exterior da célula.

Estendendo-se esta classificação para o caso de topologias *multihop*, pode se dizer que a topologia em árvore (*tree*) apresenta comunicação centralizada a nível local, enquanto a topologia em malha (*mesh*) possibilita a comunicação direta entre estações vizinhas.

1.4.3 Coordenação de acesso ao meio

O tipo de coordenação de acesso ao meio é um dos parâmetros pelos quis os diferentes protocolos de controlo de acesso ao meio (MAC - *Medium Access Control*) podem ser classificados. As categorias nas quais podem ser inseridos estes protocolos e respetivas características são apresentados na secção 4.2.2. A coordenação do acesso ao meio pode ser baseada em controlo centralizado ou distribuído:

- **Controlo centralizado:** Neste caso, a rede possui um controlador central (CC, *Central Controller*), que é uma estação especial à qual é conferida autoridade para regular o acesso ao meio por parte das outras estações da rede. Neste contexto, uma estação que deseje transmitir dados no meio não poderá decidir o instante de fazê-lo por conta própria, mas antes deverá esperar pelo momento atribuído pelo controlador central. Esta atribuição pode ser feita de diferentes formas, dando origem a diferentes categorias de protocolos de controlo de acesso ao meio baseados em controlo centralizado. Embora a transmissão de dados das estações esteja sujeita à autorização por parte do controlador central, estes protocolos normalmente permitem que as estações transmitam pacotes de controlo especiais sem necessidade de autorização prévia, para que estas possam enviar ao coordenador central os seus pedidos de oportunidade de transmissão. No caso específico das redes baseadas em infraestrutura que

operam com controlo centralizado, o papel de controlador central normalmente é desempenhado pela estação base.

- **Controlo distribuído:** Neste caso, o acesso das estações ao meio é decidido de forma distribuída por todas as estações participantes na rede, segundo as regras definidas pelo protocolo de controlo de acesso ao meio utilizado. Os diversos tipos de protocolos desenvolvidos com base nesta filosofia diferem quanto às suas regras particulares, que devem ser seguidas por todas as estações que fazem parte da rede de forma a haver justiça na repartição da largura de banda disponível.

1.5 Tipos de redes de comunicação sem fios

Devido à grande variedade e à constante evolução das tecnologias e aplicações de redes de comunicações sem fios, a tarefa de classificar estas redes em categorias é complexa. A classificação apresentada abaixo agrupa estas redes em cinco categorias:

- Redes celulares móveis.
- Redes de acesso fixo sem fios.
- Redes de comunicação móvel via satélite.
- Redes de área local sem fios.
- Redes de área pessoal sem fios.

As redes celulares móveis, redes de acesso fixo sem fios e redes de satélite proporcionam o acesso dos utilizadores a uma infraestrutura de rede. Nestes três tipos de redes, normalmente o equipamento de rede é propriedade de uma operadora, que cobra uma taxa de utilização pelos serviços oferecidos. Os utilizadores precisam adquirir apenas o equipamento terminal. Estes sistemas normalmente operam em banda de frequências que requerem licença de operação.

As redes celulares móveis surgiram com o objetivo de possibilitar a transmissão de tráfego de voz sem a restrição de mobilidade imposta pelos

telefones fixos. O utilizador transporta o equipamento terminal (telemóvel) consigo, de modo a ter acesso à rede telefónica pública em qualquer local dentro da zona de cobertura da rede. Para possibilitar o aumento da cobertura e do número de utilizadores servidos, a área coberta pela rede é repartida em células[3]. Como o nível de sinal decresce com a distância, as células suficientemente afastadas entre si podem reutilizar as frequências de operação disponíveis sem que haja interferência significativa. Estes sistemas têm evoluído no sentido do aumento do débito disponível para os utilizadores, da diversificação dos serviços oferecidos e da possibilidade de transmissão de tráfego multimédia.

As redes de acesso fixo sem fios visam oferecer acesso a serviços de comunicação de voz, vídeo e dados na casa do utilizador, em alternativa a tecnologias de acesso por cabo, fibra ou DSL (*Digital Subscriber Line*). A principal diferença em relação aos sistemas celulares móveis é que a localização do equipamento terminal do subscritor é normalmente fixa, permitindo oferecer potencialmente serviços de mais alto débito a um custo mais reduzido. Um exemplo deste tipo de tecnologia é a norma IEEE 802.16 original, conhecida como WiMAX (*Worldwide Interoperability for Microwave Access*) fixo, embora uma versão móvel tenha sido lançada posteriormente. Como a evolução da tecnologia e a concorrência das redes celulares e redes locais sem fios, o mercado potencial deste tipo de redes tem vindo a decrescer, nomeadamente em áreas urbanas.

As redes de comunicação móvel via satélite oferecem comunicação bidirecional de voz e dados com os terminais móveis dos utilizadores utilizando uma constelação de satélites que orbitam próximo à Terra (LEO - *Low Earth Orbit*). A principal vantagem destes sistemas é a cobertura global. Vários sistemas deste tipo surgiram na década de 90, como são exemplo Iridium, Globalstar, Teledesic e Orbcomm. Porém, devido ao custo elevado e à concorrência de outros sistemas terrestres, muitas destas empresas

[3] Vindo daí a designação destes sistemas.

enfrentaram graves dificuldades financeiras ao verem a sua quota de mercado prevista decrescer significativamente. No entanto, outros sistemas de comunicação baseados em satélites prosperam no mercado, como é o caso de sistemas de empresas como a Eutelsat e a Astra que utilizam satélites geoestacionários para a transmissão de sinal de televisão e rádio.

Ao contrário das redes celulares móveis, as redes de área local sem fios (WLAN - *Wireless Local Area Network*) surgiram com o objetivo de transmitir tráfego de dados (assíncrono), visando a comunicação de dados entre os computadores dentro de uma organização. Neste tipo de redes, assim como nas redes de área pessoal, o equipamento tende a ser adquirido pelos utilizadores para uso privado. Outro fator diferenciador é que estas redes operam em bandas de frequências que não requerem licença de utilização. As redes locais sem fios têm evoluído em diversas vertentes, nas quais se realça o aumento do débito disponível e a introdução de suporte de qualidade de serviço para diferentes classes de tráfego.

As redes locais sem fios baseados no conjunto de normas IEEE 802.11 são, de longe, as mais bem-sucedidas no mercado atualmente. O HIPERLAN/2 é uma tecnologia de rede de área local alternativa. Devido à concorrência do IEEE 802.11, que apresenta uma implementação mais simples e chegou primeiro ao mercado, o HIPERLAN/2 nunca chegou a ter representatividade em termos de implementação comercial. No entanto, muitos dos conceitos e mecanismos concebidos para o HIPERLAN/2 foram aproveitados por outras redes, como é o caso da especificação da camada física da norma IEEE 802.11a, que é quase idêntica à camada física do HIPERLAN/2. A secção 1.6 apresenta uma breve descrição da história das redes de área local.

O conceito de redes de área pessoal sem fios (WPAN - *Wireless Personal Area Network*) surgiu mais recentemente, devido à crescente profusão de dispositivos portáteis. O tipo de tráfego transportado depende da aplicação dada a uma determinada rede de área pessoal em particular. O alcance das transmissões deste tipo de redes é inferior ao das redes de área local, visto que o objetivo das redes de área pessoal é, como diz o seu nome, abranger uma área em torno do utilizador. O custo, a complexidade e o consumo dos

equipamentos também tendem a ser inferiores. Dois exemplos de redes de área pessoal são o Bluetooth, que é descrito no capítulo 5, e o ZigBee, descrito no capítulo 7. A secção 1.7 apresenta uma visão geral das redes de área pessoal e das principais normas nesta área.

A Figura 1.7 ilustra diferentes tecnologias de redes de comunicações sem fios, classificadas quanto à área aplicação principal, a taxa de transferência de dados e o alcance da ligação sem fios.

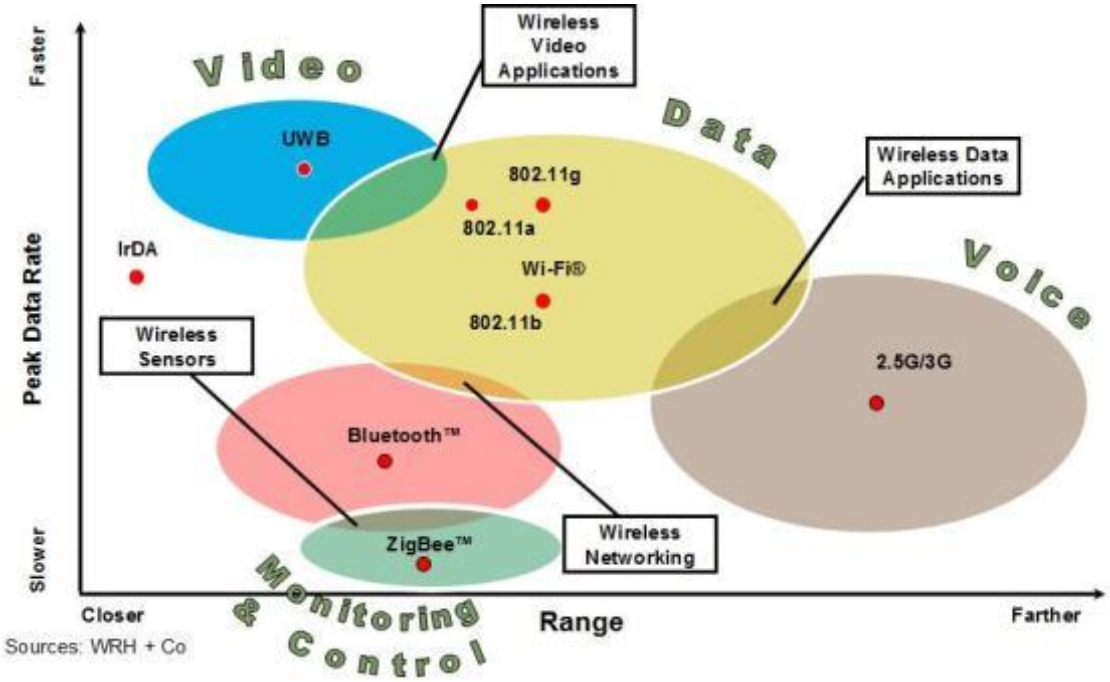

Figura 1.7: Tecnologias de redes de comunicação sem fios.

1.6 Redes de área local sem fios

O mercado de redes de área local sem fios (WLAN - *Wireless Local Area Network*) teve um primeiro impulso em meados da década de 80, com a decisão da FCC (*Federal Communications Commission*), nos Estados Unidos, de autorizar a utilização pública das bandas ISM (*Industrial, Scientific and Medical*), eliminando com isso a necessidade de obtenção de licenças para a operação dos produtos WLAN. Entretanto, a falta de normas fez com que aparecessem no mercado diversos produtos proprietários incompatíveis entre si, limitando o desenvolvimento da indústria de redes locais sem fios.

A primeira tentativa de definição de um padrão de redes locais sem fios foi feita no final da década de 80. O grupo de trabalho IEEE 802.4 foi mandatado para desenvolver um protocolo de controlo de acesso ao meio baseado em passagem de testemunho para utilização em redes WLAN. Porém, este grupo chegou à conclusão de que o mecanismo de passagem de testemunho era inadequado para utilização em redes sem fios, pelo que o desenvolvimento de um mecanismo alternativo foi sugerido.

Na sequência desta opção, o comité executivo 802 do IEEE decidiu criar o grupo de trabalho 802.11. Com base nos produtos existentes no mercado e no esforço de investigação, este grupo concluiu a primeira versão das normas IEEE 802.11 em 1997. Esta norma define três opções de camadas físicas, sendo que duas delas operam na banda ISM de 2.4 GHz utilizando espalhamento espectral: uma por saltos em frequência (FHSS - *Frequency Hopping Spread Spectrum*) e a outra por sequência direta (DSSS - *Direct Sequence Spread Spectrum*). Uma terceira opção de camada física foi definida para operação na banda de infravermelhos. O débito máximo especificado por esta norma situa-se em 2 Mbit/s a nível da camada física, sendo o controlo de acesso ao meio baseado num protocolo de acesso aleatório do tipo CSMA/CA. Um outro protocolo baseado em *polling*, de implementação opcional, também é disponibilizado para suporte a tráfego isócrono.

Em 1999, dois suplementos à versão original da norma foram aprovados. O IEEE 802.11b, baseado na camada física que opera na banda ISM de 2.4 GHz e utilizando espalhamento espectral por sequência direta (DSSS), expande o débito máximo a 11 Mbit/s, mantendo porém a compatibilidade com a versão original baseada em DSSS. Por outro lado, o IEEE 802.11a opera na banda de 5 GHz com modulação OFDM (*Orthogonal Frequency Division Multiplexing*), sendo capaz de atingir um débito máximo de 54 Mbit/s. Todas estas versões operam com os mesmos protocolos de controlo de acesso ao meio, embora os seus parâmetros sejam diferentes em função da camada física utilizada. O IEEE 802.11 é descrito com detalhe no capítulo 4.

Paralelamente ao desenvolvimento do IEEE 802.11, outro padrão de redes de área local sem fios, denominado HIPERLAN (*High Performance European*

Radio LAN), foi desenvolvido pelo comité técnico RES10 (*Radio Equipment and Systems*) do ETSI. Esta primeira versão do HIPERLAN foi concebida para operar na banda de 5.2 GHz com a utilização de modulação de banda estreita, oferecendo um débito de transmissão da ordem de 25 Mbit/s. O controlo de acesso ao meio é baseado num protocolo de acesso aleatório, denominado EY-NPMA (*Elimination Yield Non-Preemptive Priority Multiple Access*), que permite a atribuição de diferentes níveis de prioridade aos pacotes que competem pelo acesso ao meio. Este sistema é conhecido pela denominação HIPERLAN/1.

Após a definição das normas do HIPERLAN/1, o ETSI decidiu unificar o trabalho de normalização em redes sem fios de banda larga, incluindo as redes locais sem fios e as redes de acesso fixo sem fios, no projeto BRAN (*Broadband Radio Access Networks*). Sob a alçada deste projeto, foi desenvolvido outro padrão de redes locais sem fios de alto débito, denominado HIPERLAN/2, concebido para o transporte eficiente de células ATM (assim como outros tipos de tráfego, como pacotes IP), pelo que também costuma ser classificado como uma rede ATM sem fios (WATM - *Wireless* ATM). O HIPERLAN/2 opera na banda de 5 GHz utilizando modulação OFDM, permitindo alcançar um débito máximo de 54 Mbit/s ao nível da camada física, tal como o IEEE 802.11a. Ao contrário deste, o controlo de acesso ao meio do HIPERLAN/2 é baseado num protocolo de reserva dinâmica explícita. A utilização deste protocolo permite oferecer um suporte de qualidade de serviço (QoS) muito mais completo.

1.7 Redes de área pessoal

O conceito de rede de área pessoal (PAN - *Personal Area Network*), ou rede pessoal, refere-se à comunicação entre múltiplos dispositivos que se encontram nas proximidades de um indivíduo. A motivação para o aparecimento das redes pessoais deve-se ao facto de, no seu dia-a-dia, cada vez mais as pessoas passarem a conviver com uma maior diversidade de dispositivos eletrónicos, à medida que estes dispositivos tornam-se cada vez

menores e mais baratos. As redes pessoais visam proporcionar o intercâmbio de informação entre esses dispositivos, quando necessário, de uma forma conveniente para o utilizador. A comunicação sem fios é apropriada neste caso, pois evita que o utilizador tenha frequentemente de conectar e desconectar os cabos de ligação entre os dispositivos, dado que as conexões entre os mesmos tendem a ser de curta duração. Além disso, a mobilidade dos dispositivos é francamente favorecida.

Conceptualmente, a principal diferença entre as redes pessoais sem fios (WPAN)[4] e as redes locais sem fios (WLAN) é que as primeiras tendem a ser centradas em torno de um utilizador, enquanto que as últimas costumam servir múltiplos utilizadores, embora esta distinção às vezes não se verifique na prática, sendo que nalguns casos estas redes nem mesmo interagem diretamente com pessoas, mas sim com sensores e atuadores, como é o caso das redes pessoais utilizadas em aplicações na área das redes de sensores sem fios (WSN - *Wireless Sensor Network*). As redes pessoais costumam ter em comum um alcance limitado a poucos metros e uma configuração simples e rápida das ligações. Entre os dispositivos que podem ser ligados numa rede pessoal encontram-se computadores portáteis e de mesa, *palmtops*, teclados, ratos, impressoras, pontos de acesso a redes locais, telemóveis, auriculares, câmaras fotográficas e de vídeo, relógios de pulso, entre outros.

Para comunicação entre dispositivos portáteis a curtas distâncias, o sistema mais utilizado há alguns anos atrás baseava-se nas normas publicadas pela *Infrared Data Association* (IrDA). Este sistema opera por comunicação ótica na banda de infravermelhos, proporcionando ligações ponto a ponto com uma abertura do feixe de cerca de 30 graus, alcance limitado a cerca de 1 m e débito máximo de 4 Mbit/s. Entre as vantagens desta tecnologia estão o seu baixo custo e consumo. Por outro lado, o IrDA requer a existência

[4] Dado que as redes pessoais existentes geralmente operam sem fios, na prática, os termos PAN e WPAN são sinónimos.

de linha de vista entre os dispositivos, oferece um alcance pequeno e reduzida mobilidade.

Desenvolvido por iniciativa de membros da indústria de eletrónica e telecomunicações, o Bluetooth [Haar00] é outro exemplo de rede pessoal sem fios. As suas características principais são a operação na banda ISM de 2.4 GHz com a utilização da técnica de espalhamento espectral por saltos em frequência (FHSS), um alcance típico de 10 m, o suporte de canais síncronos e simétricos de 64 kbit/s para transmissão de voz, e de canais assíncronos para transmissão de dados. Estes últimos oferecem débitos assimétricos de até 723.2 kbit/s, numa direção, e 57.6 kbit/s, na outra, ou débitos simétricos de até 432.6 kbit/s. O Bluetooth é descrito com mais pormenor no capítulo 5.

Embora o grupo de trabalho IEEE 802.11 para redes de área local sem fios já existisse, o IEEE decidiu formar, em 1999, um novo grupo (802.15), com o objetivo específico de desenvolver normas para redes de área pessoal sem fios. Esta opção ficou a dever-se ao facto das aplicações das redes pessoais procurarem soluções muito mais restritivas quanto ao custo, consumo e dimensão dos produtos do que as redes locais. O grupo de trabalho IEEE 802.15 para redes de área pessoal sem fios (WPAN) é constituído pelos grupos de tarefa (TG - *Task Group*) descritos abaixo:

- **TG1: WPAN/Bluetooth.** Este grupo foi formado com o objetivo de desenvolver uma especificação para redes de área pessoal sem fios baseada no Bluetooth. Normas foram publicadas em 2002 [IEEE02] e 2005.
- **TG2: Coexistência.** Este grupo desenvolveu recomendações no sentido de facilitar a coexistência entre redes pessoais sem fios e outras redes operando em bandas isentas de licença na mesma área, como é o caso de redes locais sem fios, de forma a minimizar a interferência mútua. A norma IEEE 802.15.2-2003 foi publicada em 2003 e após isso este grupo entrou em hibernação.
- **TG3: WPAN de alto débito.** Este grupo visa desenvolver normas de redes pessoais sem fios de alto débito para atender às necessidades de

aplicações de imagem digital e multimédia em dispositivos portáteis, enquanto mantém os requisitos de baixo custo e baixo consumo. Diversas normas foram publicadas por este grupo entre 2003 e 2009.

- **TG4: WPAN de baixo débito.** O objetivo deste grupo consiste em desenvolver redes de baixo débito (20 a 250 kbit/s), mas com longa autonomia (meses a anos, utilizando baterias) e complexidade muito baixa. Possíveis aplicações incluem sensores, brinquedos interativos, comandos remotos e automação residencial. A primeira versão da norma IEEE 802.15.4 foi publicada em 2003. Esta norma define a camada física (PHY) e a camada MAC. Diversas redes e protocolos, abertos ou proprietários, assentam sobre as camadas definidas na norma IEEE 802.15.4, como é o caso do ZigBee, 6LoWPAN, IEEE 802.15.5, WirelessHART e ISA100.11a. As normas IEEE 802.15.4 e ZigBee são descritas com mais detalhes nos capítulos 6 e 7.
- **TG5: WPAN mesh networking.** Este grupo visa a definição de recomendações para a interoperabilidade, estabilidade e escalabilidade de redes de área pessoal baseadas em topologias em malha. A norma IEEE 802.15.5-2009 foi publicada em maio de 2009.
- **TG6: Redes de área corporal.** Este grupo foi formado em 2007 com o objetivo de desenvolver uma norma de rede sem fios de baixa potência em curto alcance para redes de área corporal (BAN - *Body Area Network*), otimizada para operação no interior, sobre, ou em torno do corpo humano (mas não limitada a humanos), destinada a servir um conjunto variado de aplicações, incluindo as áreas da medicina, desporto e entretenimento. A norma IEEE 802.15.6-2012 foi publicada em fevereiro de 2012.
- **TG7: VLC - Visible Light Communications**. Este grupo foi criado com o objetivo de especificar a camada física e a camada MAC de um sistema de comunicação ótica utilizando luz visível de curto alcance capaz de suportar serviços multimédia de áudio e vídeo. O grupo publicou a norma IEEE 802.15.7-2011 em setembro de 2011.

Referências

[Haar00] J. C. Haartsen, “The Bluetooth Radio System”, *IEEE Personal Communications*, pp. 28-36, February 2000.

[IEEE.15] IEEE 802.15 Documents. https://mentor.ieee.org/802.15/documents

[ETSIPub] ETSI Publications Download Area. http://pda.etsi.org/pda/queryform.asp

[IEEE02] IEEE 802.15.1 “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), 2002.

[IEEE802] IEEE 802 LAN/MAN Standards Committee. http://www.ieee802.org/

[IEEEGet] IEEE Get Program, IEEE Standards Association. http://standards.ieee.org/about/get/

[Schi08] Jochen Schiller, “Mobile Communications” Addison-Wesley, 2008.

[Tan03] A. S. Tanembaum, “Computer Networks”, Prentice Hall, 2003.

2. Camada física

2.1 O espectro eletromagnético

A utilização do espectro eletromagnético, tanto pelas redes de comunicação sem fios como por outros sistemas que emitem ondas de rádio, é rigorosamente controlada de modo a possibilitar a partilha do meio de transmissão por todos os utilizadores. Entre as organizações responsáveis pela alocação de bandas de frequência para a operação dos diferentes sistemas, encontram-se o Comité Europeu de Radiocomunicações (ERC - *European Radiocommunications Committee*), vinculado ao CEPT (*European Conference of Postal and Telecommunications Administrations*), na Europa, e a FCC (*Federal Communications Commission*), nos Estados Unidos da América. Normalmente, a operação numa dada banda de frequências requer a negociação com estas organizações e o pagamento de uma taxa. Após a análise das características do sistema, como a potência de transmissão e a cobertura geográfica, as instituições competentes conferem a atribuição da licença de operação, ou seja, o direito de utilização da banda de frequências.

A Figura 2.1 apresenta o espectro eletromagnético. Como se pode ver na figura, o espectro é composto por diversas gamas de frequência: rádio, micro-ondas, infravermelhos, luz visível, ultravioletas (UV - *Ultraviolet*), raios X e raios gama. Na figura também se podem ver as partes do espectro utilizadas por tecnologias como o par entrançado (*twisted pair*), cabo coaxial, satélites e fibras óticas.

O espectro também foi dividido em diversas bandas pelo ITU: VLF (*Very Low Frequency*), LF (*Low Frequency*), MF (*Medium Frequency*), HF (*High Frequency*), VHF (*Very High Frequency*), UHF (*Ultra High Frequency*), SHF (*Super High Frequency*), EHF (*Extra High Frequency*) e THF (*Tremendously High Frequency*). O avanço da tecnologia veio possibilitar o uso das bandas de frequências superiores, que não eram utilizadas na época em que foi feita

esta classificação, sendo esse o motivo da denominação curiosa das bandas a partir do UHF.

A banda UHF, que abrange frequências entre 300 MHz e 3 GHz, é a mais utilizada por redes de comunicação sem fios atualmente. Essas frequências correspondem a comprimentos de onda entre 1 m e 10 cm, respetivamente. Essa correspondência é dada pela fórmula $\lambda = c/f$, onde λ é o comprimento de onda, f é a frequência e c é a velocidade da luz no vácuo ($3x10^8$ m/s).

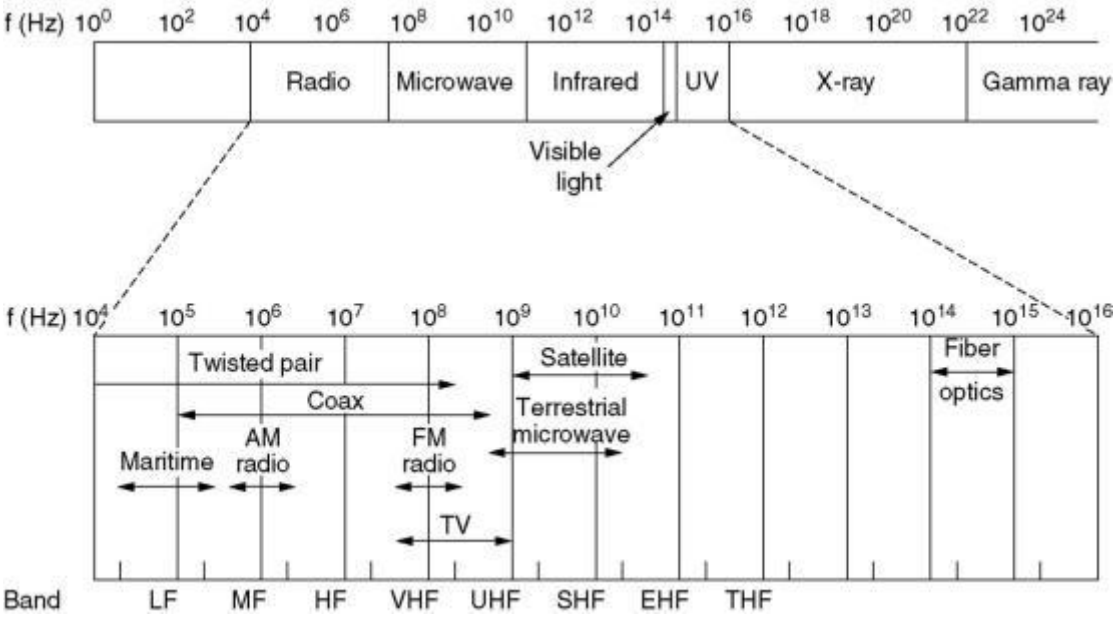

Figura 2.1: O espectro eletromagnético [Tane89].

Devido às dificuldades que o processo de licenciamento impõe aos utilizadores individuais, foram definidas bandas de frequências que podem ser usadas sem necessidade de licença, embora não deixem de estar sujeitas a restrições relativamente à potência máxima de transmissão e à técnica de modulação utilizada. Estas bandas são conhecidas pela designação ISM (*Industrial, Scientific and Medical*). Como o nome sugere, essas bandas já eram utilizadas anteriormente por diversos equipamentos, desde aparelhos de instrumentação médica e científica até fornalhas industriais e fornos de micro-ondas. Estes equipamentos, assim como outras redes sem fios que operem na vizinhança, podem provocar interferências nas comunicações de uma rede sem fios. Apesar das técnicas de espalhamento espectral permitirem diminuir

os efeitos da interferência, a resolução do problema não é garantida, sendo esta uma desvantagem associada à utilização de uma banda que não requer licença de operação. A banda ISM mais popular, disponível em todo o globo, está localizada nos 2.4 GHz.

O Quadro Nacional de Atribuição de Frequências para os diversos serviços em Portugal pode ser consultado no site da ANACOM, através do link: http://www.anacom.pt/render.jsp?contentId=779479.

2.2 Degradação do sinal

Os sinais que se propagam num meio sem fios estão sujeitos a diversos fatores que degradam a sua qualidade, dificultando a recuperação da informação original que foi transmitida e, consequentemente, causando erros de transmissão. Estes fatores são listados abaixo:

- Atenuação.
- Perda em espaço livre.
- Ruído.
- Interferência.
- Propagação multipercurso.

A atenuação consiste na redução da intensidade do sinal eletromagnético com a distância devido à absorção e espalhamento de fotões ao longo do meio de transmissão no caminho entre o emissor e o recetor. O sinal deve chegar ao recetor com uma intensidade suficiente para que este possa interpretar o sinal. Além disso, quanto maior o nível do sinal que chega ao recetor em comparação com o ruído, menor será a probabilidade de ocorrência de erros na descodificação do sinal. A atenuação tende a ser maior para frequências mais altas.

A atenuação do sinal pode aumentar significativamente caso haja obstáculos (por exemplo, uma parede) entre o emissor e o recetor, sendo este fenómeno denominado obstrução (*shadowing*).

A perda em espaço livre, ao contrário da atenuação, está relacionada a dispersão do sinal pelo espaço, que faz com que a densidade de potência por unidade de área diminua com o quadrado da distância, e com a área efetiva da antena recetora, que é proporcional ao quadrado do comprimento de onda do sinal. No caso da antena isotrópica ideal, isso resulta na seguinte expressão:

$$\frac{P_t}{P_r} = \frac{(4\pi d)^2}{\lambda^2} = \frac{(4\pi f d)^2}{c^2} \tag{2.1}$$

P_t é a potência transmitida, P_r é a potência recebida à distância d, λ é o comprimento de onda, f é a frequência e c é a velocidade da luz no vácuo. Todas as grandezas estão expressas em unidades do Sistema Internacional.

Essa perda (*path loss*) também pode ser expressa em dB. Note que como $P_r < P_r$, essa perda tem um valor positivo.

$$PL[dB] = L_{dB} = 10\log_{10}\left(\frac{P_t}{P_r}\right) \tag{2.2}$$

A propagação multipercurso (*multipath*) consiste na receção de um mesmo sinal por múltiplos caminhos, devido aos fenómenos de reflexão, espalhamento e difração do sinal transmitido em objetos existentes no ambiente, o que faz com que múltiplas cópias do mesmo sinal cheguem ao recetor. Estas cópias são recebidas com desfasamento umas das outras, como consequência de as diferentes cópias percorrerem caminhos com comprimentos diferentes, dando origem a dois efeitos:

- O desvanecimento multipercurso (*multipath fading*) resulta da combinação, construtiva ou destrutiva, das diferentes cópias, que pode provocar flutuações significativas na intensidade do sinal resultante.
- A interferência intersimbólica (ISI - *InterSymbol Interference*) ocorre quando uma parcela da energia de um símbolo (por exemplo, um bit) sobrepõe-se à do símbolo seguinte, dificultando a identificação do símbolo correto.

2.3 Controlo de erros

Devido aos fatores descritos na secção anterior, as redes sem fios estão sujeitas a taxas de erros muito mais intensas e variáveis do que as redes cabladas. Os mecanismos de compensação de erros que podem ser implementados a nível da camada física, com o propósito de aumentar a fiabilidade das comunicações, incluem técnicas de equalização, diversidade e correção antecipada de erros. Essas técnicas são descritas com mais detalhes na secção 3.3.

Referências

[Schi04] Jochen Schiller, “Mobile Communications”, 2nd edition, Addison-Wesley, 2004

[Stal02] William Stallings, “Wireless Communications and Networks”, Prentice-Hall, 2002.

[Tane89] A. S. Tanembaum, “Computer Networks”, Prentice Hall, 1989.

3. Qualidade de serviço

3.1 Introdução

Algumas aplicações são relativamente insensíveis à degradação transitória da qualidade de serviço oferecida pela rede. Por exemplo, num serviço de transferência de ficheiros, a redução da largura de banda disponível ou o aumento do atraso dos pacotes podem afetar o desempenho da aplicação, mas não comprometem a sua operação. Devido à capacidade de adaptação a variações na disponibilidade de recursos, tais aplicações são denominadas de elásticas. Essas aplicações contentam-se com um serviço do tipo melhor esforço, no qual a rede compromete-se apenas a tentar transmitir o tráfego gerado pela aplicação, sem no entanto oferecer garantias de desempenho.

Já no caso de aplicações de tempo real, a diminuição da largura de banda disponível ou o aumento do atraso podem inviabilizar a sua operação. Neste caso, a rede necessita de reservar recursos para as aplicações de modo que, mesmo em momentos de maior carga na rede, os requisitos mínimos de desempenho destas aplicações sejam atendidos, ou seja, a rede deve fornecer um serviço com garantias de qualidade de serviço (QoS - *Quality of Service*).

A recomendação E.800 do ITU-T define Qualidade de Serviço (QoS) como:

"*O efeito coletivo do desempenho de um serviço que determina o grau de satisfação de um utilizador desse serviço*".

Esta é uma definição subjetiva, uma vez que associa a qualidade de serviço à perceção que o utilizador tem do serviço. Por outro lado, existem parâmetros objetivos que permitem quantificar a qualidade de serviço oferecida por um sistema de comunicação.

No contexto das redes de comunicação, os parâmetros objetivos[5] de qualidade de serviço [Chal99] podem ser classificados em três domínios: tempo, débito e fiabilidade, conforme indicado na Tabela 3.1.

Tabela 3.1: Domínios e parâmetros objetivos de qualidade de serviço.

Domínio	**Parâmetro (exemplos)**	**Descrição**
Tempo	Atraso	Tempo que os dados demoram a atravessar a rede de comunicação desde o emissor até o recetor.
	Jitter	Variação do atraso sofrido pelos pacotes que percorrem a rede.
Débito	*Throughput*	Débito bruto (incluindo cabeçalhos do protocolo).
	Goodput	Débito útil (considera apenas os dados transferidos pela camada).
Fiabilidade	PER	Packet Error Rate.
	Delivery ratio	Proporção das mensagens geradas no emissor que chegam sem erros ao receptor.

No domínio do tempo, os principais parâmetros são o atraso (ou latência) e o *jitter*. O atraso é o intervalo de tempo que os dados demoram para percorrer a rede desde o emissor até o recetor. Quanto maior o atraso, maior é a quantidade de dados em trânsito na rede, e menor é a interatividade

O atraso total é composto por diversos componentes ao longo do percurso dos dados:

[5] Em oposição aos parâmetros subjectivos associados à percepção da qualidade de serviço por parte do utilizador.

- **Atraso de envio.** Atraso desde que os dados são enviados pela camada de aplicação até chegarem à camada MAC. É não determinístico, pois depende de tempos de processamento associados a diferentes tarefas do sistema operativo.
- **Atraso em fila de espera** (*queuing delay*). Pode ocorrer no emissor ou em nós intermédios, em redes *multihop*.
- **Atraso no acesso ao meio** (*access delay*). Tempo que demora desde que o pacote chega à camada MAC até que começa a ser transmitido no canal. Este atraso é não determinístico em protocolos MAC baseados em contenção, sendo determinístico em protocolos baseados em TDMA fixo.
- **Tempo de transmissão.** Tempo que o pacote demora a ser transmitido no canal, do primeiro ao último bit. É um atraso determinístico, sendo calculado pela expressão $T_{tx} = L / R$, em que L é o tamanho do pacote, em bits, e R é o débito da rede.
- **Atraso de propagação.** É um atraso determinístico expresso por $T_p = d / c$, em que d é a distância entre o emissor e o recetor e c é a velocidade da luz no meio.
- **Atraso de receção.** Análogo ao atraso de envio, mas no recetor. Atraso desde que os dados são enviados pela camada MAC até chegarem à camada de aplicação. É não determinístico, dependendo de tempos de processamento associados a diferentes tarefas do sistema operativo.

O *jitter* consiste na variação do atraso sofrido pelos pacotes no percurso entre o emissor e o recetor. Valores elevados de *jitter* podem causar *timeout* no protocolo de transporte, dificultando a sua ação. Em aplicações não interativas, o *jitter* pode ser suavizado com o uso de um *playback buffer* colocado no recetor (ou em nós intermédios), configurado para um valor de atraso máximo. Em aplicações de tempo-real, os pacotes recebidos com um atraso superior ao atraso máximo (*deadline*) são descartados. A Figura 3.1 apresenta um exemplo de gráfico da distribuição de atrasos de um fluxo de dados recolhido de uma rede IEEE 802.11, no qual se pode observar o *jitter*.

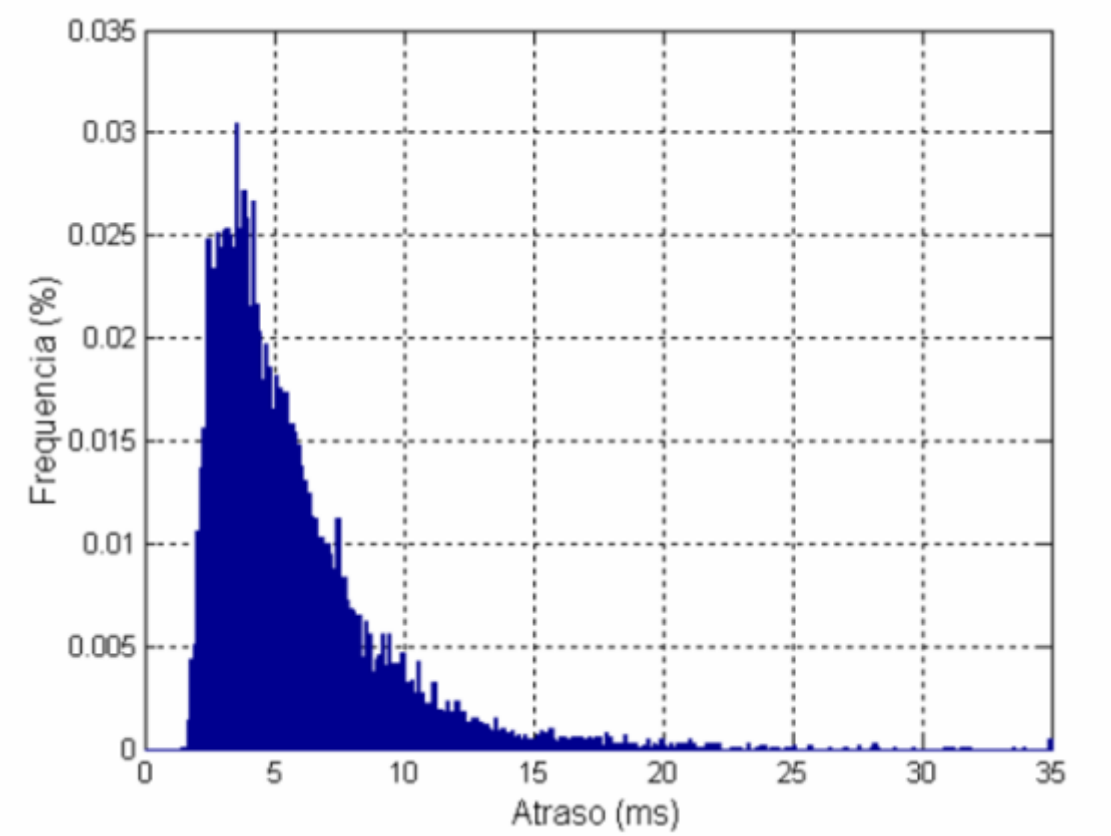

Figura 3.1 - Exemplo de gráfico da distribuição de atrasos de um fluxo de dados.

O débito consiste na taxa de transferência de dados entre o emissor e o recetor. O débito máximo que se pode obter está limitado pelo débito da rede. O débito de um fluxo também pode ser afetado pelos outros fluxos que partilham a rede. As aplicações elásticas conseguem adaptar o seu tráfego ao débito oferecido pelo canal, as inelásticas não, pelo que estas podem sofrer severa degradação da qualidade de serviço se o débito oferecido pela rede for inferior ao débito do tráfego gerado pela aplicação.

Do ponto de vista das redes, convém distinguir três tipos de débito:

- **Débito da rede ou canal:** Corresponde à cadência com que os bits de dados são transmitidos no meio físico. É o limite máximo para o débito do fluxo de dados, que nunca é atingido devido ao *overhead* introduzido pelos protocolos da rede. O *overhead* de um protocolo inclui, por exemplo, os intervalos entre os pacotes e os cabeçalhos. Se o tráfego transportado pela

rede estiver a ser repartido com outros fluxos, o débito obtido será ainda menor.

- **Débito bruto (*throughput*):** É o débito dos pacotes transmitidos, ou seja, o número total de bits transmitidos em vários pacotes dividido pelo tempo decorrido. Não faria sentido utilizar o tempo decorrido na transmissão de um só pacote, visto que neste caso o débito obtido seria igual ao débito da rede. Porém, como existem intervalos entre a transmissão dos pacotes (necessários para a operação dos protocolos), a consequência é que o débito bruto é inferior ao débito de rede.
- **Débito efetivo (*goodput*):** Corresponde ao débito útil, ou seja, o débito efetivamente disponível para a aplicação. Neste caso, em vez de se incluir todos os bits dos pacotes no cálculo do débito como no caso anterior, considera-se apenas os bits de dados (o payload) dos pacotes, ou seja, não se considera os bits dos cabeçalhos e trailers.

Fiabilidade é a medida da capacidade de entrega dos dados no recetor da mesma forma como foram entregues à rede pelo emissor. Parâmetros relevantes nesta categoria incluem o BER (*Bit Error Rate*) a nível da camada física, e o delivery ratio, o PER (*Packet Error Rate*) e o PLR (*Packet Loss Rate*) em camadas superiores. Em aplicações intolerantes a erros, a perda de pacotes exige a retransmissão dos dados, o que aumenta o atraso. Em aplicações tolerantes a erros, a perda de pacotes provoca degradação do serviço. Para aumentar a fiabilidade dos sistemas de comunicação, foram concebidas diversas técnicas de controlo de erros. Algumas destas técnicas são descritas na secção 3.3.

Parâmetros objetivos de qualidade de serviço permitem quantificar o desempenho fornecido pela rede. Numa rede que ofereça garantias de qualidade de serviço, esses parâmetros servem de base para a negociação, entre as aplicações e a rede, de limites mínimos de desempenho a serem satisfeitos pela rede, independentemente da carga. Esses limites podem ser especificados de forma determinística, por exemplo, pela garantia de um débito superior a 100 kbit/s para o fluxo durante o seu tempo de vida; ou probabilística,

por exemplo, pela garantia de um atraso inferior a 50 ms para 99% dos pacotes.

Para que possa oferecer garantias de desempenho para uma aplicação, a rede deve reservar recursos para o respetivo fluxo. A quantidade de recursos a reservar depende da intensidade de tráfego gerado, pelo que a rede deve ser informada dos parâmetros de tráfego que a aplicação se propõe a respeitar. Caso a aplicação exceda os limites de tráfego negociados, a rede pode optar por armazenar os pacotes em excesso até estarem em conformidade com o contrato, marcá-los como tendo baixa prioridade para que sejam descartados mais adiante na rede em caso de congestionamento, ou mesmo descartá-los.

No contexto dos protocolos MAC, duas abordagens diferentes de suporte de QoS podem ser adotadas.

- **Diferenciação de serviços:** Neste caso, o tráfego que circula na rede é separado em classes de tráfego, e diferentes prioridades são associadas a cada classe. Essas prioridades permitem que algumas estações tenham maior probabilidade de aceder ao meio do que outras, em função do tráfego que desejam transmitir. Esta abordagem permite oferecer diferentes níveis de qualidade de serviço para diferentes classes de tráfego, porém, as conexões de uma mesma classe não são protegidas umas das outras, pelo que o comportamento agressivo de uma conexão afecta desfavoravelmente as outras na mesma classe. Mesmo o tráfego de menor prioridade pode afetar a qualidade de serviço das conexões de maior prioridade, dependendo da carga na rede e dos parâmetros do protocolo utilizado.
- **Garantias de qualidade de serviço:** Neste caso, as garantias de qualidade de serviço são fornecidas através de um cuidadoso processo de controlo de admissão de conexões e escalonamento das transmissões, sendo possível satisfazer requisitos de qualidade de serviço por conexão individual. A operação deste tipo de protocolos requer a presença de uma entidade denominada controlador central (CC, *Central Controller*), responsável pelo escalonamento de tráfego e pela reserva de recursos.

A classificação das classes de tráfego e dos parâmetros de qualidade de serviço varia para diferentes organizações internacionais, como o ATM Forum, a ITU, o IETF, o IEEE e o 3GPP [McD98] [IEEE98] [IET97] [3GPP01]. A classificação adotada nas redes ATM é uma das mais completas, sendo por isso apresentada como exemplo na próxima secção.

3.1.1 Qualidade de serviço em redes ATM

A tecnologia ATM (*Asynchronous Transfer Mode*) foi concebida desde o início tendo em vista a integração e suporte de serviços com diferentes características e requisitos de qualidade de serviço numa mesma rede de comunicação. Na fase de estabelecimento de conexão, a aplicação negoceia com a rede um contrato onde são especificados a categoria de serviço desejada e os respetivos parâmetros de tráfego e de QoS.

Os parâmetros de tráfego especificam os limites impostos à fonte para o tráfego injetado na rede, sendo utilizados para verificação de conformidade do fluxo de células:

- ***Peak Cell Rate* (PCR):** É o limite superior para o débito da fonte, sendo definido como o inverso do intervalo mínimo entre as células geradas na interface entre as camadas ATM e física.
- ***Sustained Cell Rate* (SCR):** Representa o limite superior para o débito médio do fluxo.
- ***Minimum Cell Rate* (MCR):** É o débito mínimo garantido, aplicável para a categoria de tráfego ABR (*Available Bit Rate*).
- ***Maximum Burst Size* (MBS):** Corresponde ao número máximo de células consecutivas que podem ser transmitidas ao débito máximo (PCR).
- ***Cell Delay Variation Tolerance* (CDVT)**: Especifica a variação em relação ao instante nominal de inserção de células na rede pela fonte.

Os parâmetros de QoS, por outro lado, definem os requisitos que a rede deve satisfazer no que respeita à qualidade de serviço oferecida:

- ***Cell Transfer Delay* (CTD):** É o tempo decorrido entre a injeção de uma célula na rede por parte da fonte e a sua entrega ao destinatário.
- ***Cell Delay Variation* (CDV):** Exprime a diferença ente os valores máximo e mínimo do CTD.
- ***Cell Loss Ratio* (CLR):** Expressa a relação entre o número de células que podem perder-se durante o trânsito na rede (por exemplo, devido a congestionamento) e o número total de células do fluxo.
- ***Cell Error Rate* (CER):** Expressa a relação entre o número de células afetadas por erros e o número total de células.
- ***Cell Misinsertion Rate* (CMR):** Corresponde à taxa de células inseridas num fluxo e que pertencem a outros fluxos, ou seja, que são incorretamente encaminhadas.
- ***Severely Errored Cell Block Ratio* (SECBR):** Exprime a relação entre o número de blocos severamente corrompidos e o número total de blocos.

As categorias de serviço definidas pelo ATM Forum tem implicação na forma como os parâmetros de tráfego e de QoS são utilizados:

- ***Constant Bit Rate* (CBR):** Destina-se a aplicações de tempo real de débito constante com requisitos exigentes quanto a atrasos e perdas. O débito é caracterizado pelo parâmetro PCR, o atraso pelos parâmetros CTD e CDV e as perdas pelo parâmetro CLR. A rede reserva recursos correspondentes ao PCR mesmo que a aplicação transmita a um débito inferior. Esta categoria é utilizada para emulação de circuitos e transmissão de tráfego de voz, áudio e vídeo de débito fixo.
- ***Real-Time Variable Bit Rate* (rt-VBR):** Esta categoria destina-se a aplicações de tempo real de débito variável com restrições temporais. As conexões desta categoria são caracterizadas pelos parâmetros PCR, SCR, MBS, CLR, CTD e CDV. Esta categoria destina-se principalmente a aplicações multimédia, como o transporte de vídeo e áudio interativos.
- ***Non-Real-Time Variable Bit Rate* (nrt-VBR):** Esta categoria à semelhante à anterior, porém não apresenta as restrições temporais, sendo

caracterizada pelos parâmetros PCR, SCR, MBS e CLR. É adequada para serviços de transporte de áudio e vídeo sem interatividade.

- ***Unspecified Bit Rate* (UBR):** Esta categoria é utilizada para o transporte de tráfego do tipo melhor esforço, não sendo oferecidas nenhumas garantias de qualidade de serviço.
- ***Available Bit Rate* (ABR):** Nesta categoria não são dadas quaisquer garantias quanto ao atraso, mas garante-se um débito mínimo (MCR), bem como uma taxa de perdas pequena caso a fonte adapte o seu débito de acordo com a informação de controlo de fluxo enviada pela rede no sentido inverso.

3.2 Escalonamento de tráfego

Quando pacotes associados a diferentes fluxos partilham um mesmo recurso, como, por exemplo, a saída de um multiplexador, torna-se necessário utilizar um algoritmo de escalonamento [Kesh97] para determinar a ordem em que os pacotes são servidos. No algoritmo de escalonamento mais simples, denominado FCFS (*First Come First Served*), os pacotes dos diferentes fluxos são colocados numa mesma fila de espera, na ordem em que chegam, e são servidos nessa mesma ordem. Este algoritmo, porém, não é capaz de oferecer justiça, proteção entre os fluxos ou garantias de qualidade de serviço.

Para superar essas deficiências, diversos outros algoritmos de escalonamento foram propostos na literatura. Os algoritmos concebidos para o escalonamento de tráfego assíncrono são, na sua maioria, baseados no algoritmo ideal denominado GPS (*Generalized Processor Sharing*), também conhecido pela designação FFQ (*Fluid Fair Queuing*). Em termos lógicos, o FFQ mantém uma fila de espera por cada fluxo, e visita as filas ocupadas em sequência, servindo uma quantidade infinitesimal de dados de cada fila, de modo que, num intervalo de tempo finito, cada fila é visitada pelo menos uma vez. Aos fluxos podem ser associados diferentes pesos, o que permite que a quantidade de dados servida de um dado fluxo seja proporcional ao respetivo peso quando há dados na fila de espera.

Uma forma simples de implementar o algoritmo FFQ é através de rotação (*round-robin*). As filas de espera são servidas em sequência, como no FFQ, porém, este esquema serve um pacote de cada vez, e não uma quantidade infinitesimal de dados. A rotação é uma boa aproximação do algoritmo FFQ quando os fluxos têm o mesmo peso e os pacotes têm o mesmo tamanho. O algoritmo WRR (*Weighted Round-Robin*) é uma variação da rotação que serve os fluxos na proporção dos seus pesos.

O WFQ (*Weighted Fair Queueing*) é um algoritmo que implementa melhor os critérios definidos pelo FFQ, nomeadamente quando os pacotes são de tamanho variável, mas com uma maior complexidade que a do WRR. O algoritmo WFQ calcula o instante em que cada pacote teria o seu serviço terminado, caso o algoritmo GPS fosse usado, e identifica os pacotes com os números calculados, servindo-os na ordem determinada por esses identificadores.

O algoritmo WFQ também pode ser utilizado com tráfego de tempo real. Entretanto, quanto menor o atraso desejado para a conexão, maior terá de ser a largura de banda reservada, mesmo que não seja utilizada [Kesh97]. Como no meio sem fios a largura de banda é um recurso escasso, este algoritmo de escalonamento não é muito indicado para lidar com tráfego com requisitos de reduzido atraso em redes de comunicação sem fios.

Para o escalonamento de tráfego de tempo real, existem outras alternativas, como o EDD (*Earliest Due Date*), também conhecido como EDF (*Earliest Deadline First*). No EDD, atribui-se um prazo de validade (*deadline*) a cada pacote e o escalonador serve os pacotes pela ordem dos seus prazos de validade. Neste algoritmo, um pacote, ao qual é atribuído um prazo mais próximo do instante de chegada sofre um atraso menor na fila de espera do que outro ao qual tenha sido atribuído um prazo mais distante. Dependendo da carga, pode não ser possível servir todos os pacotes antes de se atingir os respetivos prazos que lhes foram atribuídos.

3.3 Controlo de erros

Existem diversas técnicas de controlo de erros [Vars99] [Liu97] que procuram minimizar os efeitos dos erros no canal sobre a informação transmitida, à custa do aumento do *overhead*. O controlo de erros pode ser aplicado em diferentes camadas: física, de ligação de dados, de transporte ou de aplicação. Os critérios que condicionam a escolha das técnicas de controlo de erros a empregar numa rede sem fios incluem a largura de banda disponível, o padrão de erros no canal, o tempo de propagação entre o emissor e o recetor, a existência de um canal de retorno, e as possíveis limitações de memória, autonomia e capacidade de processamento das estações. A seguir, descrevem-se algumas das técnicas de controlo de erros utilizadas em redes sem fios.

3.3.1 Equalização

A técnica de equalização é utilizada para compensar a distorção no sinal provocada pela interferência intersimbólica (ISI). O recetor calcula os parâmetros a utilizar na equalização com base nas alterações de amplitude e fase sofridas por uma sequência de treino conhecida, transmitida pelo emissor. Como as características do canal sem fios tendem a variar com o tempo, os parâmetros utilizados na equalização têm que ser constantemente atualizados, pelo que a sequência de treino costuma ser repetida sempre que há uma transmissão.

3.3.2 Diversidade

Nesta técnica, a mesma informação é recebida através de diversas vias independentes. Com isso, a probabilidade de que todas as versões da informação sejam corrompidas por erros é pequena. A diversidade de vias pode ser implementada de várias formas: diversidade temporal, de frequências, de antenas ou de polarização. As duas primeiras técnicas requerem largura de banda extra para a transmissão das diferentes versões,

pelo que a sua utilização não é muito difundida em redes sem fios, nas quais a largura de banda é um recurso escasso. Para que um sistema beneficie da diversidade de antenas, os sinais devem apresentar baixa correlação, o que implica que as antenas devem estar separadas de pelo menos metade do comprimento de onda da portadora. Esta técnica é utilizada principalmente no combate ao desvanecimento multipercurso.

3.3.3 Correção antecipada de erros

A técnica de correção de erros FEC (*Forward Error Correction*) baseia-se na transmissão de informação redundante pelo emissor, de modo a habilitar o recetor a corrigir os erros nas mensagens recebidas. A técnica de correção de erros tradicional não adapta dinamicamente o nível de redundância às condições variáveis do canal, pelo que a largura de banda pode ser desperdiçada devido ao *overhead* da técnica de correção de erros quando as condições do canal são boas. Por outro lado, o nível de redundância pode ser insuficiente para corrigir os erros quando as condições são más.

Quando os erros introduzidos pelo canal resultam dum estado de perturbação de duração relativamente curta, a técnica de entrelaçamento (*interleaving*) possibilita a aplicação eficaz da técnica de correção de erros, ao espalhar os erros que normalmente estariam concentrados em poucos bits. Uma desvantagem da técnica de entrelaçamento é que a sua utilização provoca o aumento do atraso.

3.3.4 Deteção de erros e retransmissão

Na técnica de deteção de erros e retransmissão (ARQ - *Automatic Repeat reQuest*), o emissor inclui em cada pacote um campo destinado à deteção de erros, baseado, por exemplo, em CRC (*Cyclic Redundancy Check*). O valor deste campo é calculado em função da informação contida no pacote, e permite ao recetor detetar se o pacote foi corrompido por erros no canal. Em caso positivo, o recetor requisita ao emissor a retransmissão do pacote, seja de forma explícita, pelo envio de uma mensagem de reconhecimento negativo

(NAK), ou de forma implícita, pelo não envio de uma mensagem de reconhecimento positivo (ACK), num intervalo de tempo estabelecido a seguir à receção do pacote.

Esta técnica é mais adaptável às condições variáveis do canal do que a técnica de correção de erros, porque o seu nível de redundância, expresso pela razão entre retransmissões e transmissões, não é fixo. Por outro lado, a técnica de deteção de erros e retransmissão necessita de um canal de retorno, que não é necessário na técnica de controlo de erros.

A utilização da técnica de deteção de erros e retransmissão não é aconselhável para a transmissão de tráfego de tempo real quando o tempo de propagação é elevado ou quando o débito de transmissão é pequeno, porque o atraso cumulativo das retransmissões pode fazer com que o atraso final exceda o valor máximo aceitável. Por outro lado, esta técnica é mais fiável do que a correção de erros para transmissão de tráfego intolerante a erros, pois permite que as retransmissões sejam realizadas até que a informação seja recebida corretamente.

3.3.5 *Hybrid* ARQ (HARQ)

Estes esquemas combinam a correção de erros com a retransmissão de pacotes. Existem três tipos básicos de esquemas HARQ [Alme02]. No HARQ tipo I, os pacotes incluem um código de correção de erros. Se este não for suficiente para corrigir os erros no pacote, o recetor requisita a retransmissão do mesmo. Nos esquemas HARQ tipo II e III, introduz-se redundância nos pacotes retransmitidos para correção de erros. A diferença é que, no HARQ tipo II, o pacote original inclui um código de deteção de erros (como no ARQ), enquanto no HARQ tipo III o pacote original contém um código de correção de erros (como no HARQ tipo I).

Referências

[3GPP01] 3GPP Doc. 3G TS 23.107 v3.1.0, “QoS Concept and Architecture”, September 2001.

[Alme02] J. N. T. Almeida, “High-Speed Wireless Mobile LAN Communications: Improved Error Control Mechanisms for Real-Time Services”, PhD thesis, Universidade do Porto, June 2002.

[Chal99] D. Chalmers and M. Sloman, “A Survey of Quality of Service in Mobile Computing Environments”, *IEEE Communications Surveys*, Second Quarter 1999.

[Kesh97] S. Keshav, “An Engineering Approach to Computer Networking, Chapter 9: Scheduling”, Addison-Wesley, 1999.

[IEEE98] IEEE 802.1D, “IEEE standard for local and metropolitan area networks - Common specifications - Media access control (MAC) Bridges”, 1998.

[IET97] J. Wroclawski, “The Use of RSVP with IETF Integrated Services”, IETF RFC2210, September 1997.

[Liu97] H. Liu, H. Ma, M.E. Zarki and S. Gupta, “Error control schemes for networks: An Overview”, Mobile Networks and Applications, Vol. 2, No. 2, pp. 167-182, 1997.

[McD98] D. E. McDysan and D. L. Spohn, “ATM Theory and Application”, McGraw-Hill, 1998.

[Vars99] U. Varshney, “Error Control Techniques for Wireless ATM Networks”, IEEE International Performance Computing and Communications Conference IPCCC’99, Phoenix, Arizona, USA, pp. 104-110, February 1999.

4. Controlo de acesso ao meio

4.1 Técnicas de acesso múltiplo

A largura de banda disponível para a operação de uma rede de comunicação sem fios pode ser partilhada por entre as suas estações de quatro modos básicos associados a quatro domínios distintos: **frequência**, **tempo**, **código** e **espaço**. A cada um destes domínios é associada uma técnica de acesso múltiplo respetiva [Rubi97].

- **Acesso Múltiplo por Divisão de Frequência** (FDMA - *Frequency Division Multiple Access*): Nesta técnica a largura de banda disponível é repartida em múltiplas bandas de frequências (canais), cada qual com a sua portadora. As estações transmitem em bandas diferentes, possibilitando a ocorrência de múltiplas transmissões simultâneas no meio.
- **Acesso Múltiplo por Divisão de Tempo** (TDMA - *Time Division Multiple Access*): Nesta técnica as estações partilham a mesma banda de frequências. Neste caso, se duas ou mais estações transmitirem em simultâneo, normalmente não é possível descodificar o sinal de nenhuma delas. Sendo assim, esta técnica procura fazer com que as transmissões das diferentes estações ocorram em períodos distintos, de modo a evitar colisões.
- **Acesso Múltiplo por Divisão de Código** (CDMA - *Code Division Multiple Access*): Nesta técnica o sinal de cada estação da rede é codificado com um código diferente antes da transmissão. Isso possibilita que as estações possam transmitir ao mesmo tempo utilizando a mesma banda de frequências. Com base no código usado pelo emissor, o recetor é capaz de descodificar corretamente o sinal da estação desejada, mesmo na presença de outras transmissões. No entanto, a codificação utilizada neste caso faz com que a largura de banda necessária para a transmissão do

sinal codificado seja maior do que a necessária para a transmissão do sinal original.

- **Acesso Múltiplo por Divisão de Espaço** (SDMA - *Space Division Multiple Access*): Como a intensidade do sinal transmitido no espaço decresce com o aumento da distância, a mesma banda de frequências pode ser utilizada em comunicações simultâneas, desde que as estações recetoras estejam próximas das respetivas estações transmissoras mas suficientemente afastadas das outras estações transmissoras para que estas não causem interferência significativa. As redes celulares aproveitam-se da dimensão espacial para distribuírem as bandas de frequências atribuídas para a operação da rede por áreas específicas (células) segundo padrões geométricos apropriados, possibilitando assim a reutilização dessas frequências. Outra forma de explorar a dimensão espacial consiste na divisão de uma célula em múltiplos setores (como fatias de uma piza), aliada à utilização de antenas diretivas. Esta estratégia permite a coexistência de múltiplas transmissões em simultâneo na mesma banda de frequências na mesma célula.

A utilização da técnica de acesso múltiplo por divisão de frequência (FDMA) apresenta algumas desvantagens. Uma delas é a pouca flexibilidade na alocação dinâmica de largura de banda às estações de acordo com as suas necessidades, o que é mais problemático quando o tráfego das aplicações possui débito variável. Outra desvantagem consiste na sensibilidade dos sinais transmitidos à interferência de banda estreita.

As redes celulares móveis de primeira geração eram baseadas em FDMA e empregavam tecnologia analógica. Na migração para as redes celulares móveis de segunda geração, baseadas em tecnologia digital, o FDMA deixou de ser a técnica de acesso múltiplo principal, dando lugar ao TDMA e ao CDMA.

A técnica de acesso múltiplo por divisão de tempo (TDMA) possibilita uma maior flexibilidade na alocação de largura de banda para as diferentes estações, quando comparada à técnica de FDMA. Por outro lado, como no

TDMA as estações transmitem sequencialmente, e não em simultâneo, o débito de transmissão utilizado tem que ser mais elevado, pois a mesma quantidade de dados tem que ser transmitida num período menor, o que tende aumentar a interferência intersimbólica (ISI). A modulação OFDM (*Orthogonal Frequency Division Multiplexing*) [Rohl99], utilizada em redes locais sem fios de alto débito, consegue reduzir a interferência intersimbólica através da conversão do fluxo de dados de alto débito da estação em múltiplos fluxos paralelos de mais baixo débito, que são utilizados para modular um igual número de portadoras ortogonais entre si.

O TDMA é utilizado por praticamente todas as redes sem fios de área local e pessoal no mercado, bem como em grande parte das redes celulares móveis de segunda geração, como por exemplo o GSM. O TDMA também é usado, a par do CSMA, em redes de acesso fixo sem fios de banda larga e redes celulares móveis de terceira geração.

Nas redes sem fios baseadas em TDMA com comunicação centralizada, existem duas opções para a multiplexação das transmissões feitas nos sentidos ascendente (*uplink*) e descendente (*downlink*), denominadas técnicas de *duplex*. Na técnica de divisão na frequência (FDD - *Frequency Division Duplex*), uma banda de frequências é alocada para o tráfego no sentido ascendente e outra para o tráfego no sentido descendente. Já na técnica de divisão no tempo (TDD - *Time Division Duplex*), o tráfego nos dois sentidos é multiplexado no tempo, ocupando a mesma banda de frequências. A técnica de TDD é mais eficiente quando a proporção de tráfego nos dois sentidos é variável.

Existem dos tipos básicos de acesso múltiplo por divisão de código (CDMA), consoante a técnica de espalhamento espectral[6] (SS - *Spread Spectrum*) [Glis97] que é aplicada:

[6] Algumas redes locais e pessoais sem fios, como por exemplo as redes assentes nas normas IEEE 802.11 e IEEE 802.15.4, utilizam o espalhamento espectral para poderem operar sem licença em bandas ISM (*Industrial, Scientific and Medical*), ao mesmo tempo que

- **CDMA por saltos em frequência** (FH-CDMA - *Frequency Hopping CDMA*): Nos sistemas baseados em FH-CDMA, a frequência da portadora no emissor sofre variações discretas e periódicas (dentro de uma banda de frequências predefinida) em função da sequência (código) usada pelo modulador. Para recuperar o sinal modulante, o recetor aplica a mesma sequência, em fase, no desmodulador.
- **CDMA por sequência direta** (DS-CDMA - *Direct Sequence CDMA*): Nos sistemas baseados em DS-CDMA (normalmente de implementação mais complexa), cada bit do sinal é modulado por uma sequência de *chips*[7]. Com isso, o sinal resultante é espalhado por uma banda muito maior do que a necessária para transmitir o sinal original. O recetor utiliza a mesma sequência pseudo-aleatória adotada pelo emissor para a recuperação do sinal original.

Quando os códigos utilizados pela técnica de CDMA são ortogonais, as transmissões não interferem entre si, mas existe um limite rígido no número máximo de utilizadores que o sistema pode suportar. Já quando os códigos não são ortogonais, não há um limite estrito no número máximo de utilizadores, mas o sistema fica sujeito à interferência mútua entre as fontes, que aumenta linearmente com o número de utilizadores no sistema [Sari00].

Um problema associado ao DS-CDMA, conhecido pela designação *near-far effect*, é que o recetor tem dificuldade de descodificar o sinal desejado de um emissor mais distante quando está a sofrer interferência de outro sinal mais forte de um emissor mais próximo. A resolução deste problema requer a implementação de um mecanismo de controlo dinâmico da potência de transmissão (TCP - *Transmit Power Control*), normalmente baseado em

beneficiam da sua robustez. No entanto, as estações que fazem parte da rede partilham todas o mesmo código de espalhamento espectral. Sendo assim, nessas redes o acesso múltiplo não é baseado em CDMA, mas sim em TDMA.

[7] Os bits num código de espalhamento espectral por sequência direta recebem a denominação de *chips*.

informação sobre o nível de sinal fornecida pelo recetor, com o objetivo de fazer com que os sinais transmitidos por diferentes emissores cheguem ao recetor com a mesma intensidade, independentemente da distância, possibilitando assim a descodificação correta do sinal CDMA desejado. O DS-CDMA é utilizado nalgumas redes celulares móveis de segunda geração e em diversas redes da terceira geração em diante.

4.2 Protocolos de controlo de acesso ao meio

Esta secção aborda o controlo de acesso ao meio do ponto de vista das redes baseadas em acesso múltiplo por divisão do tempo (TDMA), visto que a quase totalidade das redes de área local e pessoal existentes atualmente operam com base no princípio da divisão do tempo.

Num meio partilhado por diversas estações, quando as transmissões de duas ou mais estações sobrepõem-se num recetor, mesmo que parcialmente, normalmente os pacotes são corrompidos por erros, impedindo a sua correta receção. Neste caso, diz-se que ocorreu uma colisão. A retransmissão de pacotes corrompidos aumenta a carga na rede, o que colabora para o aumento da frequência de colisões. Este processo, se não for controlado, pode tender para o colapso da rede, inviabilizando completamente a comunicação entre as estações. Sendo assim, é necessário que a rede implemente um mecanismo de controlo de acesso ao meio (MAC - *Medium Access Control*) de modo a disciplinar o acesso das estações ao meio e procurar minimizar ou mesmo eliminar a possibilidade de colisões, de forma a melhorar o desempenho do sistema.

4.2.1 Critérios de avaliação de desempenho

Uma grande variedade de protocolos de controlo de acesso ao meio tem sido proposta na literatura [Chan00]. Um dos principais critérios para avaliação desses protocolos é o suporte de qualidade de serviço (QoS) oferecido. Neste sentido, duas abordagens diferentes podem ser adotadas:

- Diferenciação de serviços;
- Garantias de qualidade de serviço.

Grande parte dos protocolos de controlo de acesso ao meio adotados pelas primeiras redes locais não oferecia suporte de qualidade de serviço, proporcionando apenas um serviço do tipo melhor esforço. Estes protocolos geralmente procuram minimizar o atraso médio dos pacotes, desde o instante em que são colocados na fila de espera do emissor até ao momento em que são entregues com sucesso ao recetor. No entanto, o atraso médio de todos os fluxos de informação tende a aumentar à medida que aumenta a carga global na rede.

Outros critérios utilizados para avaliar o desempenho dos protocolos de controlo de acesso ao meio são a eficiência, a justiça, a escalabilidade e o consumo de energia.

- **Eficiência:** A eficiência de um protocolo de controlo de acesso ao meio é uma medida do aproveitamento da largura de banda disponível, sendo normalmente expressa pela razão entre o débito útil (*goodput*) e o débito da rede (capacidade). Um protocolo de controlo de acesso ao meio deve procurar maximizar a eficiência sem comprometer a qualidade de serviço oferecida às conexões. Para isso, deve procurar minimizar o *overhead* (tamanho dos cabeçalhos dos pacotes, pacotes de controlo, períodos inativos entre os pacotes) que introduz.
- **Justiça (*fairness*):** Um protocolo de controlo de acesso ao meio é considerado justo se não exibir preferência por nenhuma estação em particular quando múltiplas estações competem pelos recursos, no caso de as diferentes conexões pertencerem a uma mesma classe de tráfego. Entre diferentes classes de tráfego, o protocolo deve atribuir recursos na proporção de suas alocações.
- **Escalabilidade:** A escalabilidade é uma medida da capacidade da rede de permitir o aumento do número de estações e, ao mesmo tempo, continuar a prestar um serviço satisfatório.

- **Consumo de energia:** Minimizar o consumo de energia é importante quando este recurso é escasso, como é o caso das estações que operam com bateria, pois permite aumentar a sua autonomia. O consumo de energia costuma ser um critério ainda mais fundamental na conceção e avaliação de desempenho de protocolos MAC para redes de sensores sem fios, visto que nessas redes muitas vezes não é viável recarregar as baterias das estações.

4.2.2 Classificação dos protocolos MAC

Como foi visto na secção 1.4.3, os protocolos MAC podem ser classificados, no que concerne à coordenação de acesso ao meio, em dois grupos: protocolos com controlo distribuído e protocolos com controlo centralizado. Além da coordenação de acesso ao meio, outras características permitem subdividir os protocolos MAC em seis categorias, sendo três pertencentes ao primeiro grupo e três ao segundo grupo:

- **Controlo distribuído:**
  - Acesso aleatório;
  - Passagem de testemunho;
  - Reserva dinâmica implícita.
- **Controlo centralizado:**
  - *Polling*;
  - Reserva fixa;
  - Reserva dinâmica explícita.

4.2.2.1 *Acesso aleatório*

Nos protocolos pertencentes a esta categoria, as estações competem pelo acesso ao meio de forma distribuída. A decisão sobre o momento de efetuar a transmissão é feita com base em regras que todas as estações que fazem

parte da rede devem seguir, conhecidas pelo nome de “algoritmo de resolução de contenção” (CRA - *Contention Resolution Algorithm*). Sendo assim, o que diferencia os protocolos MAC pertencentes a esta categoria é o algoritmo utilizado.

Os protocolos de acesso aleatório também são chamados protocolos de contenção, em que a palavra contenção (*contention*, em inglês) tem o significado de disputa, no sentido em que pode-se dizer que as estações que estão a executar o algoritmo definido pelo protocolo num dado momento (ou seja, as estações que possuem pacotes pendentes à espera de transmissão) estão a competir pelo acesso ao meio.

O protocolo ALOHA foi o primeiro protocolo de acesso aleatório a ser proposto. O seu princípio de operação é bem simples: quando uma estação tem um pacote pendente para transmissão, transmite-o imediatamente. Depois disso, a estação aguarda durante um período, que tem em conta o tempo de propagação entre emissor e recetor, pela confirmação do recebimento do pacote por parte do recetor. Caso a confirmação não chegue nesse período, o emissor retransmite o pacote (normalmente após um outro período aleatório).

A Figura 4.1 mostra que o período de vulnerabilidade a colisões de um pacote. Tomando o início da transmissão do pacote mais escuro como referência, este pacote fica vulnerável a colisões com outros pacotes que comecem a ser transmitidos no intervalo entre um período t antes e um período t depois, ou seja, durante um intervalo total igual a 2t, em que t é o tempo de transmissão de um pacote. A colisão, mesmo que parcial, de pacotes transmitidos em simultâneo por diferentes estações faz com que os mesmos sejam corrompidos, pelo que a eficiência teórica máxima deste protocolo é muito baixa (cerca de 18 %).

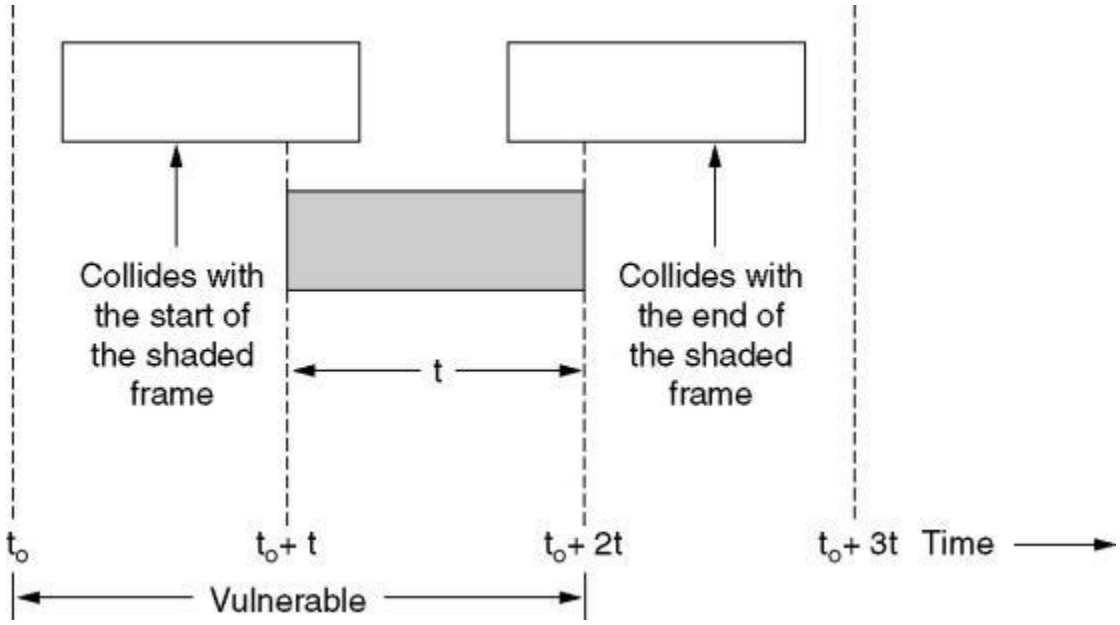

Figura 4.1: Período de vulnerabilidade a colisões de um pacote (pacote mais escuro) no protocolo ALOHA [Tane89].

O protocolo Slotted AHOHA, ou S-ALOHA, é uma variante do protocolo ALOHA na qual o tempo é dividido em *slots* de duração fixa. Quando uma estação quer transmitir um pacote, ela espera pelo início do *slot* seguinte. Isso reduz para metade o período de vulnerabilidade a colisões da transmissão, duplicando a eficiência teórica máxima relativamente ao protocolo ALOHA. Por outro lado, a sua utilização requer a sincronização entre as estações. Este protocolo é usado, por exemplo, na requisição de canais de comunicação em redes celulares móveis.

A Figura 4.2 apresenta um exemplo comparativo do funcionamento dos protocolos ALOHA e Slotted ALOHA. Neste exemplo, o terceiro pacote da estação A consegue evitar a colisão ao adiar o início da transmissão para o *slot* seguinte.

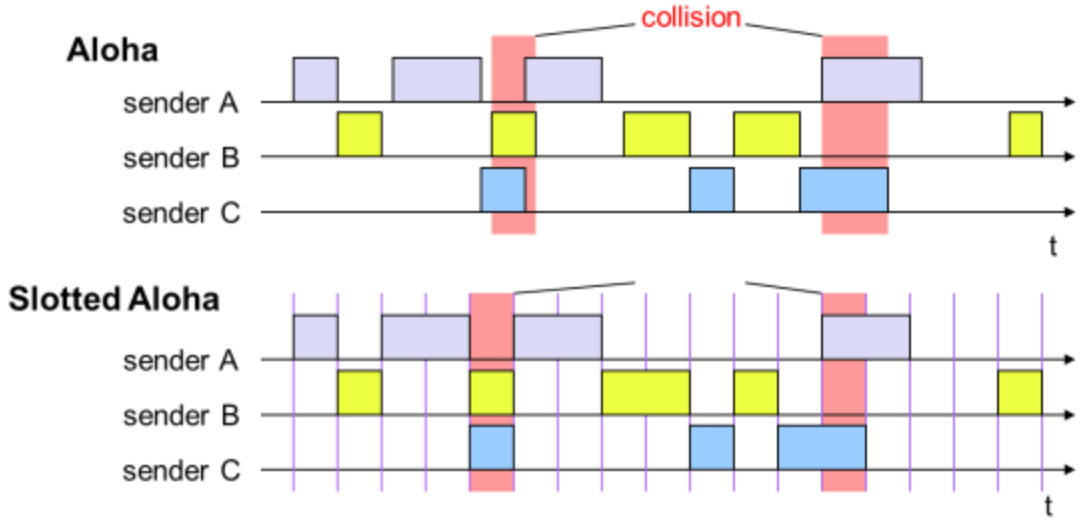

Figura 4.2: Exemplo de funcionamento dos protocolos ALOHA e Slotted ALOHA [Schi04].

A Figura 4.3 apresenta um gráfico eficiência teórica (S) desses protocolos, expressa com base no débito bruto normalizado em relação ao débito de rede, em função da carga na rede (G), ou seja, do tráfego normalizado injetado na rede. Esse resultado teórico assume uma população (número de estações emissoras) infinita, para não haver pacotes bloqueados nas filas de espera das estações, o que diminuiria a carga na rede. Também é assumido que os pacotes têm um tamanho fixo e que são gerados com base na distribuição de Poisson. A Figura 4.4 apresenta a eficiência do protocolo ALOHA, obtida por meio de simulação, utilizando o software OMNeT++ [Varg00]. Neste caso, consegue-se apresentar os resultados para um número variável de estações (nós), ao contrário da análise teórica, que teve que assumir uma população infinita para reduzir a complexidade do problema. A análise por meio de simulação também torna mais simples a obtenção de resultados para outros cenários. Por exemplo, pode-se deixar de assumir que os pacotes têm todos o mesmo tamanho, gerar tráfego com base em outras distribuições, considerar que alguns pacotes são perdidos devido a erros de transmissão, etc.

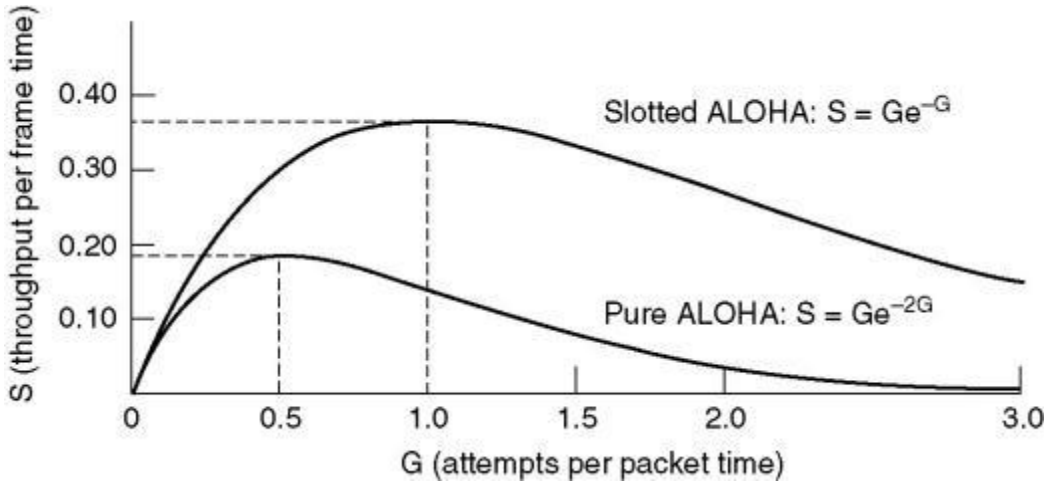

Figura 4.3: Eficiência teórica dos protocolos ALOHA e S-ALOHA [Tane89].

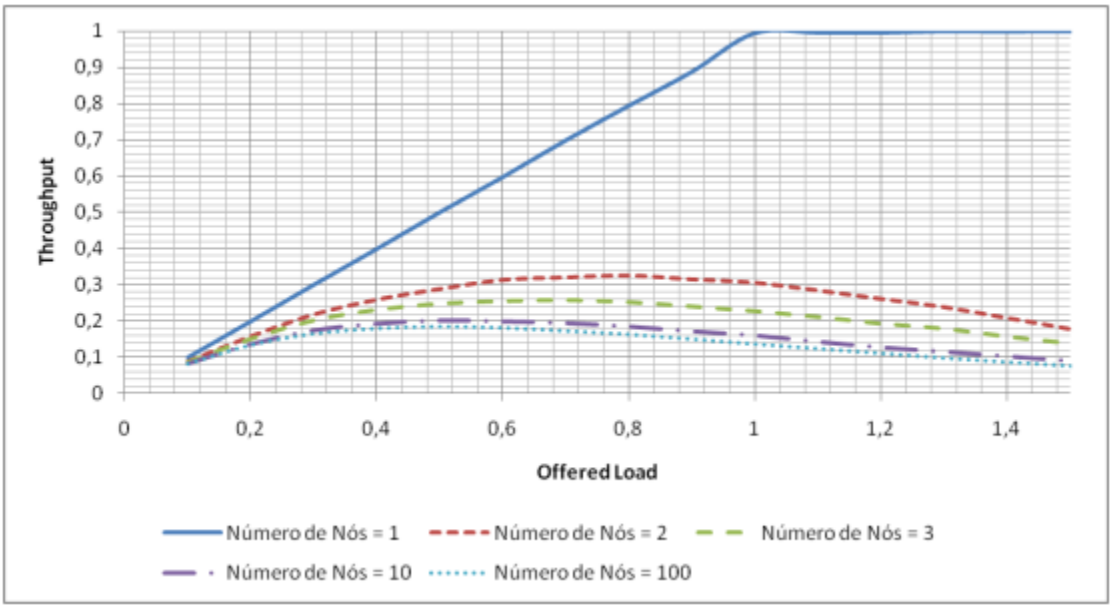

Figura 4.4: Eficiência do protocolo ALOHA para um número variável de estações (nós), obtida por meio de simulação.

Caso o tempo de propagação seja pequeno em comparação com o tempo de transmissão dos pacotes, como no caso das redes de área local, quando uma estação começa a sua transmissão, as outras estações na rede podem ficar a saber quase imediatamente e, desta forma, adiar as suas transmissões de forma a evitar a colisão. Este processo, conhecido como deteção de portadora, está na base do protocolo CSMA (*Carrier Sense Multiple Access*). Este protocolo apresenta um desempenho superior ao do protocolo ALOHA, pois as estações precisam de começar as suas transmissões quase ao mesmo

tempo para que ocorra uma colisão. Apesar disso, a probabilidade de colisões ainda pode ser significativa, nomeadamente quando a carga na rede é elevada.

No protocolo CSMA, quando ocorre uma colisão, o meio fica ocupado até que as estações envolvidas terminem suas transmissões, embora os pacotes envolvidos na colisão sejam descartados. Este desperdício de largura de banda pode ser minimizado caso as estações emissoras interrompam as suas transmissões logo que detectem a ocorrência de colisão. Este procedimento é utilizado pelo protocolo CSMA/CD (*Carrier Sense Multiple Access/Collision Detection*), adotado pela rede Ethernet (IEEE 802.3) [I802.3].

Infelizmente, a deteção de colisões é impraticável nas redes sem fios. Num meio sem fios, quando uma estação transmite, parte do sinal alcança o estágio de receção[8]. Devido à proximidade entre os estágios de transmissão e receção da estação, esta interferência é muito mais forte do que os sinais provenientes de outras estações, inviabilizando a deteção de outras transmissões enquanto a estação transmite. Por isso, as redes sem fios utilizam uma variante do protocolo CSMA conhecida pela denominação CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*), que procura evitar colisões em vez de detectá-las. Diferentes redes sem fios implementam diferentes algoritmos CSMA/CA, adaptados às suas especificidades. Dois exemplos de redes que utilizam protocolos CSMA/CA são as baseadas nas normas IEEE 802.11/Wi-Fi[9] e IEEE 802.15.4.

4.2.2.2 *Polling*

Nas redes que utilizam protocolos de *polling* existe uma estação, conhecida pela designação de mestre, que faz o papel de controlador central, ou seja, regula o acesso ao meio por parte das outras estações, que recebem a

[8] Este fenómeno é denominado *self-interference*.

[9] O protocolo CSMA/CA do IEEE 802.11 é denominado função de coordenação distribuída (DCF - Distributed Coordination Function).

denominação de escravos. Uma estação só pode transmitir após ser interrogada pelo mestre. Juntamente com a interrogação, o mestre pode incluir dados para a estação. Após a resposta da estação, o mestre repete o processo com a estação seguinte na lista de *polling*. A Figura 4.5 exemplifica o funcionamento de um protocolo de *polling*, Na parte de cima da figura estão identificados os pacotes de interrogação enviados pelo mestre. Cada um desses pacotes contém o endereço do escravo ao qual é concedida a autorização de transmissão. Na parte de baixo da figura são apresentados os pacotes de resposta à interrogação enviados pelos respetivos escravos. Caso um escravo não tenha dados para enviar na altura em que é interrogado, o procedimento normal consiste no envio de um pacote sem dados denominado pacote nulo (*null packet*).

A forma mais simples de implementar o escalonamento no protocolo de *polling* consiste em fazer a rotação (*round-robin*) da interrogação por todas as estações presentes na lista de *polling*. No entanto, esta forma de escalonamento não leva em consideração os padrões de tráfego ou os requisitos de qualidade de serviço dos fluxos de dados. Caso seja frequente a situação na qual as estações não tenham dados a transmitir em resposta às interrogações, a eficiência deste protocolo será baixa, devido ao *overhead* associado ao processo de interrogação/resposta. Sendo assim, este protocolo é mais adequado para cenários em que as estações geram tráfego contínuo, em oposição a cenários em que o tráfego gerado é esporádico. Exemplos de redes que utilizam protocolos de *polling* específicos incluem as redes IEEE 802.11[10] e Bluetooth.

[10] O protocolo de *polling* definido pela norma IEEE 802.11 é denominado função de coordenação pontual (PCF - Point Coordination Function).

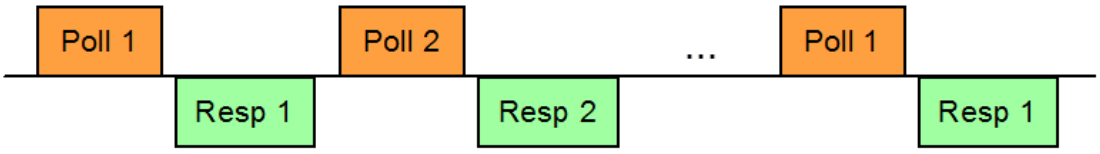

Figura 4.5: Exemplo de funcionamento de um protocolo de *polling*.

4.2.2.3 Reserva fixa

Os protocolos de controlo de acesso ao meio desta categoria operam com base na reserva de canais de transporte (por exemplo, *slots* TDMA) com capacidade fixa. As estações normalmente requisitam estes canais com recurso a um protocolo de acesso aleatório, utilizando para isso canais de sinalização apropriados e distintos dos canais de transporte de dados. Os protocolos de reserva fixa são adequados para o transporte de tráfego de débito constante, mas são ineficientes para o transporte de tráfego de débito variável, pois a largura de banda de um canal não pode ser aproveitada por outros fluxos quando o canal não está a ser usado. Mesmo para cenários de tráfego de débito constante, a flexibilidade para acomodar fluxos de diferentes estações com requisitos de débito diferentes é limitada. A reserva fixa costuma ser usada em redes de comutação de circuitos, como as redes celulares móveis de primeira e segunda geração, para o transporte de tráfego de voz. Exemplos de sistemas baseados em reserva fixa incluem o GSM e o DECT (*Digital Enhanced Cordless Telecommunication*).

A Figura 4.6 apresenta um exemplo de alocação de canais baseado em reserva fixa utilizado pelo sistema de telefonia fixa DECT. Este sistema disponibiliza 10 portadoras alocadas no espectro de frequências. Para cada portadora, o tempo e dividido em tramas sucessivas, cada qual composta por 12 *slots* para tráfego no sentido descendente (da estação base para os telefones sem fios) e 12 *slots* para tráfego ascendente. Cada estação reserva um *slot* descendente em combinação com slot ascendente da mesma portadora (ou seja, este é um sistema baseado em TDD).

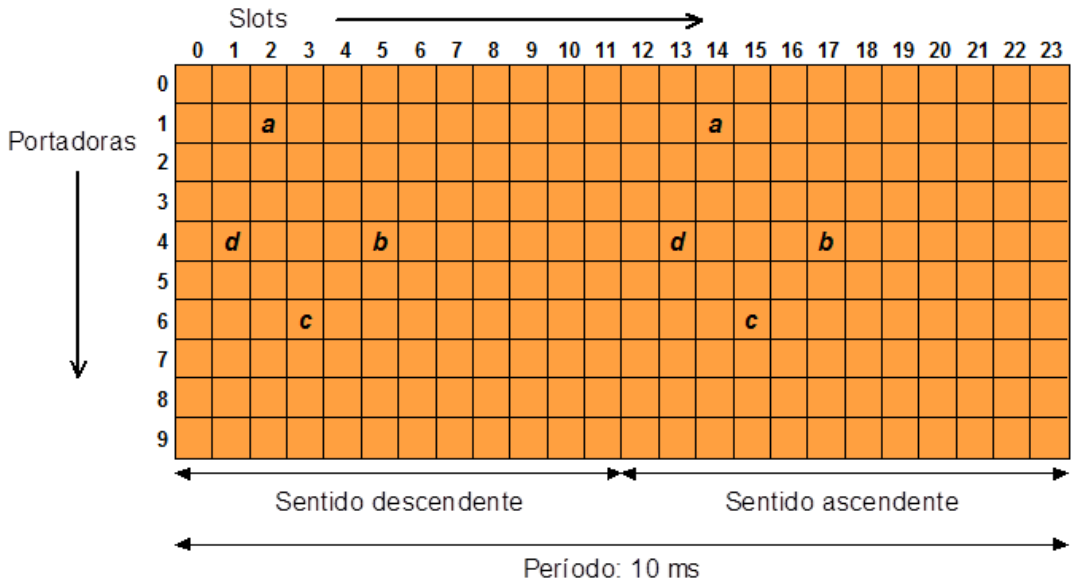

Figura 4.6: Exemplo de alocação de canais no sistema DECT.

4.2.2.4 Reserva dinâmica implícita

Estes protocolos foram concebidos com o objetivo de possibilitar a multiplexação estatística do tráfego de voz e de dados. A motivação principal consiste no suporte de serviços de dados em redes celulares móveis baseadas em TDMA. Nos protocolos de reserva dinâmica implícita, o tempo é dividido em tramas compostas de *slots*. O período de uma trama coincide com o intervalo de geração dos pacotes de voz, e o tamanho de cada *slot* é apropriado para a transmissão de um pacote de voz ou de dados. As estações competem pelos *slots* vazios, utilizando um processo aleatório.

A diferença destes protocolos em relação aos protocolos de acesso aleatório é que um pacote de voz enviado com sucesso num dado *slot* reserva, implicitamente, o respetivo *slot* nas tramas seguintes. Desta forma, os outros pacotes da conexão podem ser transmitidos livres de contenção. O *slot* é libertado para utilização das outras conexões a partir do momento em que é deixado vazio. Devido à estrutura rígida da trama, estes protocolos são pouco flexíveis para o transporte de uma mistura de conexões de tempo real com diferentes características.

Um exemplo de protocolo de reserva dinâmica implícita é o PRMA (*Packet Reservation Multiple Access*) [Good89], cujo funcionamento é exemplificado na Figura 4.7. O primeiro *slot* da trama K estava reservado para tráfego de voz (R_V) de uma dada estação, e continua a sê-lo na trama K+1. O segundo *slot* estava desocupado (I - *idle*) na trama K e, tendo sido alvo de uma colisão (C), continuou livre na trama seguinte, na qual foi ocupado por um pacote de dados (D). O quarto *slot* da trama K, que estava livre, foi ocupado por um pacote de voz (V), pelo que na trama seguinte ficou automaticamente reservado para tráfego de voz daquela estação. Em contraste, o sexto *slot* da trama K, que também estava livre, foi ocupado com um pacote de dados, que não dá direito à reserva do *slot*, tendo assim ficado livre na trama seguinte, na qual foi alvo de uma colisão.

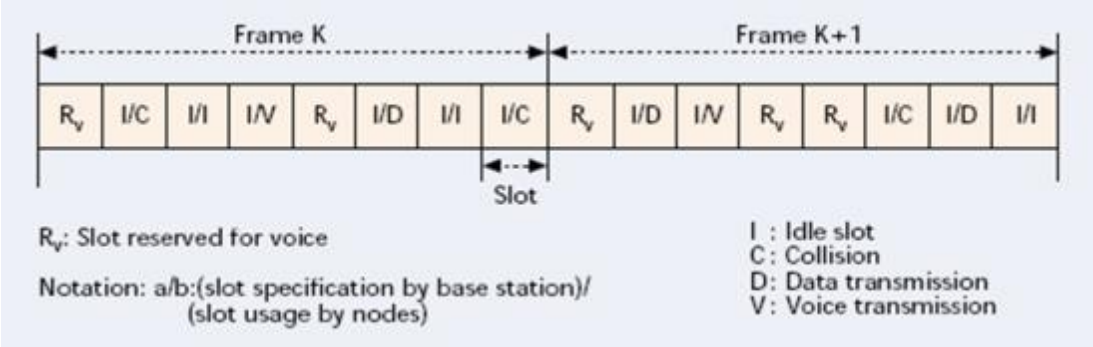

Figura 4.7: Exemplo de funcionamento do protocolo PRMA [Chan00].

4.2.2.5 Reserva dinâmica explícita

Na reserva dinâmica explícita, as estações enviam pedidos de recursos para o controlador central (CC). O formato da informação contida no pedido de recursos é dependente do protocolo, e pode variar desde o simples pedido de um número fixo de *slots* por trama até à especificação detalhada de requisitos de qualidade de serviço, que pode incluir parâmetros como o débito médio e o atraso máximo tolerável. Os pedidos de recursos normalmente são feitos usando um mecanismo de acesso aleatório, em *slots* apropriados. Alguns protocolos também permitem o envio de pedidos de recursos em resposta a

interrogações do CC, evitando assim o processo de contenção, ou a anexação de pedidos nos pacotes de dados transmitidos.

Com base nos pedidos recebidos, o controlador central efetua o escalonamento do tráfego das estações, tendo em consideração os requisitos de qualidade de serviço dos diferentes fluxos. Periodicamente, o controlador central divulga a informação sobre a atribuição de recursos efetuada, para que cada estação possa saber os períodos certos nos quais pode efetuar as suas transmissões. Como estes períodos são reservados às estações, não há risco de colisões, ao contrário do que ocorre nos protocolos baseados em contenção. Por outro lado, estes protocolos implicam uma complexidade maior na coordenação entre as estações devido à necessidade de sincronização e de troca de mensagens de sinalização.

As redes ATM sem fios (*wireless* ATM) estão na base do desenvolvimento destes protocolos. Entretanto, outros tipos de redes também podem beneficiar de suas características. A Figura 4.8 apresenta a estrutura da trama do protocolo MASCARA (*Mobile Access Scheme based on Contention and Reservation for* ATM), composto pelo *frame header period*, no qual o CC divulga a informação sobre a atribuição de recursos na mesma trama, o *down period*, no qual ocorre a transmissão de dados para as estações, o *up period*, no qual as estações efetuam as suas transmissões, e o *contention period*, no qual as estações efetuam os pedidos de recursos.

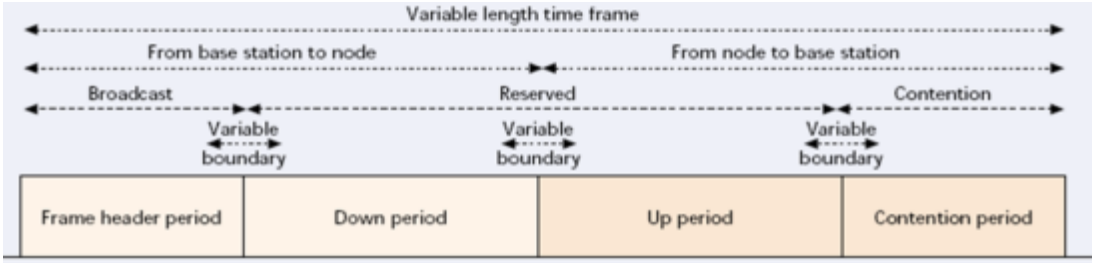

Figura 4.8: Estrutura da trama do protocolo MASCARA [Chan00].

4.2.2.6 Passagem de testemunho

Além dos protocolos descritos anteriormente, existem ainda os protocolos de passagem de testemunho (*token passing*), utilizados por algumas redes cabladas. Nestes protocolos, a estação em posse do testemunho controla o acesso ao meio. O testemunho é passado de estação para estação, em sequência, para que todas tenham oportunidade de transmitir, pelo que o controlo de acesso é distribuído. Os problemas de eficiência destes protocolos são semelhantes aos dos protocolos de *polling* que operam com um esquema de rotação.

Os protocolos de controlo de acesso ao meio das redes *Token Bus* (IEEE 802.4) e *Token Ring* (IEEE 802.5) são exemplos de protocolos de passagem de testemunho utilizados em redes cabladas com topologias em barramento e em anel, respetivamente. No entanto, estes protocolos não são apropriados para redes sem fios [Will02] [Chan00], pois a perda do testemunho seria frequente, dada a natureza instável das ligações sem fios, e o processo de recuperação do testemunho é dispendioso.

4.3 Protocolos MAC em redes sem fios

As ligações sem fios introduzem mais desafios à implementação de protocolos MAC do que as ligações por cabos. Alguns desses problemas já foram referidos em secções anteriores:

- A potência do sinal recebido em meio livre decresce com o quadrado da distância.
- A deteção de colisão costuma ser impraticável, devido ao fenómeno de *self-interference*, pelo que um protocolo do tipo CSMA/CD não pode ser utilizado.
- A taxa de erros no meio sem fios é maior e mais variável que nos meios cablados, devido a fatores como interferência, obstrução e desvanecimento multipercurso.

Além desses problemas, importa ressaltar o problema da estação oculta, que é descrito na próxima secção.

4.3.1 Problema da estação oculta

O problema da estação oculta, ou nó oculto, afeta protocolos MAC baseados em deteção de portadora (*carrier sense*). Um exemplo da ocorrência deste problema é ilustrado na Figura 4.9a, onde o alcance da transmissão das estações A e B estão representados pelos círculos desenhados em sua volta, e as estações destinatárias das transmissões estão identificadas pelas setas. Suponha que A está a transmitir o seu pacote para a estação C e que B quer começar a transmitir para a estação D. Como B está fora do alcance de A, será incapaz de detetar a transmissão em curso, ou seja, a deteção de portadora ira falhar. Como consequência, B irá começar a transmitir, causando uma colisão em C, e consequentemente, a perda do pacote enviado por A. Neste caso, diz-se que A está oculta de B.

A Figura 4.9b apresenta uma variação do problema na qual A e B transmitem para um mesmo destinatário (C). Neste caso, ambos os pacotes são perdidos na colisão.

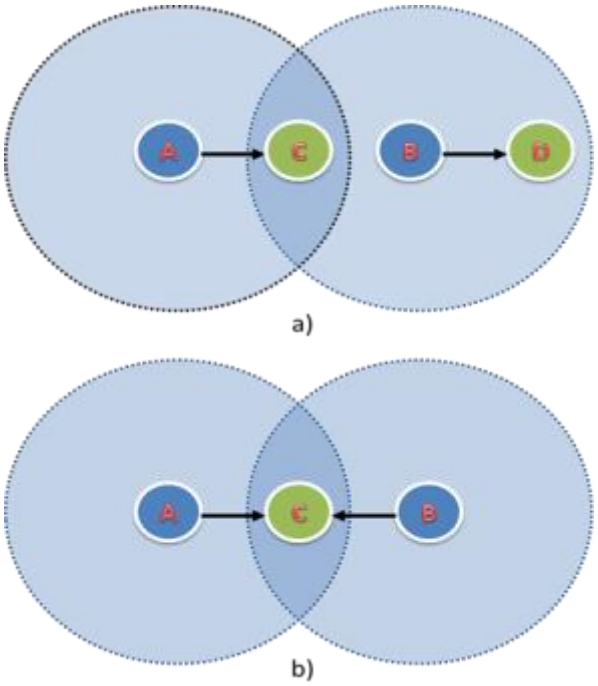

Figura 4.9: Exemplos de ocorrência do problema da estação oculta [Mace10].

O problema da estação oculta ocorre quando o sinal transmitido por uma estação chega muito fraco a outra estação na mesma rede, provocando uma falha no mecanismo de deteção da portadora. A perda em espaço livre, o desvanecimento multipercurso e a obstrução são fatores que podem reduzir a intensidade do sinal detetado por uma estação.

Embora, nos exemplos dados, B também esteja oculta de A, essa simetria nem sempre se verifica. Naturalmente, quanto mais estações ocultas de outras houver numa rede, maior tenderá a ser a degradação do desempenho desta rede.

Os protocolos MAC que não dependem da deteção de portadora para a sua operação não são afetados pelo problema da estação oculta. Por exemplo, numa rede baseada em *polling* não há problema em haver escravos ocultos de outros escravos, porque o funcionamento do protocolo depende apenas da interação dos escravos com o mestre. Naturalmente que se o sinal transmitido pelo mestre chegar com intensidade fraca a um escravo, ou vice-versa, haverá um problema de fiabilidade das comunicações. No entanto, é um problema de

transmissão do sinal e não de deteção do sinal, pelo que não se trata de um problema de estação oculta.

Vários mecanismos foram propostos na literatura para diminuir os efeitos do problema da estação oculta [Koub09]. Nos mecanismos baseados no sinal de ocupado (*busy tone*), uma estação que esteja a escutar uma transmissão em curso (C, nos exemplos da Figura 4.9) envia um sinal de ocupado num outro canal enquanto estiver a receber a transmissão (de A). Caso outra estação (B) deseje transmitir, não irá fazê-lo enquanto a transmissão em curso não acabar, porque será capaz de detetar o sinal de ocupado. A principal desvantagem deste mecanismo é a necessidade um canal de comunicação extra para a transmissão do sinal de ocupado, o que acarreta novos custos (a diferentes níveis) associados ao *hardware* adicional.

Outro mecanismo proposto para reduzir o número de colisões, particularmente as associadas ao problema da estação oculta, é o mecanismo proposto no protocolo MACA (*Multiple Access with Collision Avoidance*). Este mecanismo utiliza dois pacotes curtos de controlo (RTS e CTS), que são trocados antes da transmissão do pacote de dados[11]. Com o pacote RTS (*Request To Send*), enviado em primeiro lugar, o emissor requisita a transmissão de um pacote de dados para um destinatário. Em resposta, se estiver apto a receber, o destinatário autoriza a transmissão pelo envio de um CTS (*Clear To Send*) para o emissor.

Tanto o RTS como o CTS contém a seguinte informação:

- Endereço do emissor;
- Endereço do destinatário;
- Duração completa da troca de pacotes, incluindo o pacote de dados.

A Figura 4.10 apresenta um exemplo do funcionamento do mecanismo RTS/CTS. Neste exemplo, as estações A e C querem enviar dados para B.

[11] Em contraste com o sinal de ocupado do mecanismo de *busy tone*, que é transmitido durante a transmissão do pacote de dados

Primeiramente, A envia um pacote RTS para B, que responde com o envido de um pacote CTS para A autorizando a transmissão. O mesmo pacote RTS chega a C, que fica assim ciente de que está a decorrer uma troca de pacotes entre A e B (embora não consiga detetar a transmissão de A), pelo que C adia a sua transmissão para depois do fim da transmissão em curso, cuja duração é especificada no pacote CTS.

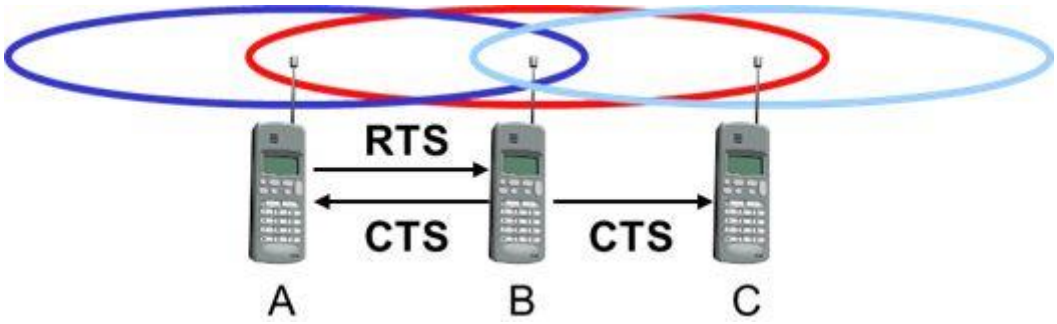

Figura 4.10: Exemplo de funcionamento do mecanismo RTS/CTS [Schi04].

A principal desvantagem do mecanismo RTS/CTS é o *overhead* introduzido pela necessidade de transmissão de dois pacotes de controlo adicionais antes da transmissão de dados propriamente dita, que tem impacto no consumo de largura de banda da rede e no consumo de energia das estações. Sendo assim, a utilização deste mecanismo só compensa quando o tamanho dos pacotes de controlo é pequeno comparado com o tamanho do pacote de dados. Uma variante do mecanismo RTS/CTS foi adotada pela norma IEEE 802.11.

Referências

[Chan00] A. Chandra, V. Gummalla and J. O. Limb, “Wireless Medium Access Control Protocols”, IEEE Communications Surveys & Tutorials, Second Quarter, 2000.

[Glis97] S. Glisic, “Spread Spectrum CDMA Systems for Wireless Communications”, Artech House, 1997.

[Good89] D. J. Goodman, R. A. Valenzuela, K. T. Gayliard and B. Ramamurthi, “Packet Reservation Multiple Access for Local Wireless

Communications", IEEE Transactions on Communications, Vol. 37, No. 8, pp. 885-890, August 1989.

[I802.3] IEEE 802.3, "Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", 2002.

[Koub09] A. Koubâa et al., "Improving Quality-of-Service in Wireless Sensor Networks by Mitigating Hidden-Node Collisions", IEEE Transactions on Industrial Informatics, Vol. 5, No. 3, August 2009.

[Mace10] P. Macedo, "Desenvolvimento de Modelos de Simulação de Redes de Sensores sem Fios", Dissertação de Mestrado, Mestrado Integrado em Engenharia Eletrónica Industrial e Computadores, Universidade do Minho, Novembro de 2010.

[Rohl99] H. Rohling, T. May, K. Brüninghaus and R. Grünheid, "Broad-Band OFDM Radio Transmission for Multimedia Applications", Proceedings of the IEEE, Vol. 80, No. 10, October 1999.

[Rubi97] I. Rubin, "Multiple Access Methods for Communications Networks", Book Chapter, "The Communications Handbook", J. D. Gibson (Ed.), CRC Press, 1997.

[Sari00] H. Sari, F. Vanhaverbeke and M. Moeneclaey, "Extending the Capacity of Multiple Access Channels", IEEE Communications Magazine, pp. 74-82, January 2000.

[Schi04] J. Schiller, "Mobile Communications", 2nd edition, Addison-Wesley, 2004.

[Stal02] W. Stallings, "Wireless Communications and Networks", Prentice-Hall, 2002.

[Tane89] A. S. Tanembaum, "Computer Networks", Prentice Hall, 1989.

[Varg00] A. Varga, "OMNET++ Discrete Event Simulation System", User Manual, Department of Telecommunications, Technical University of Budapest, 2000.

[Will02] A. Willig, “Analysis of the PROFIBUS Token Passing Protocol over Wireless Links”, *IEEE International Symposium on Industrial Electronics ISIE’02*, L'Aquila, Italy, July 2002.

5.A rede IEEE 802.11

5.1 Introdução

Os primeiros produtos para redes locais sem fios, utilizando tecnologia proprietária, foram introduzidos no início da década de 90, aproveitando a disponibilidade das bandas ISM para operação sem necessidade de licença. Estes produtos operavam na banda ISM de 900 MHz, disponível na América do Norte. Algum tempo depois, surgiram produtos a operar na banda ISM de 2.4 GHz e, mais para o final da década, começaram a aparecer produtos que utilizam a banda de frequências de 5 GHz.

O principal problema das soluções proprietárias de redes sem fios foi a pouca aceitação no mercado, por falta de um padrão que garantisse a compatibilidade entre os produtos disponibilizados pelos diversos fabricantes. Para resolver este problema, após vários anos de discussão, o IEEE aprovou a primeira versão das normas IEEE 802.11, publicada em 1997.

5.1.1 Arquitetura

De acordo com a denominação utilizada pelas normas do IEEE 802.11, um grupo de duas ou mais estações sob o controlo direto de uma mesma função de coordenação[12] forma um conjunto básico de serviço (BSS - *Basic Service Set*). A área coberta por um BSS é designada por área básica de serviço (BSA - *Basic Service Area*), e pode ser vista como o análogo a uma célula numa rede celular móvel.

As redes IEEE 802.11 podem operar em modo *ad hoc* ou em modo baseado em infraestrutura. Um BSS isolado, em que as estações comunicam

[12] Função de coordenação é o nome utilizado pelo IEEE 802.11 para se referir ao mecanismo de controlo de acesso ao meio.

apenas entre si, formando uma rede *ad hoc*, é denominado IBSS (*Independent BSS*), como é exemplificado na Figura 5.1.

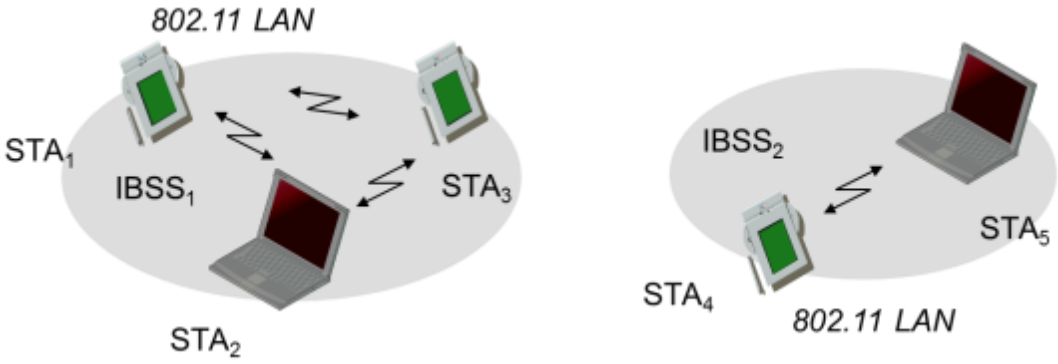

Figura 5.1: Exemplo de redes ad hoc IEEE 802.11 [Schi04].

A Figura 5.2 representa os componentes da arquitetura da rede IEEE 802.11 na configuração baseada em infraestrutura. Este modo de operação requer a presença de uma estação especial no BSS, denominada ponto de acesso (AP - *Access Point*), que serve de interface entre o BSS e o sistema de distribuição (DS - *Distribution System*) e possibilita a comunicação entre as estações (STA - *Station*) do BSS e entidades externas. O sistema de distribuição (DS) permite interligar múltiplos BSSs, formando um conjunto estendido de serviço (ESS - *Extended Service Set*). Do ponto de vista da subcamada de ligação lógica (LLC) das estações que compõem o ESS, este aparenta ser um único BSS alargado. Normalmente, o sistema de distribuição consiste numa rede de área local convencional, embora outras redes possam ser utilizadas, visto que as normas não entram em detalhes quanto à implementação do sistema de distribuição.

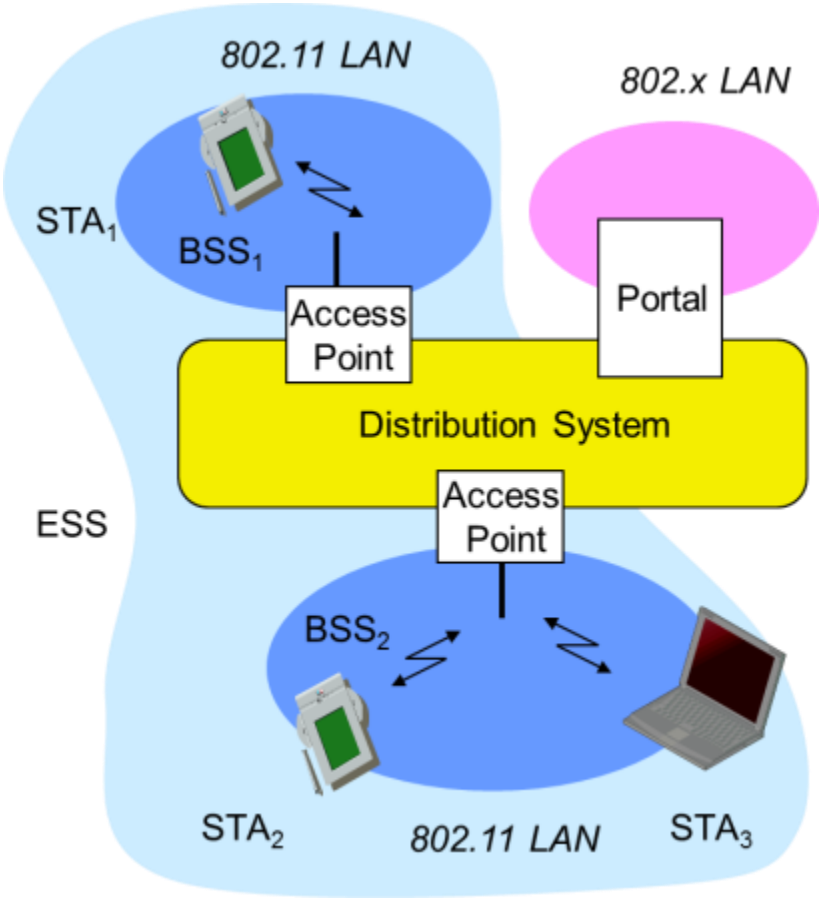

Figura 5.2: Componentes da arquitetura da rede IEEE 802.11 baseada em infraestrutura [Schi04].

5.1.2 Segurança

Numa rede cablada, apenas as estações fisicamente conectadas ao meio de transmissão estão aptas a captar as transmissões, o que não acontece nas redes sem fios. Qualquer estação compatível pode monitorar o tráfego de uma rede IEEE 802.11 que utilize a mesma camada física sem que seja detetada, bastando para isso estar dentro do raio de alcance da rede. Um dos primeiros mecanismos de segurança especificados pelo IEEE 802.11 foi o protocolo WEP (*Wired Equivalent Privacy*). O WEP define um algoritmo criptográfico, de utilização opcional, destinado a proporcionar um nível de confidencialidade à transmissão de dados que seja similar (subjetivamente) à confidencialidade existente numa rede local cablada que não utilize técnicas criptográficas para aumentar a privacidade das comunicações.

5.1.3 Associação

Antes que uma estação possa encaminhar mensagens de dados através de um ponto de acesso, ela deve associar-se ao mesmo. O processo de associação permite ao sistema de distribuição determinar a que ponto de acesso uma estação está associada, de modo a poder encaminhar mensagens para a mesma. Uma estação não pode estar associada a mais que um ponto de acesso de cada vez. O processo de associação é sempre iniciado pela estação, pelo envio de uma mensagem de requisição de associação.

5.1.4 Autenticação

A autorização de acesso à rede por parte das estações no IEEE 802.11 precede o processo de associação, sendo negociada através do serviço de autenticação. Se um nível aceitável de autenticação não for estabelecido entre a estação e o ponto de acesso, a associação não é realizada. O IEEE 802.11 suporta diversos mecanismos de autenticação, como, por exemplo, a autenticação por chave compartilhada (*shared key*), em que a identidade da estação é demonstrada pelo conhecimento da chave de encriptação secreta do protocolo de segurança WEP.

5.1.5 Gestão de consumo de energia

O IEEE 802.11 proporciona suporte para gestão de consumo de energia das estações. O ponto de acesso armazena os dados destinados às estações que estão a operar em modo de poupança de energia e difunde informação nas tramas *Beacon*. Para esse efeito, as tramas *Beacon* contém um mapa de indicação de tráfego (TIM - *Traffic Indication Map*) que informa às estações da existência de dados pendentes armazenados no ponto de acesso. As estações que operam no modo de poupança de energia acordam periodicamente para escutar a trama *Beacon*. Quando uma estação recebe indicação de que o ponto de acesso tem tramas armazenadas para si, ela interroga o ponto de

acesso, pelo uso da trama de controlo PS-Poll[13], requisitando o envio das tramas armazenadas.

5.2 Camada física

No âmbito das normas IEEE 802.11, foram especificados diversos tipos de camadas físicas, como é descrito a seguir.

5.2.1 Camadas físicas originais

A norma IEEE 802.11 original [IEEE99] especifica três camadas físicas distintas, baseadas em diferentes tecnologias:

- Espalhamento espectral por sequência direta (DSSS);
- Espalhamento espectral por saltos em frequência (FHSS);
- Comunicação ótica (DFIR, *diffuse infrared*).

As duas primeiras operam na banda ISM de 2.4 GHz, enquanto a última utiliza a banda de infravermelhos. Todas estas camadas físicas suportam débitos de transmissão de 1 Mbit/s e 2 Mbit/s.

Para permitir que a camada MAC do IEEE 802.11 possa operar de forma independente da camada física, esta última camada é dividida em duas subcamadas:

- Subcamada PLCP (*Physical Layer Convergence Procedure*);
- Subcamada PMD (*Physical Medium Dependent*).

A subcamada superior (PLCP) efetua o mapeamento das tramas MAC num formato adequado à transmissão da informação entre as estações da rede utilizando as funções da subcamada inferior (PMD), enquanto esta última define as características e métodos de transmissão e receção de dados dependentes da tecnologia utilizada no meio sem fios.

[13] PS significa *Power Save*.

A camada física do IEEE 802.11 recebe a trama MAC e anexa o preâmbulo e o cabeçalho da PLCP à sua frente. O preâmbulo e o cabeçalho do pacote da camada física são sempre transmitidos à taxa de transmissão mínima da rede[14], ao contrário do que acontece com o resto do pacote, a partir do início da trama MAC, que pode utilizar uma taxa de transmissão de dados mais elevada. Isso permite a coexistência de estações que suportem débitos máximos diferentes e simplifica a tarefa de equalização. Por outro lado, isso faz com que o *overhead* da camada física tenha grande impacto na eficiência de transmissão, que é tão mais significativo quão maior for a taxa de transmissão de dados em comparação com a taxa mínima.

5.2.2 IEEE 802.11b

A norma IEEE 802.11b [IEE99b], introduzida em 1999, estende a especificação da camada física baseada em espalhamento espectral por sequência direta (DSSS), aumentando o débito máximo de transmissão para 11 Mbit/s. Esta versão suporta ainda o débito de 5.5 Mbit/s e os débitos de 2 Mbit/s e 1 Mbit/s da versão original, enquanto assegura retrocompatibilidade com a mesma. O aumento do débito de transmissão é alcançado pela utilização de modulação CCK (*Complementary Code Keying*).

As redes IEEE 802.11b dispõem de 14 canais[15] na banda ISM dos 2.4 MHz para operação, cada qual ocupando 22 MHz. Os canais adjacentes sobrepõem-se parcialmente, pelo que no máximo apenas 3 canais podem ser usados simultaneamente, como é exemplificado na Figura 5.3.

[14] 6 Mbit/s na rede IEEE 802.11a, 1 Mbit/s nos demais casos.

[15] Em alguns países, a disponibilidade de canais é menor.

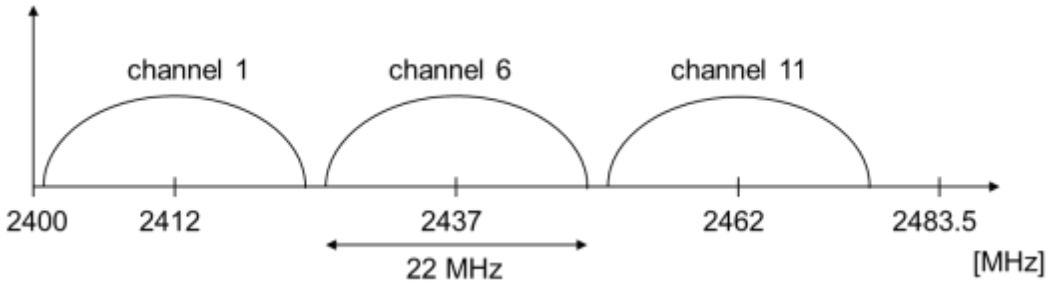

Figura 5.3: Exemplo de canais IEEE 802.11b não sobrepostos na banda de 2.4 GHz [Schi04]

Para reduzir o *overhead* associado à camada física, a norma IEEE 802.11b define um formato curto para o preâmbulo e o cabeçalho da PLCP, em alternativa ao formato normal. O formato curto é opcional e só pode ser utilizado para comunicação entre estações que o suportem. A Figura 5.4 apresenta o formato longo (acima) e o formato curto (abaixo) do PPDU da subcamada PLCP da norma IEEE 802.11b. Os bits de sincronização do preâmbulo são utilizados para sincronização, ajuste de ganho, deteção de energia e compensação de desvio de frequência. O SFD (*Start Frame Delimiter*), que corresponde à sequência 1111001110100000, é usado para identificação do início do cabeçalho do PPDU. O campo *signal* indica a taxa de transmissão que será utilizada no payload do PPDU, ou seja, no MPDU. O campo *service* é reservado para uso futuro. O campo *length* contém o comprimento do payload. O campo HEC (*Header Error Check*) é utilizado para deteção de erros no cabeçalho do PPDU.

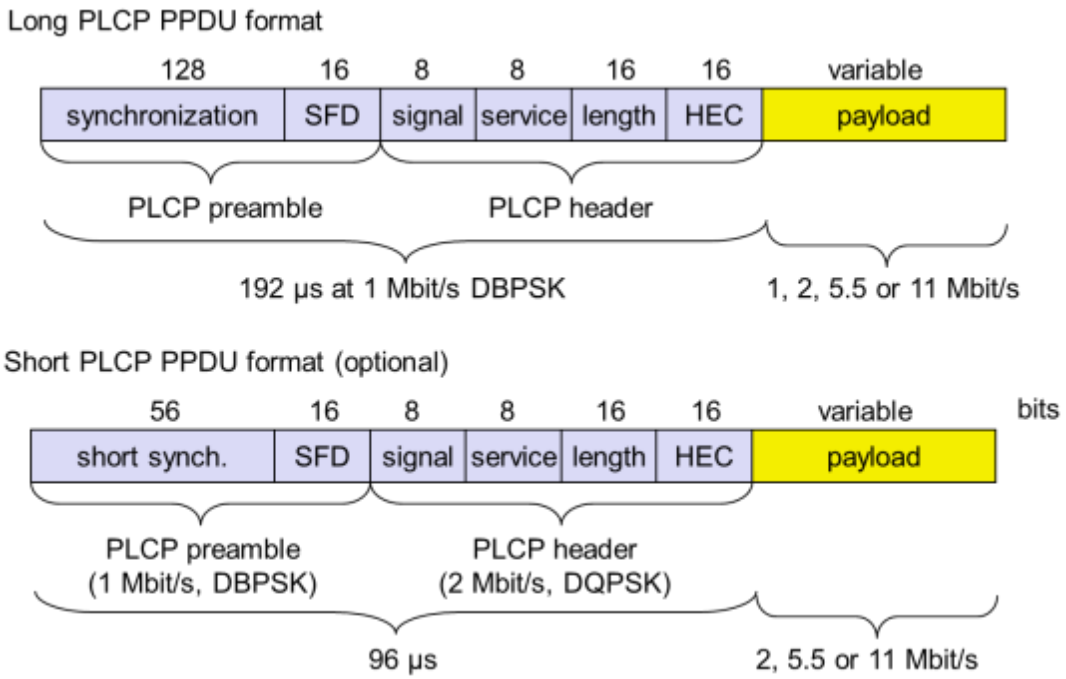

Figura 5.4: Formatos longo e curto do PPDU da subcamada PLCP da norma IEEE 802.11b [Schi04].

A norma IEEE 802.11a, que define uma camada física diferente das mencionadas anteriormente, é descrita com mais detalhe na próxima secção.

5.2.3 IEEE 802.11a

A norma IEEE 802.11a [IEE99a] especifica a operação da rede IEEE 802.11 na banda de frequências de 5 GHz, sendo baseada na técnica de modulação OFDM (*Orthogonal Frequency Division Multiplexing*). São utilizadas 52 subportadoras: 48 para o transporte de dados e 4 para sinais piloto. As 48 subportadoras de dados podem ser moduladas utilizando BPSK, QPSK, 16QAM ou 64QAM.

Além das opções de modulação apresentadas, existem diferentes opções de taxas de codificação para correção de erros (FEC), baseadas na utilização de código convolucional. As taxas de codificação FEC disponíveis são 1/2, 2/3 e 3/4. A combinação do esquema de modulação com a taxa de codificação determina o débito de transmissão em uso. A Tabela 5.1 apresenta os oito modos de transmissão disponíveis na rede IEEE 802.11a, juntamente com os

débitos de transmissão ao nível da camada física e os parâmetros de modulação e codificação FEC.

Tabela 5.1: Modos de transmissão da rede IEEE 802.11a

Modo de transmissão	Débito (Mbit/s)	Modulação	Codificação FEC
1	6	BPSK	1/2
2	9	BPSK	3/4
3	12	QPSK	1/2
4	18	QPSK	3/4
5	24	16QAM	1/2
6	36	16QAM	3/4
7	48	64QAM	2/3
8	54	64QAM	3/4

Independentemente do débito de transmissão utilizado, o débito dos símbolos OFDM é constante, sendo igual a 250000 símbolos/s, o que corresponde a uma duração de 4 μs para cada símbolo OFDM. Entretanto, para evitar a interferência intersimbólica (ISI), um período de guarda de 0.8 μs é utilizado, deixando 3.2 μs para a parte útil do símbolo OFDM.

A subcamada PLCP (*Physical Layer Convergence Procedure*) do IEEE 802.11a adapta a trama da subcamada MAC (MPDU) a um formato (PPDU) apropriado à transmissão pela camada física baseada em modulação OFDM. O formato do PPDU, apresentado na Figura 5.5, inclui o preâmbulo da PLCP, o cabeçalho da PLCP, o PSDU (que corresponde ao MPDU), os *tail* bits e os *pad* bits.

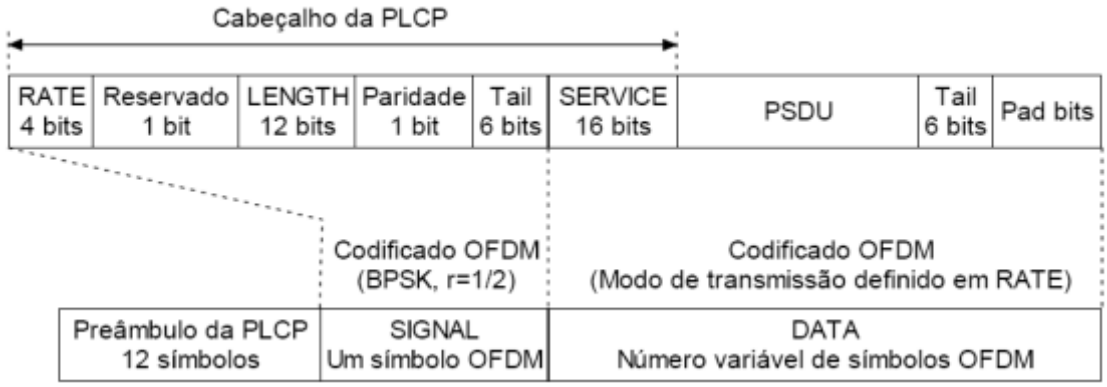

Figura 5.5: Formato do PDU da camada física (PPDU) do IEEE 802.11a.

O preâmbulo da PLCP, usado para sincronização OFDM, tem a duração de 16 μs, sendo formado por duas sequências de treino: a primeira sequência é composta por 10 símbolos curtos; enquanto a segunda sequência contém 2 símbolos longos.

A seguir ao preâmbulo da PLCP encontram-se os campos SIGNAL e DATA. O campo SIGNAL corresponde ao cabeçalho da PLCP, com exceção do campo SERVICE, que faz parte do campo DATA. O campo SIGNAL é transmitido com o modo de transmissão mais robusto disponível (6 Mbit/s), que utiliza modulação BPSK e uma taxa de codificação FEC de 1/2 (Tabela 5.1). Este campo ocupa exatamente um símbolo OFDM, pelo que a sua duração é de 4 μs.

A duração do campo DATA é variável, dependendo do comprimento do PSDU e do débito de transmissão utilizado. Esta informação encontra-se codificada nos campos LENGTH e RATE do cabeçalho da PLCP, respetivamente. Ao contrário do campo SIGNAL, os bits do campo DATA são baralhados antes da transmissão. Parte do campo SERVICE é utilizada para sincronizar o *descrambler* no recetor, enquanto a outra parte é reservada para uso futuro.

A rede IEEE 802.11a foi concebida para operar numa banda de frequências entre 5 e 6 GHz. Nesta região, a frequência central dos canais é definida em múltiplos de 5 MHz a partir de 5 GHz. A relação entre a frequência central do canal (f_{ch}), em MHz, e o número do canal (n_{ch}) é expressa por:

$$f_{ch} = 5000 + 5 \times n_{ch}, \quad (5.1)$$

sendo n_{ch} = 0, 1 ... 200.

O espaçamento entre os canais das redes IEEE 802.11a especificado na norma é de 20 MHz. O conjunto de canais válidos para operação nas bandas U-NII (*Unlicensed National Information Infrastructure*), nos Estados Unidos, é apresentado na Tabela 5.2.

Tabela 5.2: Canais válidos para operação de redes IEEE 802.11a nos Estados Unidos.

Banda (GHz)	Número do canal	Frequência central do canal (MHz)
Banda U-NII inferior (5.15 - 5.25)	36	5180
	40	5200
	44	5220
	48	5240
Banda U-NII média (5.25 - 5.35)	52	5260
	56	5280
	60	5300
	64	5320
Banda U-NII superior (5.725 - 5.825)	149	5745
	153	5765
	157	5785
	161	5805

5.2.4 IEEE 802.11g

O grupo de tarefas G do 802.11 publicou em 2003 as especificações da norma IEEE 802.11g, concebida para operar na banda ISM de 2.4 GHz com suporte de débitos até 54 Mbit/s. Tal como acontece com a norma IEEE 802.11a, a norma IEEE 802.11g é baseada em modulação OFDM. As estações baseadas no IEEE 802.11g também devem suportar todos os modos de transmissão do IEEE 802.11b, para que possam operar normalmente numa rede 802.11b, o que implica a implementação da modulação CCK.

Um problema que se coloca neste caso é a deteção das transmissões que utilizam a modulação OFDM pelas estações baseadas no IEEE 802.11b, de modo a evitar colisões. Uma alternativa consiste em preceder a transmissão de dados com as tramas RTS e CTS, transmitidas utilizando modulação CCK, que é reconhecida pelo IEEE 802.11b. Opcionalmente, pode-se utilizar um esquema de modulação híbrido, que conjuga as modulações CCK e OFDM. A modulação CCK é utilizada para transmissão do preâmbulo e do cabeçalho dos pacotes, enquanto a modulação OFDM é usado para a transmissão do *payload*. Com isso, as estações do IEEE 802.11b são alertadas do início de uma transmissão, e informadas da duração da mesma. Depois, os dados são transmitidos ao débito mais elevado proporcionado pelo OFDM. A contrapartida da compatibilidade proporcionada por estas soluções é o decréscimo do desempenho em relação à utilização exclusiva da modulação OFDM, devido ao *overhead* introduzido pelas mesmas.

Outra técnica de modulação opcional incluída no IEEE 802.11g é o PBCC (*Packet Binary Convolutional Coding*), uma solução criada pela Texas Instruments que proporciona débitos de transmissão de até 33 Mbit/s. Esta solução também é híbrida, sendo o preâmbulo e o cabeçalho transmitidos com modulação CCK para preservar a compatibilidade com o IEEE 802.11b.

5.2.5 IEEE 802.11n

A norma 802.11n, publicada em 2009, é uma extensão da norma IEEE 802.11 concebida com o propósito principal de aumentar a taxa de transmissão de dados em relação às normas 802.11a na banda de 5 GHz e 802.11g na banda de 2.4 GHz, de 54 Mbit/s para até 600 Mbit/s, pelo recurso à técnica MIMO (*Multiple-Input Multiple-Output*).

5.3 Camada MAC

O formato geral da trama de nível MAC do IEEE 802.11 é representado na Figura 5.6. Os campos endereço 2, endereço 3, controlo de sequência,

endereço 4 e corpo da trama estão presentes apenas em alguns tipos de tramas.

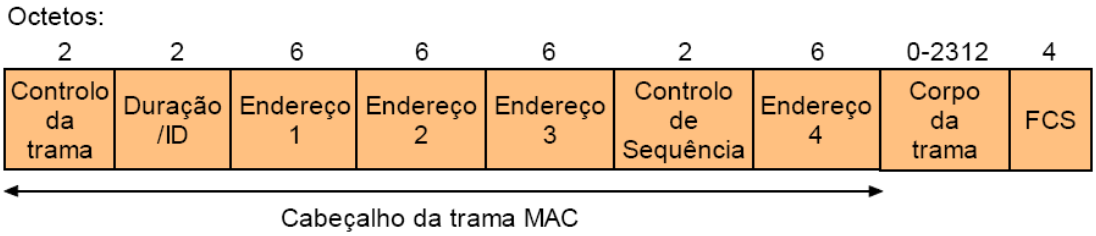

Figura 5.6: Formato geral da trama de nível MAC do IEEE 802.11.

A função de cada campo da trama é descrita sucintamente a seguir.

- O campo de controlo da trama (*frame control*) carrega informação de controlo, sendo composto por vários subcampos, entre os quais os subcampos tipo e subtipo, que identificam tanto o formato como a função da trama. O IEEE 802.11 define três tipos de trama: dados, controlo e gestão.
- O campo de duração/ID é utilizado, na maioria dos casos, pelo mecanismo de deteção de portadora virtual, que é referido mais adiante.
- Cada campo de endereço contém um endereço de nível MAC de 48 bits. Dependendo do tipo de trama e do seu eventual percurso pelo sistema de distribuição (DS), os campos de endereço podem referenciar a estação de destino (DA - *Destination Address*), a estação de origem (SA - *Source Address*), o recetor imediato (RA - *Receiver Address*), o emissor atual (TA - *Transmitter Address*) ou o BSS em que a trama é transmitida (BSSID).
- O campo de controlo de sequência (*sequence control*) é composto por dois subcampos: o número de sequência e o número de fragmento.
- O campo corpo da trama é um campo de comprimento variável que transporta informação relacionada com o tipo e subtipo de trama. No caso específico da trama de dados, este campo transporta o seu *payload*.
- O campo FCS (*Frame Check Sequence*) transporta um código CRC (*Cyclic Redundancy Code*) de 32 bits usado para a deteção de erros na trama. O FCS é calculado sobre todos os campos do cabeçalho e do corpo da trama.

5.3.1 Controlo de acesso ao meio

A camada de controlo de acesso ao meio do IEEE 802.11 implementa dois mecanismos distintos: a função de coordenação distribuída (DCF - *Distributed Coordination Function*) e a função de coordenação pontual (PCF -*Point Coordination Function*). O DCF é o mecanismo básico de controlo de acesso ao meio do IEEE 802.11, sendo um protocolo de acesso aleatório do tipo CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*). O PCF, por outro lado, é um protocolo de *polling* que permite às estações o acesso ao meio livre de contenção, o que torna sua utilização mais adequada para o transporte de tráfego de tempo real. Entretanto, a sua implementação não é obrigatória, ao contrário do DCF.

5.3.2 Função de coordenação distribuída (DCF)

De acordo com as regras do DCF, antes de iniciar a transmissão de uma trama de dados, a estação deve escutar o meio. Se no momento em que a estação deseja iniciar uma nova transmissão o meio não estiver ocupado, e se o meio continuar livre decorrido um período DIFS (*DCF Interframe Space*), a estação transmite a sua trama. Caso uma das duas condições anteriores não se verifique, a estação adia a sua transmissão e inicia o processo de *backoff*, como é exemplificado na Figura 5.7.

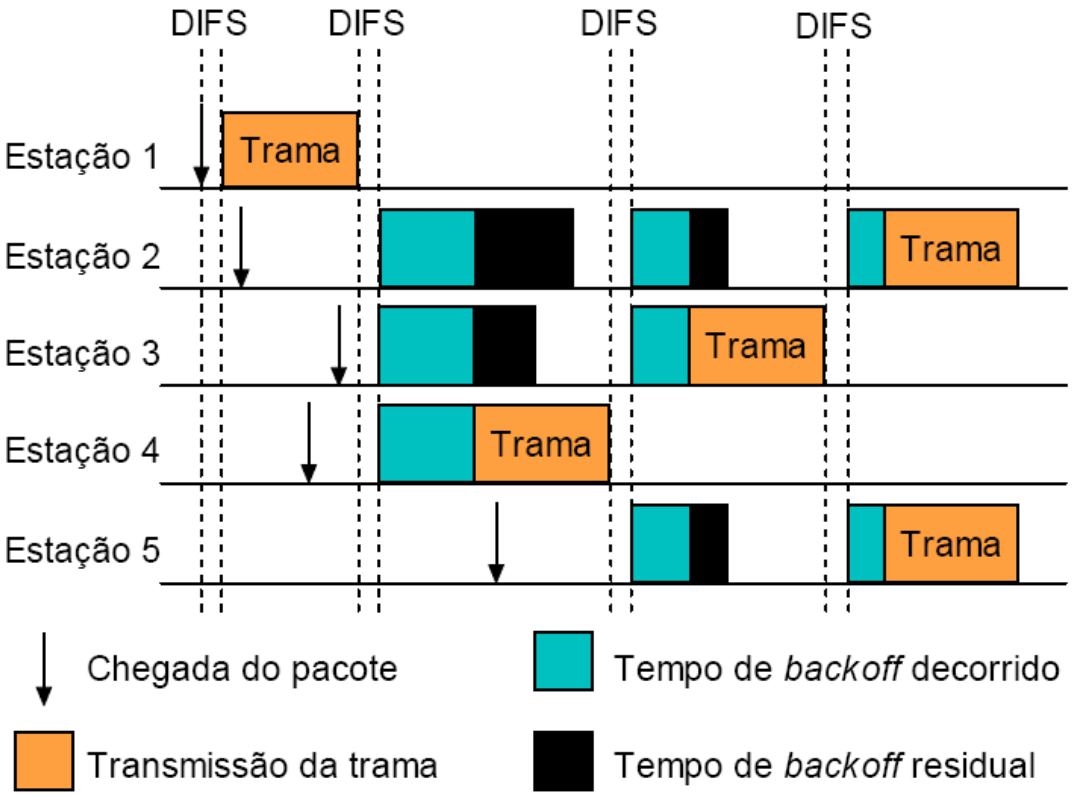

Figura 5.7: Exemplo de operação da função de coordenação distribuída (DCF).

No início do processo de *backoff*, a estação gera um número inteiro aleatório, uniformemente distribuído entre zero e o valor mínimo (CW_{min}) da janela de contenção (CW - *Contention Window*), que é utilizado para inicializar o contador de *backoff*. Quando o meio fica livre e permanece livre durante um período DIFS, a estação começa a decrementar o seu contador de *backoff*, fazendo-o a intervalos fixos (*SlotTime*) enquanto o meio continua livre, até o contador chegar a zero. Se a estação detecta uma transmissão durante esse período, porém, ela interrompe o decremento do contador e aguarda que o meio volte a ficar livre durante um período DIFS, para então recomeçar o decremento do contador de *backoff* a partir do ponto em que parou. Quando o contador chega a zero, a estação inicia a sua transmissão. Caso duas ou mais estações comecem suas transmissões ao mesmo tempo ocorre uma colisão (como é o caso das tramas transmitidas pelas estações 2 e 5, no exemplo da Figura 5.7).

De acordo com as normas do IEEE 802.11, o destinatário de uma trama de dados recebida corretamente responde com a transmissão de uma trama de reconhecimento positivo (ACK - *acknowledgement*), depois de aguardar por um período SIFS (*Short InterFrame Space*), como é mostrado na Figura 5.8.

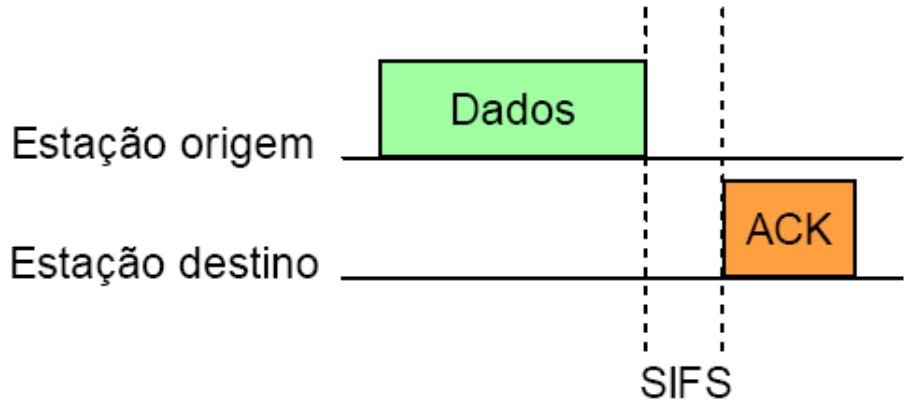

Figura 5.8: Mecanismo de reconhecimento positivo da função DCF.

Os períodos DIFS e SIFS estão relacionados pela seguinte expressão:

$$DIFS = SIFS + 2\,SlotTime \tag{5.2}$$

Como o período SIFS é menor do que o DIFS, a estação recetora pode transmitir a trama ACK sem ter que escutar o meio antes e sem risco de colisão, já que as outras estações estão inibidas de iniciar as suas transmissões durante um período (DIFS) maior. Sendo assim, na Figura 5.7, o período indicado por “Trama” contém normalmente uma trama de dados e a trama ACK correspondente, podendo conter, em certos casos, um conjunto ainda maior de tramas, sempre separadas pelo período SIFS, como nos casos do uso do mecanismo RTS/CTS ou do mecanismo de fragmentação, descritos mais adiante.

Na rede IEEE 802.11, o reconhecimento positivo é feito sempre que uma trama de dados é transmitida porque, ao contrário do que acontece nas redes cabladas, a incerteza sobre a receção correta de uma trama é muito maior, dado que num meio sem fios não é possível a deteção de colisões, além do que as transmissões estão muito mais expostas a erros no canal.

No IEEE 802.11, a estação recetora não transmite uma trama de reconhecimento negativo (NAK) quando recebe uma trama de dados corrompida por erros no canal. Assim, do ponto de vista do emissor, não há diferença entre este caso e perda da trama devido a uma colisão.

Quando o emissor não recebe uma trama ACK em resposta ao envio de uma trama de dados, assume que a trama não foi recebida com sucesso. Esgotado o período de *timeout* para a receção da trama ACK, o emissor repete o processo de *backoff*, antes de efetuar a retransmissão da trama de dados. No entanto, para diminuir a probabilidade de colisão, após cada tentativa falhada de transmissão de uma trama, a gama de valores da janela de contenção (CW) é duplicada até que seja atingido um valor máximo (CW_{max}). Após uma transmissão com sucesso (que tenha recebido reconhecimento positivo), a janela de contenção volta a assumir o valor inicial (CW_{min}). Caso a estação tenha mais dados a enviar, deve executar novamente o processo de *backoff* antes de iniciar a nova transmissão. A Figura 5.9 apresenta um exemplo do aumento da janela de contenção. Os valores dos parâmetros CW_{min} e CW_{max} dependem da versão da norma.

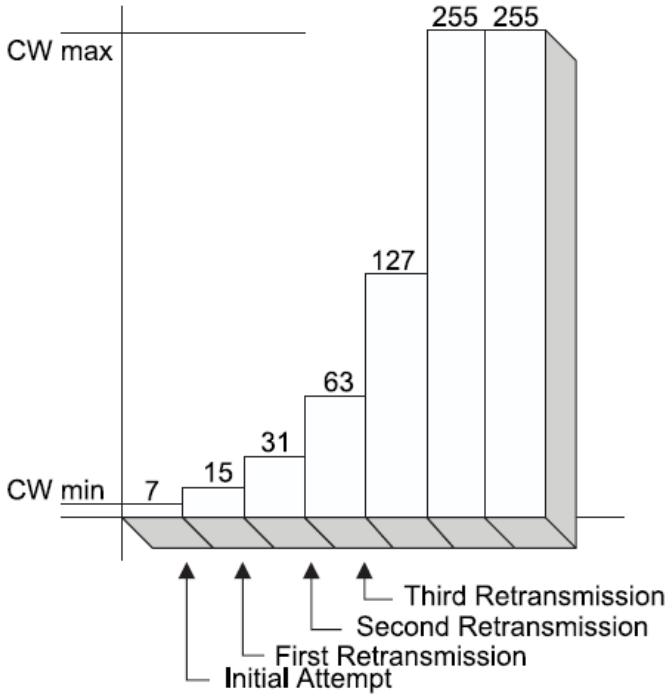

Figura 5.9: Exemplo de aumento da janela de contenção [IEEE99].

5.3.2.1 O mecanismo RTS/CTS

A deteção de portadora em redes sem fios está sujeita ao fenómeno da estação oculta (*hidden station*). Este fenómeno ocorre quando uma estação é capaz de receber o sinal de duas outras estações na sua vizinhança, mas as duas estações não conseguem detetar o sinal uma da outra, seja por estarem muito distantes entre si ou por terem o sinal bloqueado por obstáculos. Para lidar com o problema da estação oculta, o protocolo de controlo de acesso ao meio do IEEE 802.11 inclui um mecanismo opcional, baseado na troca de duas pequenas tramas de controlo antes do envio da trama de dados: a trama RTS (*Request To Send*), enviada pelo potencial transmissor da trama de dados (estação de origem); e a trama CTS (*Clear To Send*), enviada pela estação de destino em resposta à trama RTS, após um período SIFS. Se a trama CTS não for recebida, a estação de origem inicia o processo de *backoff* para a retransmissão da trama RTS. Por outro lado, se a troca das tramas RTS e CTS for bem-sucedida, esta estação pode então transmitir a sua trama de dados, como mostra a Figura 5.10.

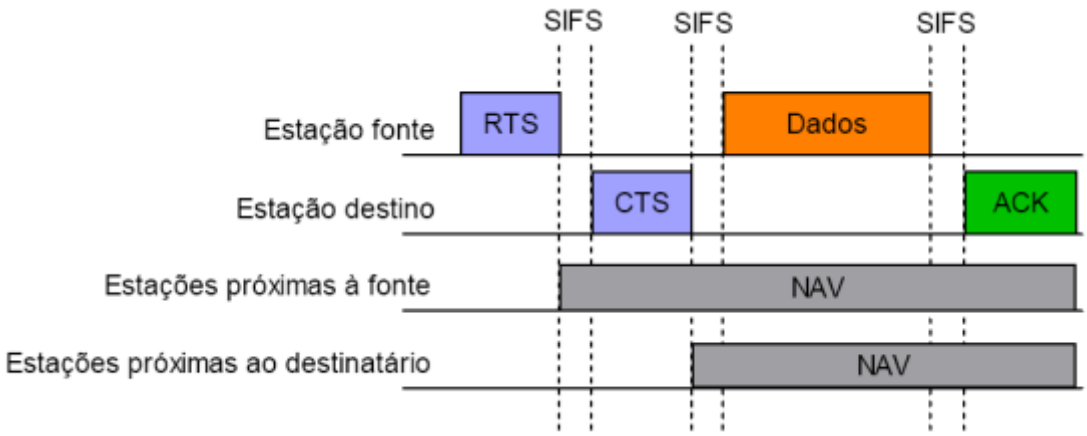

Figura 5.10: Comunicação entre as estações utilizando o mecanismo RTS/CTS.

A trama RTS possui um campo de duração que indica o período total necessário para transmissão da trama CTS, da trama de dados e da trama ACK, incluindo os períodos SIFS entre as tramas. Esse período é calculado pela estação de origem tendo em consideração o comprimento das tramas e o débito de transmissão utilizado. O campo de duração também está presente

na trama CTS, sendo preenchido pelo destinatário com base no valor anunciado na trama RTS, descontando-se o tempo necessário para a transmissão da trama CTS. As estações da rede analisam o conteúdo das tramas RTS e CTS, independentemente do destinatário, e utilizam a informação do campo de duração para atualizar os respetivos temporizadores NAV (*Network Allocation Vector*). Este temporizador inibe a transmissão da estação até o tempo programado expirar, mesmo que não haja atividade no meio, pelo que esse mecanismo é denominado deteção de portadora virtual.

A transmissão da trama RTS inibe a transmissão das estações na proximidade da estação de origem, enquanto a transmissão da trama CTS inibe a transmissão das estações na proximidade da estação de destino. Desta forma, a estação de origem tem o caminho livre para a transmissão da sua trama de dados sem o risco de colisão.

Com a utilização do mecanismo de RTS/CTS é possível a ocorrência de colisões entre tramas RTS, tal como podem ocorrer colisões entre tramas de dados sem a sua utilização. Porém, como as tramas RTS são normalmente muito menores do que as tramas de dados, o tempo desperdiçado numa colisão é menor, podendo daí resultar um aumento da eficiência do protocolo de controlo de acesso ao meio, mesmo sem se considerar o problema da estação oculta.

A desvantagem óbvia da utilização do mecanismo de RTS/CTS está no aumento do *overhead*, principalmente na transmissão de tramas de dados de comprimento pequeno. Sendo assim, o mecanismo RTS/CTS é habilitado apenas quando o comprimento da trama de dados a enviar é maior do que valor especificado por um parâmetro denominado *RTS Threshold*.

5.3.2.2 Fragmentação

Quando o comprimento do MSDU (*MAC Service Data Unit*) é grande, a sua segmentação, seguida da inserção dos segmentos em múltiplas tramas de dados de dimensão reduzida (fragmentos), pode contribuir para o aumento da

fiabilidade da transmissão, pois quanto menor é o comprimento de uma trama, menor é a probabilidade dela ser corrompida por erros no canal. Sendo assim, a fragmentação pode resultar no aumento da eficiência do protocolo quando a probabilidade de erros de bit no canal for significativa, apesar do aumento do *overhead* (cabeçalhos, preâmbulos e períodos de guarda entre os fragmentos) que esta técnica introduz. A Figura 5.11 apresenta um exemplo da transmissão de uma trama de dados divida em dois fragmentos, em conjunto com a utilização do mecanismo RTS/CTS.

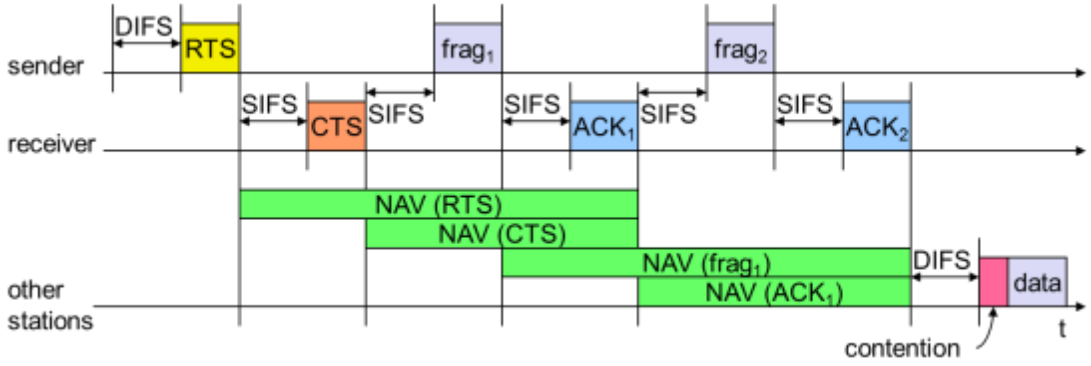

Figura 5.11: Exemplo de uso do mecanismo de fragmentação do IEEE 802.11 [Schi04].

A fragmentação é efetuada quando o comprimento da trama excede o valor definido pelo parâmetro *fragmentation threshold*. O comprimento dos fragmentos associados a um dado MSDU é igual ao valor deste parâmetro, com exceção do último fragmento, cujo tamanho depende do comprimento residual do último segmento proveniente do MSDU.

Os fragmentos associados a um mesmo MSDU são transmitidos em sequência, intercalados com as respetivas tramas ACK enviadas pelo recetor. A separação entre tramas consecutivas é de um período SIFS, pelo que o emissor mantém o controlo sobre o meio durante a transmissão dos fragmentos. O meio só é libertado após a transmissão de todos os fragmentos, ou então quando a sequência é interrompida, o que ocorre quando o emissor não recebe o reconhecimento positivo de um dado fragmento. Neste caso, o emissor inicia o processo de *backoff*, ao fim do qual transmite os restantes fragmentos associados ao MSDU, começando pelo primeiro fragmento que não obteve reconhecimento positivo.

Quando o mecanismo RTS/CTS é utilizado, as tramas RTS e CTS são transmitidas apenas uma vez, antes do primeiro fragmento. Os campos de duração destas tramas são usados para indicar a ocupação do meio somente até ao fim da primeira trama ACK, e não até ao fim da última trama ACK, pois isso inibiria a transmissão das outras estações até ao final previsto para a transmissão de todos os fragmentos, mesmo se a sequência fosse interrompida e, consequentemente, o meio ficasse livre antes. Os campos de duração do primeiro fragmento e da primeira trama ACK anunciam que o meio estará ocupado até ao final da segunda trama ACK, e assim por diante, até que todos os fragmentos tenham sido transmitidos.

5.3.3 Função de coordenação pontual (PCF)

Como o objetivo de proporcionar suporte a serviços com requisitos de tempo real, o IEEE 802.11 inclui a função de coordenação pontual (PCF). Este mecanismo de controlo de acesso ao meio utiliza um protocolo de *polling*, controlado pelo ponto de acesso (AP - *Access Point*), para determinar qual estação que tem direito de transmitir em dado momento. A função PCF é utilizada para o controlo de acesso ao meio durante o período livre de contenção (CFP, *Contention Free Period*), que alterna com o período de contenção (CP, *Contention Period*), no qual a função DCF é utilizada. A junção destes dois períodos resulta na chamada supertrama, como é representado na Figura 5.12. Além de transportar o tráfego assíncrono, o período de contenção possibilita o registo de novas estações na lista de *polling*.

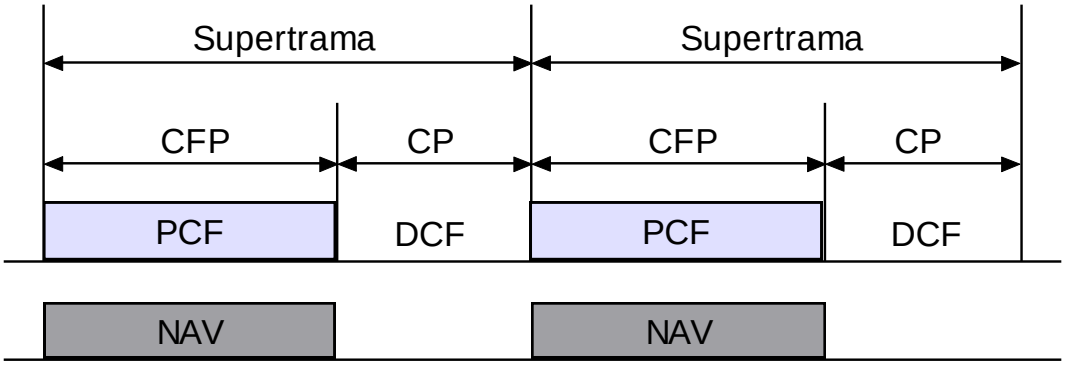

Figura 5.12: Coexistência das funções PCF e DCF na supertrama.

Para dar início a um novo período livre de contenção (CFP), o ponto de acesso aguarda que o canal permaneça livre durante um período PIFS (*PCF Interframe Space*) após o fim previsto do período de contenção (CP) da supertrama anterior, sendo válida a relação:

$$PIFS = SIFS + SlotTime, \tag{5.3}$$

o que implica que o período PIFS é maior que o SIFS e menor que o DIFS.

O período livre de contenção inicia-se com a transmissão da trama *Beacon* pelo ponto de acesso, como mostra a Figura 5.13. A seguir, é feita a interrogação das estações pertencentes à lista de *polling* usando a função PCF. A transmissão da trama CF-End, pelo ponto de acesso, encerra o período livre de contenção. Ao longo deste período, todas as tramas trocadas são espaçadas de um período SIFS.

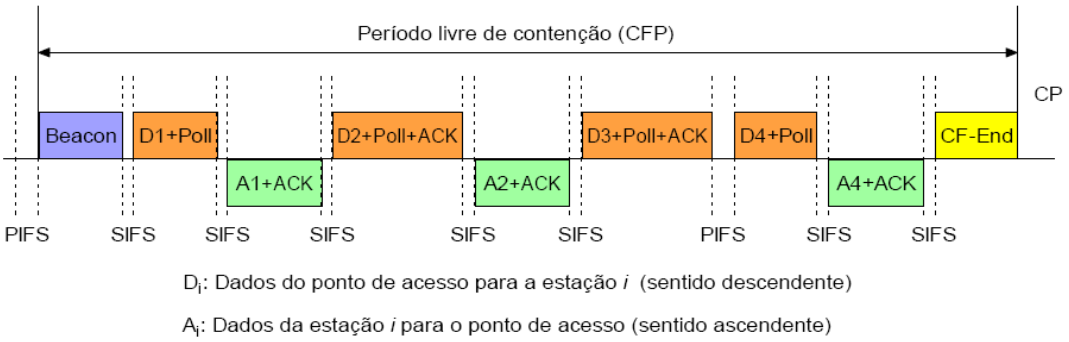

Figura 5.13: Exemplo de transmissões realizadas usando a função PCF.

A trama *Beacon* é uma trama de gestão utilizada para difundir diversas informações relacionadas com a operação da célula (BSS). Entre as informações associadas à função PCF, encontra-se o intervalo de repetição do período CFP, ou seja, a duração nominal da supertrama[16]. A trama *Beacon* inclui também o parâmetro *CFPMaxDuration*, que indica a duração máxima do período CFP atual, sendo utilizado pelas estações para atualizar os seus

[16] A duração da supertrama traduz-se por um múltiplo inteiro do intervalo entre tramas *Beacon*, pelo que, além da trama *Beacon* transmitida no início do período CFP, outras tramas *Beacon* podem ser transmitidas ao longo da supertrama.

temporizadores NAV. O valor máximo que este parâmetro pode assumir corresponde à duração nominal da supertrama menos o tempo necessário para a transmissão de um MPDU de comprimento máximo durante o período de contenção, incluindo as tramas de controlo associadas.

Durante o período livre de contenção, os seguintes subtipos de tramas de dados podem ser transmitidos[17]: Data, Data+CF-Ack, Data+CF-Poll, Data+CF-Ack+CF-Poll, Null Function (sem dados), CF-Ack (sem dados), CF-Poll (sem dados) e CF-Ack+CF-Poll (sem dados). Essas tramas são diferenciadas através dos campos tipo e subtipo inseridos no campo de controlo da trama do cabeçalho da camada MAC. As tramas contendo o CF-Poll só podem ser transmitidas pelo ponto de acesso, enquanto as outras tramas podem ser transmitidas por qualquer estação que seja capaz de comunicar usando a função PCF. A presença do CF-Poll autoriza a transmissão de dados pela estação de destino. A trama Null Function é utilizada pela estação quando é interrogada e não tem dados nem informação de reconhecimento positivo (CF-Ack) para transmitir.

Após receber dados de uma estação, o ponto de acesso pode enviar dados (Data) e interrogar (CF-Poll) a estação seguinte ao mesmo tempo que reconhece (CF-Ack) os dados recebidos da anterior. A capacidade do ponto de acesso de combinar a interrogação, o reconhecimento e os dados numa mesma trama foi concebida para aumentar a eficiência do protocolo.

Quando o ponto de acesso interroga uma estação e esta não inicia a sua transmissão no momento esperado (ou seja, decorrido um período SIFS), o ponto de acesso retoma o controlo do canal após um período PIFS, dando sequência à interrogação das estações presentes na lista de *polling*. No exemplo da Figura 5.13, esta situação ocorre quando a estação 3 é interrogada.

Ao ser interrogada pelo ponto de acesso, uma estação pode enviar uma trama de dados para outra estação, que responde com uma trama ACK com

[17] CF significa *Contention Free*.

formato idêntico ao utilizado com a função DCF. Depois disso, o ponto de acesso reassume o controlo do canal, após aguardar durante um período PIFS. De modo análogo, o ponto de acesso pode transmitir uma trama de dados para uma estação que não reconhece a função PCF durante o período livre de contenção, e esta responde com uma trama ACK da função DCF.

Se no instante previsto para o início do período livre de contenção (CFP) o meio estiver ocupado com uma transmissão inacabada associada ao período de contenção (tráfego DCF), o ponto de acesso tem que esperar pelo fim da transmissão para adquirir o controlo do canal. Porém, o período livre de contenção não se pode prolongar para além do limite especificado pelo parâmetro *CFPMaxDuration*, pelo que a sua duração máxima permitida, nessa supertrama, sofre uma redução, como é exemplificado na Figura 5.14. Como uma transmissão pode iniciar-se imediatamente antes do término previsto para o período de contenção, o período livre de contenção pode sofrer uma redução, no pior caso, igual ao tempo total necessário para a transmissão de um MPDU de comprimento máximo e as tramas de controlo associadas. O encurtamento do período livre de contenção provocado pelo alargamento (*stretching*) do período de contenção diminui a largura de banda disponível para o transporte do tráfego PCF, além aumentar o *jitter* dos fluxos.

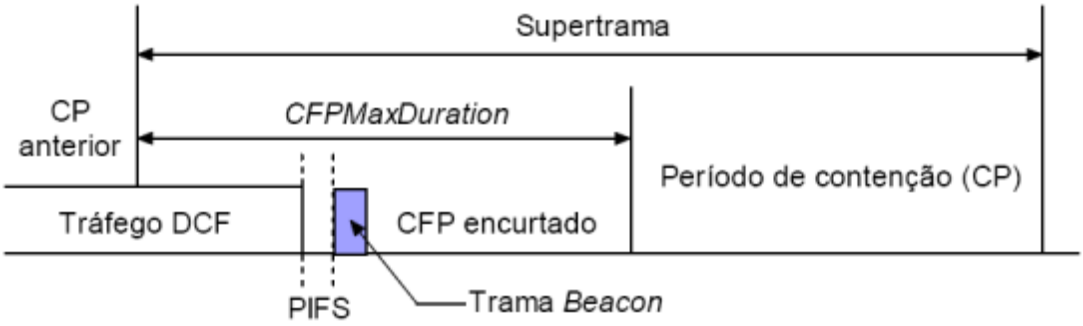

Figura 5.14: Exemplo de encurtamento do período livre de contenção.

5.4 802.11e

O grupo de tarefas E do 802.11 (TGe) desenvolveu a norma IEEE 802.11e [IEEE05], cujo objetivo é aperfeiçoar o protocolo de controlo de acesso ao meio

do IEEE 802.11, de forma a aumentar a eficiência e o suporte de qualidade de serviço. Esses aprimoramentos são também conhecidos pelas designações WMM (Wi-Fi *Multimedia*) e WME (*Wireless Multimedia Extensions*).

A norma IEEE 802.11e define um novo modo de operação para o controlo de acesso ao meio, designado função de coordenação híbrida (HCF, *Hybrid Coordination Function*), que combina acesso baseado em contenção e acesso controlado. O mecanismo de acesso baseado em contenção da função HCF é denominado EDCA (*Enhanced Distributed Channel Access*). O EDCA é um aprimoramento da função DCF do IEEE 802.11, sendo também conhecido como EDCF (*Enhanced Distributed Coordination Function*). Por sua vez, o mecanismo de acesso controlado, denominado HCCA (*HCF Controlled Channel Access*) consiste num aprimoramento da função PCF. A entidade responsável pelo controlo da qualidade de serviço numa célula que suporta o IEEE 802.11e (QBSS - *QoS Basic Service Set*) recebe a designação de coordenador híbrido (HC - *Hybrid Coordinator*) e reside no ponto de acesso. Uma estação compatível com a norma IEEE 802.11e recebe a designação QSTA (*QoS-enhanced Station*).

5.4.1 Oportunidade de transmissão

O IEEE 802.11 introduz um novo conceito, a oportunidade de transmissão (TXOP - *Transmission Opportunity*), que consiste num intervalo de tempo máximo no qual a estação tem direito de ocupar o canal de modo contínuo. Este parâmetro permite que o coordenador híbrido possa impor um limite à duração das transmissões das QSTAs, obtendo assim maior controlo sobre o acesso ao meio e podendo com isso gerir melhor a qualidade de serviço oferecida aos diferentes fluxos. A duração do TXOP para o EDCA é definida por um parâmetro incluído nas tramas *Beacon*, enquanto sua duração no caso do HCCA é especificada nas tramas de interrogação.

Uma QSTA deve abster-se de transmitir um MPDU se o período necessário para transmissão (incluindo as tramas de controlo associadas) exceder a duração da sua oportunidade de transmissão. De igual modo, uma QSTA deve

evitar a transmissão se não puder terminá-la antes do instante previsto para o início de transmissão da próxima trama *Beacon* (TBTT - *Target Beacon Transmission Time*). Consegue-se com isso evitar o problema do encurtamento do período livre de contenção, desde que não existam estações na rede que só reconheçam a função DCF.

O IEEE 802.11e também permite que uma estação transmita múltiplos MPDUs em sequência, utilizando um novo mecanismo denominado CFB (*Contention Free Burst*), desde que a duração da respetiva oportunidade de transmissão não seja ultrapassada, como é exemplificado na Figura 5.15. Este mecanismo foi introduzido com o objetivo de aumentar a eficiência do protocolo de controlo de acesso ao meio.

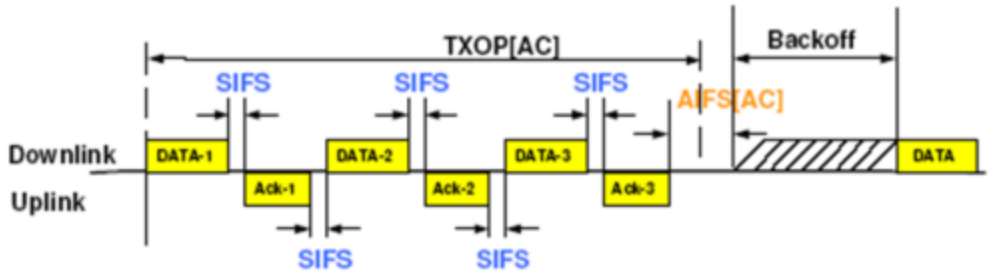

Figura 5.15: Exemplo de operação do mecanismo CFB do IEEE 802.11e [Schi04].

5.4.2 Acesso baseado em contenção

O mecanismo EDCA permite a diferenciação de serviços na rede IEEE 802.11 através da classificação dos fluxos em diferentes classes de tráfego denominadas categorias de acesso (AC - *Access Category*), em função da sua prioridade. Cada categoria de acesso é uma variante da função DCF que compete pelo acesso ao meio utilizando o seu próprio conjunto de parâmetros de *backoff*, que incluem o AIFS[AC] (*Arbitration Interframe Space*, análogo ao DIFS da função DCF), o CW_{min}[AC] e o CW_{max}[AC].

Para que o coordenador híbrido tenha prioridade no acesso ao meio em relação às demais estações, o período AIFS[AC] mínimo deve ser maior que o PIFS, pelo que não pode ser inferior ao DIFS, ou seja:

$$AIFS[AC] = SIFS + AIFSN[AC] \cdot SlotTime, \qquad (5.4)$$

onde AIFSN[AC] é um número inteiro maior ou igual a 2. A Figura 5.16 apresenta um exemplo de valores atribuídos aos parâmetros de *backoff* de quatro categorias de acesso (listadas por ordem de prioridade): voz (VO), vídeo (VI), *best effort* (BE) e *background* (BK).

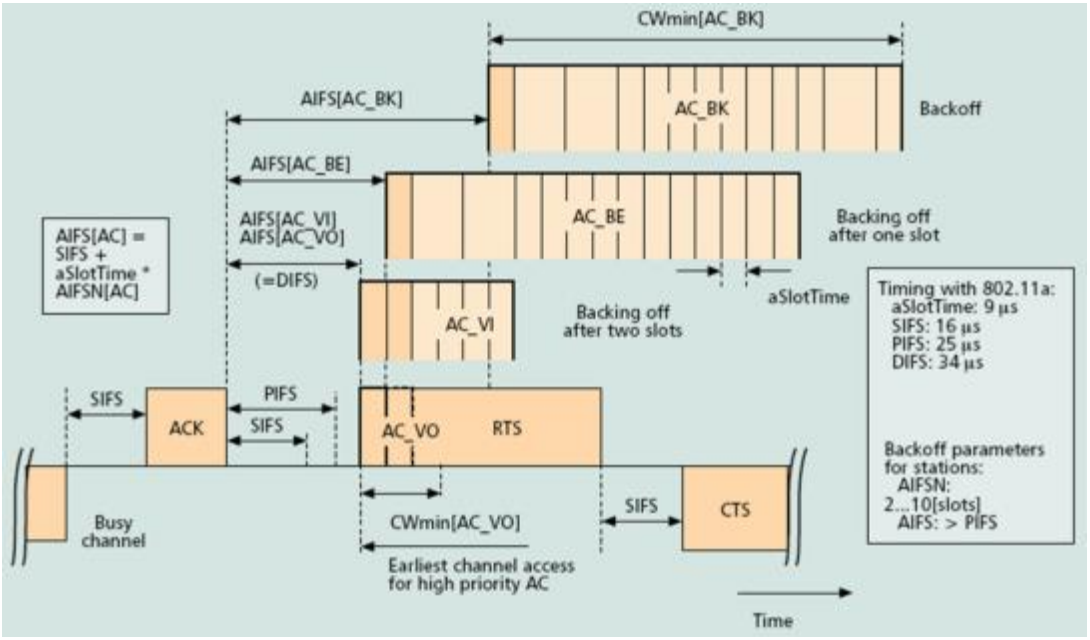

Figura 5.16: Parâmetros de *backoff* do mecanismo EDCA [Mang03].

Os valores dos parâmetros de *backoff* são anunciados pelo ponto de acesso na trama *Beacon*. Valores menores para os parâmetros de uma categoria de acesso aumentam a probabilidade de obter acesso ao meio para essa categoria, em caso de contenção com outras categorias de acesso. Desta forma, a diferenciação de serviços no mecanismo EDCA é obtida estatisticamente, pelo aumento da probabilidade de acesso ao meio para os fluxos com maior prioridade, e vice-versa. O ponto de acesso pode ajustar esses parâmetros dinamicamente em função das condições na rede para melhor satisfazer a qualidade de serviço das aplicações.

Cada estação que implementa o IEEE 802.11e (QSTA) pode possuir até quatro categorias de acesso (AC) para o suporte de oito níveis de prioridade (UP - *User Priority*), conforme definidos na norma 802.1d [IEEE98], sendo que cada nível de prioridade é mapeado numa categoria de acesso.

Cada categoria de acesso no interior de uma estação comporta-se como uma estação virtual, com a sua própria fila de espera, competindo pelo acesso ao meio e executando o processo de *backoff* de forma independente, como mostra a Figura 5.17. A diferença é que não ocorrem colisões internas quando duas ou mais categorias de acesso numa mesma estação terminam o processo de *backoff* em simultâneo. Neste caso, a estação atribui a oportunidade de transmissão à categoria de acesso mais prioritária, enquanto as demais categorias de acesso envolvidas comportam-se como se tivesse havido uma colisão externa, ou seja, incrementam a janela de contenção, calculam novo período de *backoff* e voltam a tentar aceder ao meio para transmitir o pacote (se o número máximo de tentativas não tiver sido atingido).

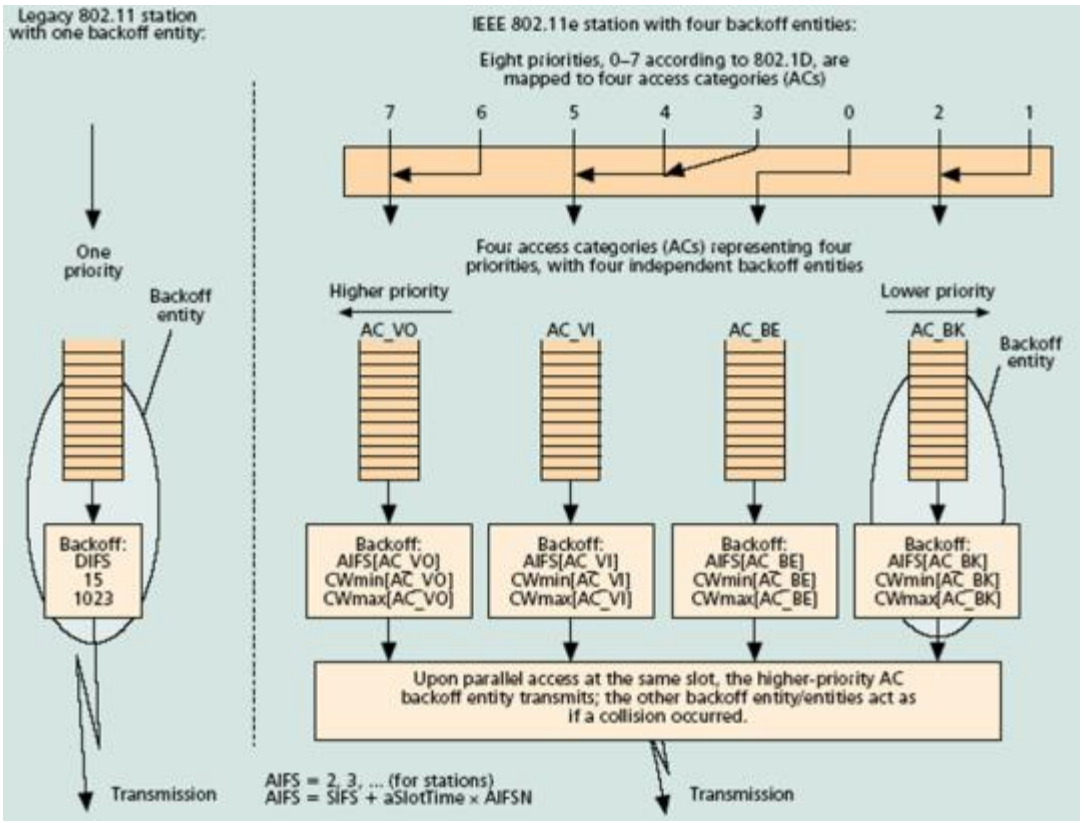

Figura 5.17: Exemplo de estações virtuais do mecanismo EDCA [Mang03].

5.4.3 Acesso controlado

O mecanismo de acesso controlado do IEEE 802.11e (HCCA) é baseado em *polling*, tal como a função PCF do IEEE 802.11. No entanto, ao contrário

desta, sua ação não está restrita ao período livre de contenção (CFP), pois permite que o ponto de acesso interrogue as estações durante o período de contenção (CP), bastando para isso que o meio permaneça livre por um período PIFS.

No HCCA, o coordenador híbrido é responsável pelo controlo de admissão e pelo escalonamento de tráfego de forma a proporcionar a qualidade de serviço negociada com as estações. Para poder utilizar o HCCA, a QSTA deve submeter uma requisição ao controlador híbrido, contendo a especificação de tráfego (TSPEC - *Traffic Specification*). O elemento TSPEC contém uma série de parâmetros que definem as características de tráfego e expectativas de qualidade de serviço associadas a um dado fluxo unidirecional. Os parâmetros considerados mais relevantes são:

- *Mean data rate* (ρ): débito médio de transferência dos pacotes.
- *Delay bound* (D): atraso máximo para a transferência do pacote na rede sem fios, incluindo o atraso na fila de espera.
- *Nominal* MSDU *size* (L): comprimento nominal dos pacotes.
- *User priority* (UP): prioridade utilizada no transporte dos pacotes com base nos níveis de prioridade definidos na norma 802.1d.
- *Maximum* MSDU *size* (M): comprimento máximo dos pacotes.
- *Maximum Burst Size* (MBS): comprimento máximo do *burst*.
- *Minimum* PHY *rate* (R): débito ao nível da camada física assumido pelo escalonador.
- *Peak data rate* (PR): débito máximo permitido.

Cabe ao coordenador híbrido avaliar se há recursos suficientes disponíveis para satisfazer a TSPEC requerida, podendo propor uma TSPEC alternativa (eventualmente com um nível de qualidade de serviço inferior) ou mesmo rejeitar a requisição por completo.

5.4.3.1 Outros aprimoramentos

Na norma IEEE 802.11 original, duas estações associadas a um BSS que opere em modo baseado em infraestrutura não podem comunicar diretamente entre si, mesmo que estejam ao alcance uma da outra. Neste caso, a estação emissora tem que enviar os dados para o ponto de acesso, que os retransmite para a estação de destino, pelo que este processo é pouco eficiente quando grande parte da comunicação se dá entre estações no mesmo BSS. Visando proporcionar a comunicação direta entre as estações num mesmo BSS, a norma IEEE 802.11e inclui um protocolo de ligação direta (DLP - *Direct Link Protocol*), de implementação opcional. Antes de iniciar a comunicação direta, as QSTAs envolvidas devem negociar com o ponto de acesso os parâmetros de transmissão utilizando o mecanismo de sinalização definido no protocolo.

No IEEE 802.11, o *overhead* associado à transmissão das tramas ACK após cada trama de dados recebida sem erros tem impacto sobre a eficiência do protocolo de controlo de acesso ao meio, tanto mais porque a trama ACK, por ser uma trama de controlo, pode ter que ser transmitida utilizando um modo de transmissão inferior ao utilizado pela trama de dados. Com o objetivo de aumentar a eficiência, a norma IEEE 802.11e define um mecanismo de reconhecimento de grupo (*Group* ACK) opcional, que permite que uma estação transmita uma sequência de tramas de dados, separadas por um período SIFS, sem que seja necessário que o recetor reconheça individualmente cada uma. O reconhecimento das múltiplas tramas de dados passa a ser feito, neste caso, por uma única trama ACK de grupo.

Referências

[IEEE98] IEEE 802.1D, “IEEE standard for local and metropolitan area networks - Common specifications - Media access control (MAC) Bridges”, 1998.

[IEEE99] IEEE 802.11 (ISO/IEC 8802-11:1999), “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, 1999.

[IEE99a] IEEE 802.11 (8802-11:1999/Amd 1:2000(E)), “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - High-speed Physical Layer in the 5 GHz Band”, 1999.

[IEE99b] IEEE 802.11, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Higher-Speed Physical Layer Extension in the 2.4 GHz Band”, 1999.

[IEEE05] IEEE Std 802.11e-2005, “IEEE Std“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements”, November 2005.

[Mang03] S. Mangold et al., “Analysis of IEEE 802.11e for QoS Support in Wireless LANs”, IEEE Wireless Communications, pp. 40-50, December 2003.

[Schi04] J. Schiller, “Mobile Communications”, 2nd edition, Addison-Wesley, 2004.

6. Bluetooth

6.1 Introdução

O Bluetooth [Haar00] [Blue01] [Joha99] é uma tecnologia de rádio de curto alcance vocacionada para a transmissão de tráfego de voz e dados cujo objetivo principal é a substituição dos cabos na conexão entre dispositivos eletrónicos de uso pessoal. O baixo custo e baixo consumo das interfaces são propícios à generalização da sua utilização em dispositivos pessoais. A comunicação entre os dispositivos compatíveis com o Bluetooth tem a vantagem de não requer a existência de linha de vista (LOS - *Line Of Sight*) entre o emissor e o recetor, ao contrário do IrDA, que era a tecnologia mais utilizada para a comunicação entre dispositivos pessoais na altura em que o Bluetooth foi introduzido.

A não ser que seja explicitamente referido, a descrição feita neste capítulo é baseada na versão 1.1 do Bluetooth, que foi a primeira versão a atingir sucesso comercial, tendo corrigido vários erros encontrados na versão 1.0B. As principais funcionalidades introduzidas pelas versões seguintes do Bluetooth são referidas na secção 6.6.

As redes Bluetooth operam sem necessidade de licença na banda ISM dos 2.4 GHz, utilizando a técnica de espalhamento espectral por saltos em frequência (FHSS). A banda de frequências disponível é dividida em 79 canais[18], com separação de 1 MHz entre as frequências das portadoras. Durante a operação da rede, o canal utilizado é alterado após cada transmissão, em função da sequência pseudo-aleatória adotada. O Bluetooth, na sua versão original, utiliza modulação GFSK (*Gaussian Frequency Shift Keying*) e proporciona um débito bruto de 1 Mbit/s. O alcance nominal do

[18] Na Espanha, na França e no Japão estão disponíveis apenas 23 canais.

Bluetooth situa-se entre 10 cm e 10 m, mas pode ser estendido até 100 m com a utilização de um amplificador de potência externo.

Na interligação de dois dispositivos, aquele que inicia a conexão é denominado mestre, enquanto o outro é conhecido como escravo. Um mestre pode manter conexões com no máximo sete escravos ao mesmo tempo, formando uma pequena rede conhecida pela denominação de *piconet*. A estação que estabelece a *piconet* torna-se o mestre. O mestre é responsável pelo controlo de acesso ao meio dentro da *piconet*, cuja operação é baseada num protocolo de *polling*. As transmissões são feitas, alternadamente, pelo mestre e pelo escravo destinatário da transmissão realizada pelo mestre. Um exemplo de *piconet* é apresentado na Figura 6.1.

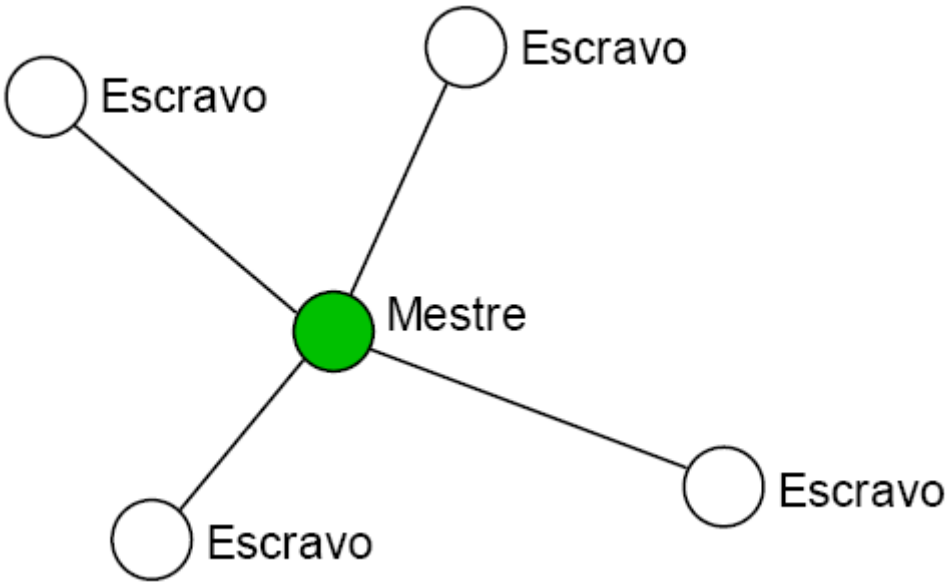

Figura 6.1: Exemplo de uma *piconet* formada por cinco dispositivos.

Cada dispositivo Bluetooth possui um endereço de dispositivo único, formado por 48 bits. A sequência de saltos utilizada numa *piconet* é única, sendo determinada pelo endereço do mestre, enquanto a fase da sequência é determinada pelo relógio do mestre. O uso de sequências pseudo-aleatórias de saltos distintas contribui para a coexistência de múltiplas *piconets* estabelecidas numa mesma área, ao minimizar a sobreposição das transmissões resultantes da utilização de um mesmo canal em simultâneo. A

princípio, qualquer dispositivo Bluetooth pode atuar como mestre ou como escravo, podendo o papel de um dispositivo alterar-se ao ser estabelecida uma nova *piconet*. Transmissões diretas de escravo para escravo não são permitidas dentro de uma *piconet*, pelo que se dois escravos desejam comunicar devem fazê-lo por intermédio do mestre da *piconet* ou, em alternativa, devem formar uma outra *piconet* em que um deles é mestre.

Múltiplas *piconets* interligadas entre si formam uma *scatternet*, como é exemplificado na Figura 6.2. A interligação de duas *piconets* é concretizada quando um dispositivo faz parte das duas *piconets*. Mesmos estando interligadas, diferentes *piconets* utilizam sequências pseudo-aleatórias de saltos distintas. Como as unidades de rádio só podem estar sintonizadas num canal em cada instante, o dispositivo só pode comunicar com uma *piconet* de cada vez. O dispositivo pode ser mestre numa *piconet* e escravo em outra, ou pode ser escravo nas duas, mas não pode ser mestre em duas *piconets* ao mesmo tempo, porque isso implica que as sequências de saltos seriam idênticas.

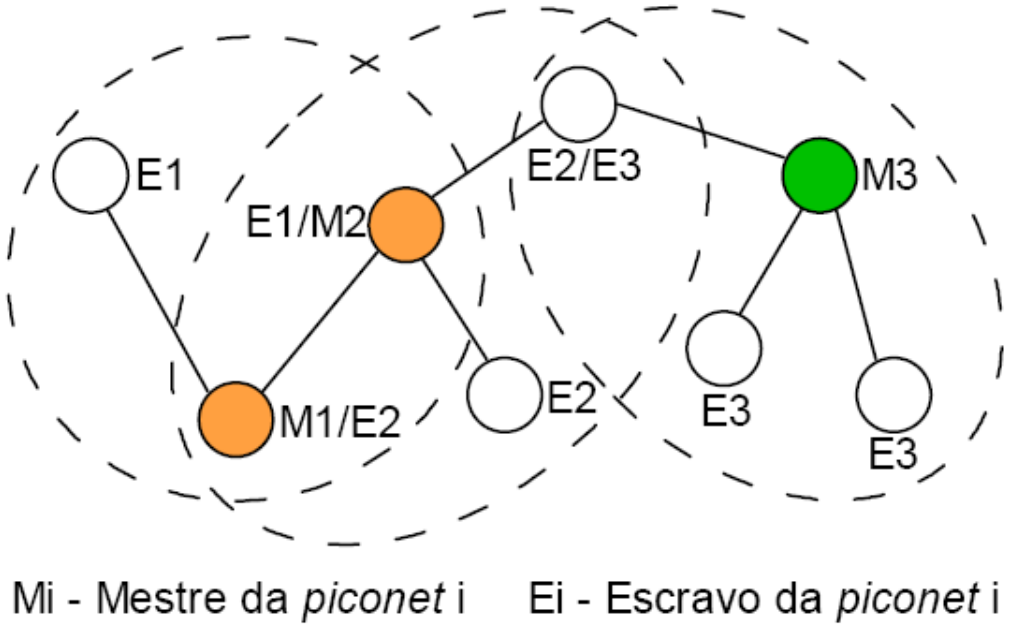

Figura 6.2: Exemplo de uma *scatternet* formada por três *piconets*.

O Bluetooth divide o tempo em *slots* de duração igual a 625 μs, sendo que os pacotes transmitidos podem ocupar um, três ou cinco *slots*. A sequência pseudo-aleatória utilizada para os saltos em frequência avança a cada transição de *slot*. No entanto, os pacotes que ocupam múltiplos *slots* são transmitidos sem mudança da frequência da portadora. Na transmissão do pacote seguinte, a frequência da portadora salta para o valor da sequência pseudo-aleatória correspondente ao *slot* em que a transmissão é iniciada, como é exemplificado na Figura 6.3.

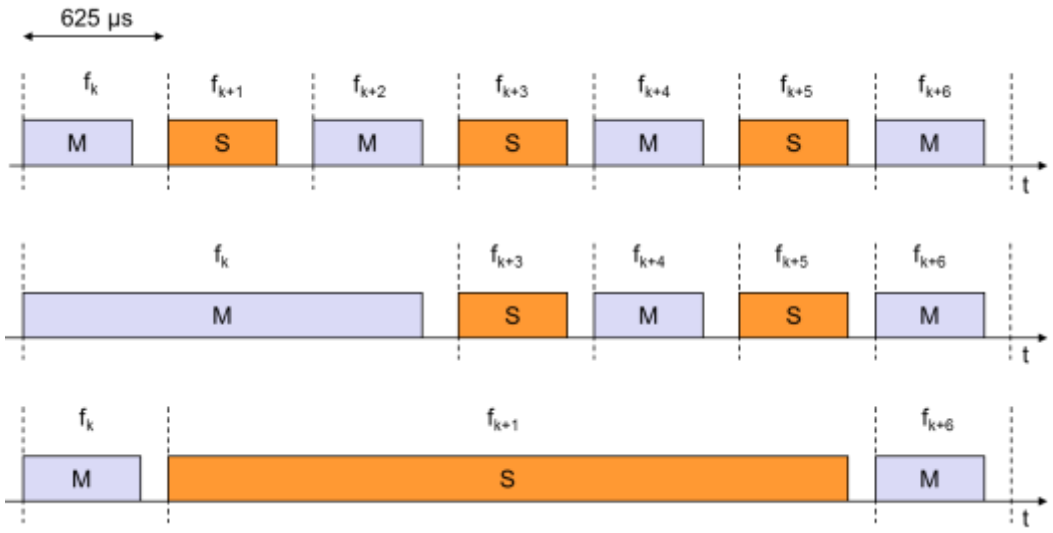

Figura 6.3: Relação entre os tamanhos de pacotes e os saltos em frequência [Schi04].

O Bluetooth define que o intervalo mínimo entre o fim da transmissão de um pacote num sentido e o início da transmissão de um pacote no sentido oposto[19] deve ser de 200 μs. Este período é relativamente elevado comparado com os intervalos definidos por redes como o IEEE 802.11; porém, isso permite a utilização de componentes de mais baixo custo.

[19] Este período é chamado *turnaround time*.

6.2 Arquitetura protocolar

O *core* da pilha protocolar do Bluetooth (ou seja, as funcionalidades definidas pelas especificações do Bluetooth) é formado por dois blocos principais: o Host (anfitrião) e um ou vários Controllers (controladores). A comunicação entre o Host e o Controller é padronizada através da interface HCI (*Host Controller Interface*). O bloco Controller, situado abaixo da interface HCI, inclui as camadas físicas e a camada de ligação (*link layer*), enquanto o bloco Host é constituído pelas camadas acima da interface HCI e abaixo dos perfis de utilização.

A versão 1.0 do Bluetooth define somente o controlador BR (*Basic Rate*), que inclui as camadas de rádio, *baseband*, e *link manager*. A versão 2.0 introduziu o EDR (*Enhanced Data Rate*) A versão 3.0 do Bluetooth [Blue09] define dois tipos de controladores: BR/EDR e AMP (*Alternate MAC/PHY*), que é novo nesta versão, acrescentando a função HS (*High Speed*). Este controlador é secundário, e permite que, após dois dispositivos efetuarem uma conexão via BR/EDR, se for encontrado o controlador AMP no outro dispositivo, o tráfego de dados possa ser movido do controlador BR/EDR para o controlador AMP e os dados serem transferidos via Wi-Fi. Basicamente, o controlador AMP utiliza a camada física e MAC do IEEE 802.11 para dar suporte à transmissão de grandes quantidades de tráfego.

A Figura 6.4 apresenta as possíveis arquiteturas da versão 3.0 do Bluetooth, combinando o bloco Host com o(s) bloco(s) Controller(s). Em a) existe apenas o controlador BR/EDR; em b) os controladores BR/EDR e AMP; e em c) o controlador BR/EDR com múltiplos controladores AMP.

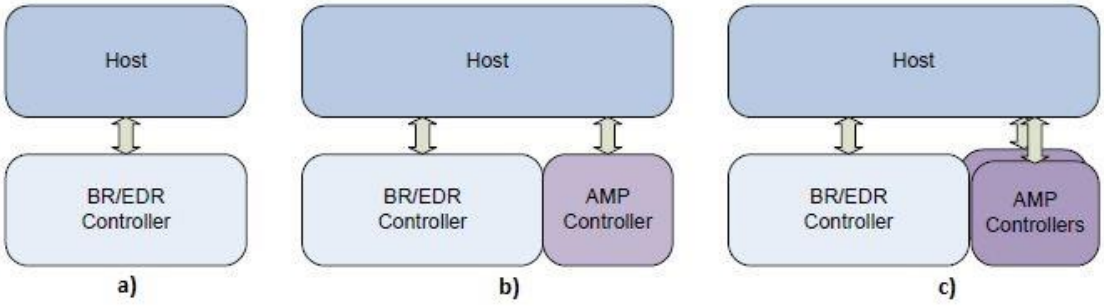

Figura 6.4. Arquiteturas do Bluetooth 3.0 [Maio14].

Em termos de débito, o Bluetooth possui um débito de 1 Mbps para a versão Basic Rate (BR), e entre 2 Mbps a 3 Mbps para a versão Enhanced Data Rate (EDR), dependendo do tipo de modulação que é usada. Pode ainda alcançar um débito de 24 Mbps caso seja usada a transmissão do tráfego via ligação Wi-Fi (IEEE 802.11). O Bluetooth suporta 3 tipos de modulação que são GFSK (*Gaussian Frequency Shift Keying*), que oferece um débito de 1Mbps; PSK (*Phase Shift Keying*), que oferece um débito de 2 Mbps; e por último a 8DPSK (*8-ary Differential Phase Shift Keying*), com um débito de 3 Mbps.

6.3 Formato dos pacotes

Todos os pacotes transmitidos no canal possuem o mesmo formato[20], constituído por três campos, como ilustra a Figura 6.5: o código de acesso (72 bits); o cabeçalho do pacote (54 bits); e o *payload*, cujo comprimento pode variar entre 0 e 2745 bits.

[20] À exceção do pacote de identidade (ID), usado para sinalização, que contém apenas o campo de código de acesso.

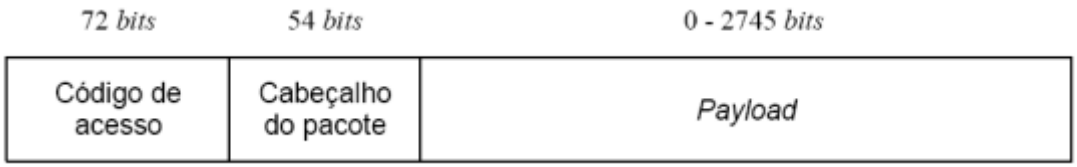

Figura 6.5: Formato do pacote do Bluetooth.

O código de acesso (*access code*) é definido pelo mestre e identifica os pacotes transmitidos no âmbito de uma *piconet.* Os pacotes transmitidos apenas são aceites por um recetor se a sua identidade é reconhecida nessa *piconet*. O código de acesso também é utilizado para sincronização, compensação do *offset* de corrente contínua e sinalização.

O cabeçalho do pacote contém informação utilizada para o controlo da ligação. Os 18 bits de informação do cabeçalho são protegidos por um código de correção de erros (FEC) de taxa 1/3, o que faz com que o cabeçalho ocupe 54 bits no total. Os campos existentes no cabeçalho, representados na Figura 6.6, possuem as seguintes funções:

- AM_ADDR (*active member address*): Contém um endereço que serve para identificar um escravo ativo da *piconet*. Tanto os pacotes enviados do mestre para o escravo quanto os pacotes enviados no sentido contrário transportam o endereço do escravo. O endereço 000 é reservado para mensagens de difusão (*broadcast*). Como os endereços são formados por três bits, no máximo sete escravos ativos são suportados numa *piconet*. Outros escravos podem fazer parte da *piconet* num estado inativo de baixo consumo de energia.
- TYPE: Define o tipo de pacote utilizado. A sua interpretação depende do tipo de ligação (síncrona ou assíncrona). Estas ligações são descritas mais abaixo.
- FLOW: É utilizado para controlo de fluxo nas ligações assíncronas.
- ARQN: Serve para reconhecimento do pacote enviado no *slot* anterior. É utilizado pelo esquema de deteção de erros e retransmissão (ARQ).
- SEQN: Contém o número de sequência utilizado pelo esquema de ARQ.

- HEC (*Header Error Check*): Serve para deteção de erros no cabeçalho. Em caso de erro, o pacote é descartado.

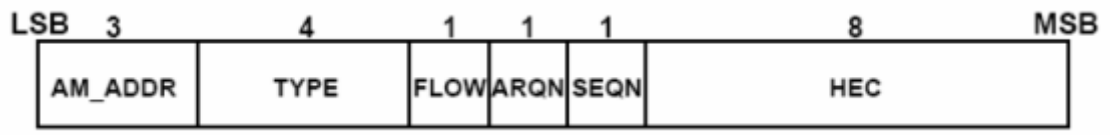

Figura 6.6: Formato do cabeçalho do pacote na rede Bluetooth.

Além dos pacotes de dados, são definidos os seguintes pacotes de controlo:

- *Identification Packet* (ID): Contém apenas o código de acesso. Utilizado para sinalização (por exemplo, durante o processo de estabelecimento de conexão).
- FHS *(FH-Synchronization) Packet:* Utilizado para a troca de informação de identidade e relógio. Contém a informação necessária para garantir que dois dispositivos efetuem os saltos em frequência de forma sincronizada.
- NULL *Packet:* Contém apenas o código de acesso e o cabeçalho do pacote. Utilizado quando não há dados no pacote.
- POLL *Packet:* Similar ao pacote NULL. Utilizado pelo mestre quando interroga um escravo e não tem dados para transmitir.

6.4 Ligações de dados

Para a comunicação entre o mestre e os escravos, dois tipos de ligação de dados foram definidos:

- Ligação SCO (*Synchronous Connection-Oriented*);
- Ligação ACL (Asynchronous Connection-Less).

A ligação SCO é uma ligação ponto a ponto simétrica entre o mestre e um escravo, e utiliza pacotes que ocupam um único *slot*. A ligação é estabelecida pela reserva de pares de *slots* consecutivos (um para cada sentido de comunicação) em intervalos regulares, pelo que se pode dizer que a ligação opera em modo circuito.

A ligação SCO suporta pacotes dos tipos HV1, HV2 e HV3 (Figura 6.7), de *High-rate Voice*, que transportam tráfego de voz a um débito útil de 64 kbit/s. Os dois primeiros tipos utilizam taxas de codificação FEC de 1/3 e 2/3, respetivamente, no seu *payload*, enquanto o terceiro transmite a informação de voz sem codificação FEC. A ligação SCO suporta ainda pacotes do tipo DV (*Data-Voice*), que transportam dados e voz em simultâneo.

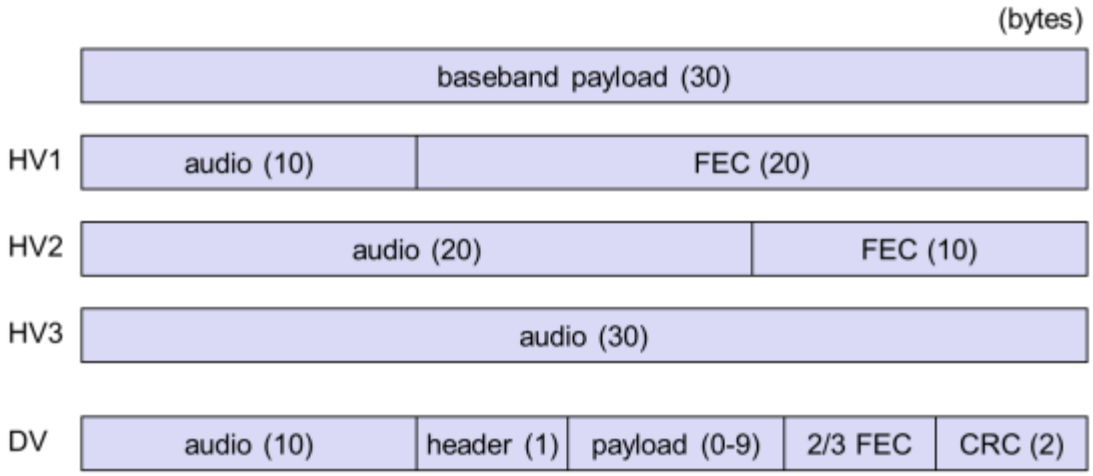

Figura 6.7: Tipos e formatos dos pacotes da ligação SCO [Schi04].

O codificador de voz do Bluetooth gera 10 bytes a cada 1.25 ms. Dado que o comprimento do *payload* dos pacotes que ocupam um *slot* é de 30 bytes, as conexões HV3 ocupam um *slot* a cada 3.75 ms (6 *slots*), em cada sentido de comunicação. Isso significa que, no máximo, três conexões de voz podem ser suportadas dentro de uma *piconet*. As conexões HV2 reduzem o comprimento útil do *payload* para 20 bytes, pelo que estas ocupam um par de *slots* em cada 4 *slots*. Já no caso das conexões HV1, o comprimento útil do *payload* é de 10 bytes, pelo que estas ocupam um par de *slots* em cada 2 *slots*, fazendo com que toda a largura de banda disponível na *piconet* seja ocupada por uma única conexão de voz.

A ligação ACL é uma ligação ponto-multiponto entre o mestre e os escravos da *piconet* que faz uso dos *slots* que não foram reservados pelas ligações SCO. Os diferentes tipos de pacotes definidos no Bluetooth podem ocupar um, três ou cinco *slots* e podem utilizar uma taxa de codificação FEC de 2/3 no seu *payload* (pacotes DM - *Data Medium rate*) ou serem transmitidos sem

codificação FEC (pacotes DH - *Data High rate*). A Figura 6.8 apresenta os tipos e formatos dos pacotes da ligação ACL.

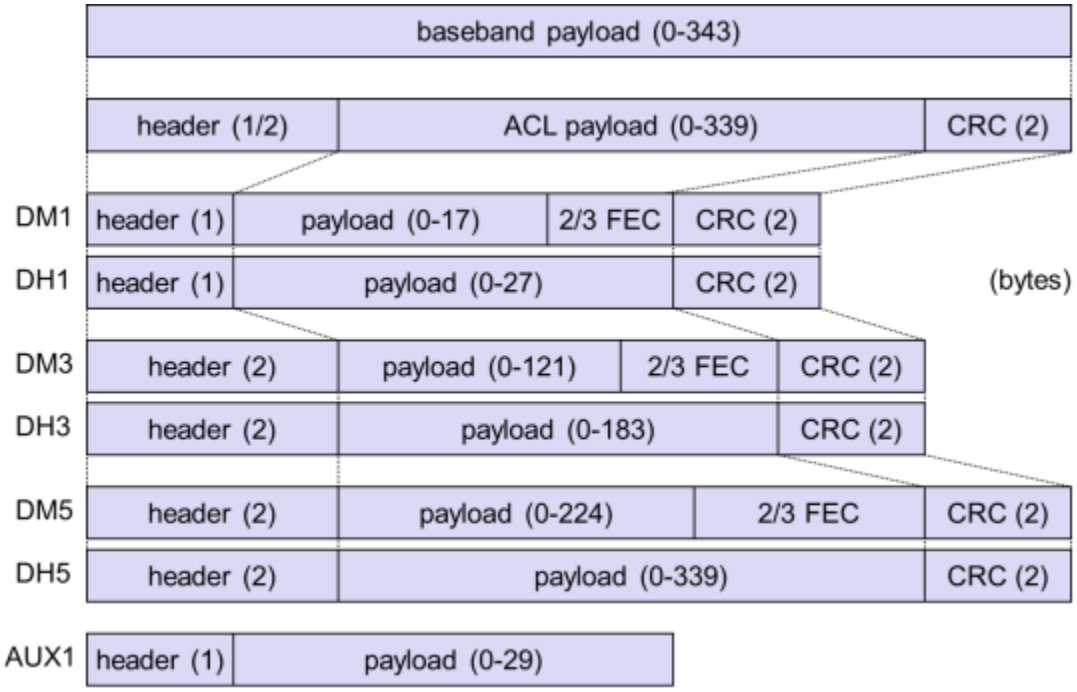

Figura 6.8: Tipos e formatos dos pacotes da ligação ACL [Schi04].

O *payload* dos pacotes transmitidos numa ligação ACL inclui um cabeçalho (1 byte nos pacotes que ocupam um *slot* e 2 bytes nos outros casos) e um campo de CRC (16 bits), ausente apenas nos pacotes do tipo AUX1. O débito assimétrico máximo que pode ser obtido é de 723.2 kbit/s, suportando uma ligação de retorno de 57.6 kbit/s; enquanto o débito simétrico máximo suportado é igual a 432.6 kbit/s.

O mestre, responsável pelo controlo de acesso ao meio, utiliza o mecanismo de *polling* para comunicar com os escravos. As ligações ACL fazem uso dos *slots* não ocupados por ligações SCO. A Figura 6.9 apresenta um exemplo da coexistência de ligações SCO (síncronas) e ligações ACL (assíncronas) numa mesma *piconet*, onde é representada uma ligação SCO do tipo HV3 com o escravo A e ligações ACL com os escravos A, B e C.

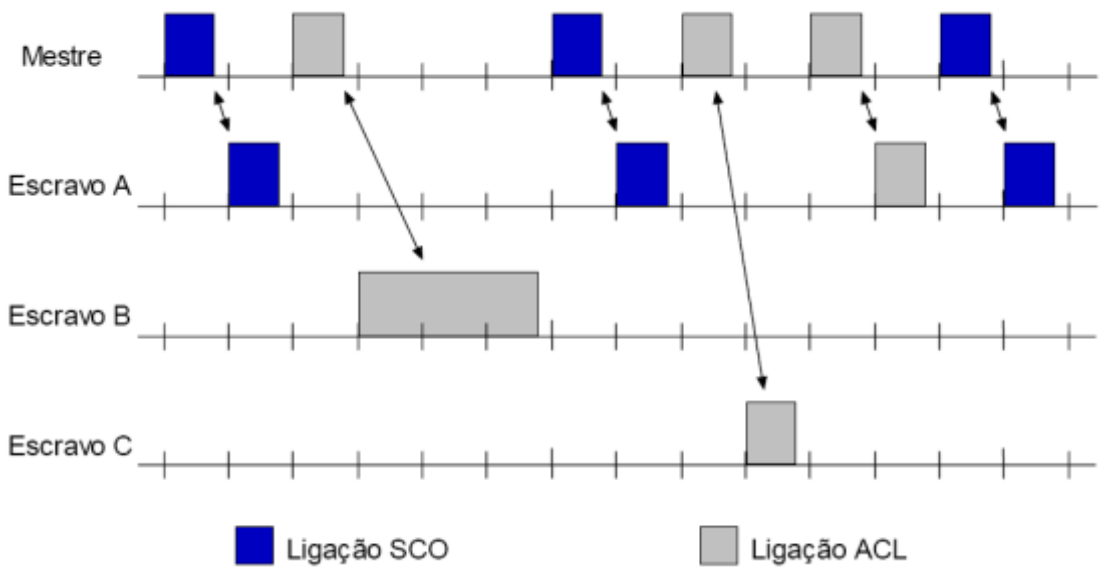

Figura 6.9: Exemplo da coexistência de ligações SCO e ACL numa mesma *piconet*.

6.5 Controlo de erros

O controlo de erros no Bluetooth baseia-se tanto na correção de erros (FEC) como na deteção de erros com retransmissão de pacotes (ARQ). No caso do FEC, códigos de taxas de 1/3 ou 2/3 são utilizados. O código FEC de taxa 1/3 é utilizado no cabeçalho do pacote e pode também ser aplicado ao *payload* dos pacotes em ligações SCO. Já o código FEC de taxa 2/3 pode ser aplicado ao *payload* dos pacotes tanto em ligações SCO como em ligações ACL. Nos dois casos, também existe a opção de não proteger o *payload* com um código FEC. Quanto maior for a redundância introduzida pelo código FEC, menor é o espaço que sobra no pacote para a transmissão de informação útil, pelo que o aumento da robustez das comunicações tem como contrapartida a redução do débito útil.

O esquema de deteção de erros e retransmissão de pacotes (ARQ) pode ser aplicado somente às ligações ACL. Neste caso, o esquema utiliza o campo de CRC presente no *payload* dos pacotes para deteção de erros. O reconhecimento positivo (ACK) ou negativo (NAK) é feito no pacote seguinte da mesma ligação ACL transmitido no sentido oposto, como é exemplificado na Figura 6.10. Para esse efeito, utiliza-se o campo ARQN presente no

cabeçalho dos pacotes, de modo que os dispositivos podem enviar os seus dados ao mesmo tempo que fazem o reconhecimento da transmissão anterior. O número de sequência (SEQN) de 1 bit é suficiente para detetar a receção de uma segunda cópia sem erros (duplicado) de um mesmo pacote, situação que pode ocorrer caso o pacote contendo o reconhecimento positivo da primeira cópia seja corrompido por erros.

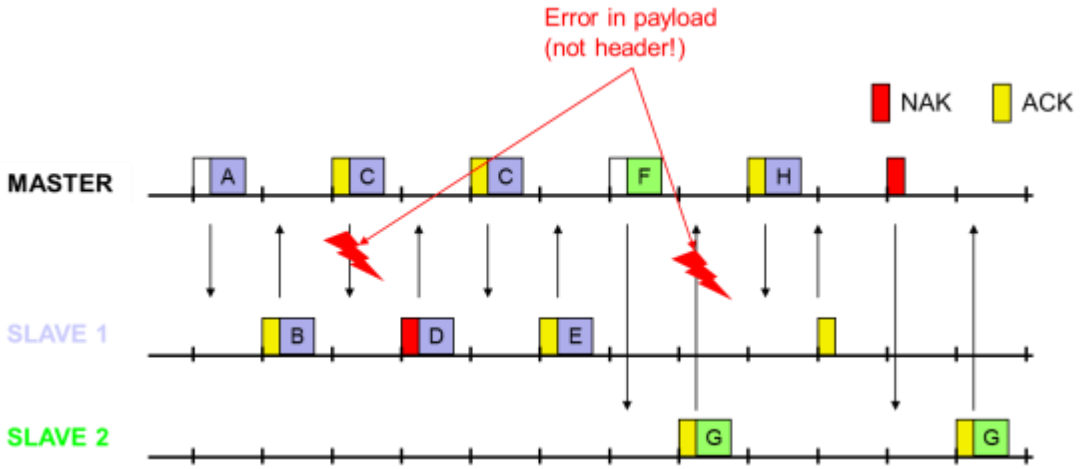

Figura 6.10: Exemplo de funcionamento do mecanismo de ARQ do Bluetooth [Schi04].

6.6 Versões do Bluetooth

A versão 1.2 do Bluetooth, compatível com a anterior, introduziu um mecanismo de Adaptive Frequency Hopping (AFH), que permite aumentar a robustez contra interferências ao evitar o uso dos canais mais congestionados na sequência de saltos. Outra novidade é um aprimoramento em relação às ligações SCO, denominado eSCO (*Extended Synchronous Connections*), que torna possível a retransmissão de pacotes corrompidos por erros, permitindo assim aumentar a qualidade das ligações de áudio e voz.

A versão 2.0, publicada em 2004, assegura retrocompatibilidade com a versão anterior. A principal diferença consiste na introdução do mecanismo EDR (*Enhanced Data Rate*) que permite aumentar a taxa de transmissão de dados no *payload* de 1 Mbit/s para até 3 Mbit/s.

A versão 3.0, adotada em 2009, permite atingir taxas de transmissão de dados até 24 Mbit/s ao substituir a ligação Bluetooth propriamente dita por uma

ligação IEEE 802.11 durante a transmissão de dados. Neste caso, a ligação Bluetooth é utilizada na fase anterior de negociação e estabelecimento da conexão.

A versão 4.0 do *standard* Bluetooth [Blue13], além de possuir os controladores BR/EDR e AMP, possui também o BLE *(Bluetooth Low Energy*) [Gome12]. O BLE é vocacionado para aplicações nas áreas dos cuidados de saúde, *fitness* e entretenimento doméstico e segurança. Neste sentido, o BLE foi criado com o propósito de transmitir pacotes de informação muito pequenos (baixo débito) de cada vez, com baixo custo e consumindo pouca energia, quando comparado com os dispositivos que suportam BR/EDR. A Figura 6.11 apresenta um exemplo de uma arquitetura possível na versão 4.0 do Bluetooth, combinando os diferentes controladores existentes. Além desta configuração é também possível definir apenas um controlador primário (BR/EDR ou BLE), contendo ou não um ou mais controladores secundários (AMP).

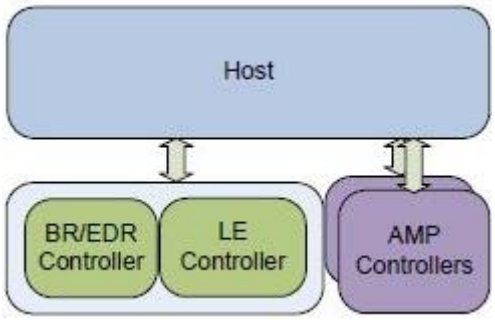

Figura 6.11. Arquitetura do Bluetooth 4.0 [Maio14].

Dispositivos que suportam BR/EDR e BLE são referidos como dispositivos *dual-mode* e encaixam na categoria Bluetooth Smart Ready*.* Tipicamente, num sistema Bluetooth 4.0, um smartphone ou um computador portátil são dois exemplos de dispositivos *dual-mode*. Já dispositivos que suportem unicamente BLE são referidos como dispositivos *single-mode*, encaixando na categoria Bluetooth Smart. Estes dispositivos são geralmente usados para aplicações que requerem baixo consumo de energia, são alimentados com recurso a baterias e apresentam tamanho reduzido. Exemplos deste tipo de dispositivos são sensores de monitorização ambiental ou de sinais vitais. A Figura 6.12 representa a interação entre os diferentes sistemas Bluetooth, onde se observa

que dispositivos Smart Ready são o elo central entre dispositivos que apenas suportam BLE (Bluetooth Smart) ou somente BR/EDR (Bluetooth).

Figura 6.12. Interação entre diferentes sistemas Bluetooth [Maio14].

Referências

[Haar00] J. C. Haartsen, “The Bluetooth Radio System”, IEEE Personal Communications, pp. 28-36, February 2000.

[Blue01] Bluetooth Special Interest Group (SIG), “Specification of the Bluetooth System - Core”, February 2001.

[Blue09] Bluetooth SIG, “Specification of Bluetooth System (Covered Core Package version: 3.0+HS)”, 2009.

[Blue13] Bluetooth SIG, “Specification of Bluetooth System (Covered Core Package version: 4.0)”, 2013.

[Joha99] P. Johansson, N. Johansson, U. Körner, J. Elg, and G. Svennarp, “Short range radio based ad-hoc networking: performance and properties”, IEEE International Conference on Communications ICC’99, Vancouver, Canada, pp. 1414-1420, 1999.

[Gome12] C.Gomez, J. Oller and J. Paradells, “Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology”, Sensors, vol. 12, 2012.

[Maio14] A. F. Maio, “Bluetooth Low Energy para Monitorização da Postura no Ciclismo”, Dissertação do Mestrado Integrado em Engenharia de Comunicações, Universidade do Minho, Dezembro de 2014.

[Schi04] J. Schiller, “Mobile Communications”, 2nd edition, Addison-Wesley, 2004.

7.IEEE 802.15.4

7.1 Introdução

As redes de área pessoal de baixo débito LR-WPAN (*Low Rate Wireless Personal Area Network*) são redes simples e de baixo custo que permitem a conectividade entre dispositivos com limitações de consumo energético e que não requerem débitos de transmissão elevados. Os principais objetivos neste tipo de redes são os de garantir fácil instalação, fiabilidade na entrega da informação no destinatário, baixo custo, baixa complexidade e elevada autonomia dos dispositivos (meses a anos, utilizando baterias, sem intervenção do utilizador). As áreas de aplicação deste tipo de tecnologia incluem as redes de sensores, brinquedos interativos, comandos remotos e automação residencial.

A norma IEEE 802.15.4 foi concebida tendo em conta essas características e aplicações. A primeira versão desta norma [IEEE03], que define a camada física (PHY) e a camada MAC da rede, foi publicada em 2003. O IEEE 802.15.4 serve de base a diversas redes e protocolos, abertos ou proprietários, que assentam sobre as suas camadas, como é o caso do ZigBee, 6LoWPAN, IEEE 802.15.5, WirelessHART e ISA100.11a.

A norma 802.15.4 define dois tipos de dispositivos: FFD (*Full Function Device*) e RFD (*Reduced Function Device*). Um FFD pode assumir qualquer uma das seguintes três funções na rede: o coordenador da PAN (*Personal Area Network*), um coordenador ou um dispositivo. Um RFD, por outro lado, não pode ser coordenador, só dispositivo. Um FFD pode comunicar com outros FFDs ou com RFDs, enquanto um RFD só pode comunicar com um FFD. Os RFDs são destinados a funções muito simples que não necessitem enviar grandes quantidades de dados, tais como um interruptor de luz ou um sensor de infravermelhos, e só podem estar associados a um FFD de cada vez. Como contrapartida, podem ser implementados utilizando menos recursos em termos de memória e capacidade de processamento.

O dispositivo FFD que dá início ao processo de formação de uma rede IEEE 802.15.4 é denominado coordenador da PAN. Este dispositivo torna-se o nó com endereço “0”. Outras tarefas do coordenador da PAN são:

- Escolha do canal de operação da rede;
- Especificação do identificador da PAN (PAN ID);
- Escolha do modelo de segurança da rede;
- Transmissão da trama *beacon*.

Na topologia em estrela (*star*) só há um único coordenador na rede: o coordenador da PAN. Todos os dispositivos da rede só podem comunicar diretamente com o coordenador da PAN, como mostra a Figura 7.1(a). Um dispositivo FFD pode formar a sua própria rede e tornar-se o coordenador da PAN, bastando para isso escolher um identificador da PAN que não esteja a ser usado por qualquer outra rede em seu redor. Qualquer dispositivo que se associe a esta rede, seja FFD ou RFD, comunica diretamente só com o coordenador da PAN. Este, por sua vez, pode reencaminhar os pacotes recebidos para qualquer dispositivo da rede.

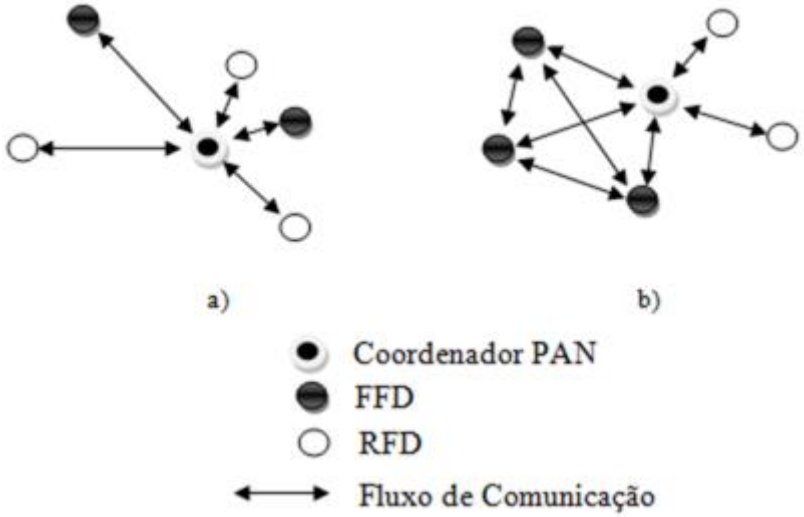

Figura 7.1: Topologias em estrela e *peer-to-peer* do IEEE 802.15.4 [Mace10].

Para que a rede tenha a autonomia desejada, o consumo dos dispositivos deve ser tido em conta no planeamento da rede. Numa rede com topologia em estrela, os dispositivos terminais são tipicamente alimentados por

baterias. Isso normalmente não é aconselhável para o coordenador da PAN, visto que, devido ao número elevado de tarefas a que o coordenador da PAN está sujeito, o seu consumo é maior do que o dos restantes dispositivos da rede.

Na topologia *peer-to-peer*, representada na Figura 7.1(b), também existe um coordenador da PAN. Contudo, esta difere da topologia em estrela na medida em que um dispositivo FFD pode comunicar com qualquer outro dispositivo FFD da rede, desde que este esteja ao seu alcance. Este tipo de topologia serve de base para a construção de redes mais complexas, como por exemplo redes em malha (*mesh*), que permitem aumentar o alcance através de múltiplos saltos (*multihop*) entre os dispositivos de origem e destino. Nestas redes podem existir outros coordenadores, para além do coordenador da PAN, que podem prestar serviços de sincronização e transferência de dados.

7.2 Camada física

A camada física é responsável pela transmissão e receção de dados, num dos canais de rádio disponíveis, usando uma técnica de modulação específica. Esta camada é também responsável pelas seguintes operações:

- **Ativação e desativação do transcetor (*transceiver*).** O rádio pode operar em três estados distintos: transmissão, receção e modo de poupança de energia (*sleep*). De acordo com a norma, o tempo que é necessário para o rádio comutar do estado de transmissão para o estado de receção e vice-versa (*turnaround time*) não deve ser superior a 12 períodos do símbolo (*symbol periods*).
- **Deteção de energia (ED - *Energy Detection*).** É uma estimativa da intensidade de sinal recebida dentro de um canal IEEE 802.15.4. Esta tarefa não faz nenhuma identificação do sinal ou descodificação no canal. A deteção de energia deve ser feita durante um tempo igual a 8 períodos do símbolo. Esta operação é tipicamente usada pela camada de rede, como parte do algoritmo de seleção de canal, ou pela função CCA (*Clear Channel Assessment*), na camada MAC.

- **Indicação da qualidade da ligação (LQI - *Link Quality Indication*).** A medição do LQI caracteriza a qualidade do sinal de um pacote recebido na ligação. Esta medição pode ser implementada usando o ED medido pelo recetor, uma estimativa da relação sinal/ruído, ou mesmo uma combinação entre estes valores. O resultado do LQI pode ser usado pelas camadas superiores.
- **Verificação de canal livre (CCA - *Clear Channel Assessment*).** Esta função é responsável por reportar o estado da atividade do meio: ocupado ou livre. O CCA pode funcionar com base em três modos de operação:
  - *Energy Detection mode*: neste caso, o CCA indica que o meio está ocupado perante uma deteção de energia superior ao ED *threshold*.
  - *Carrier Sense mode*: neste caso, o meio é dado como ocupado se o CCA detetar um sinal com as características de modulação e espalhamento espectral do IEEE 802.15.4, independentemente de esse sinal ser superior ou inferior ao ED *threshold*.
  - *Carrier Sense with Energy Detection*: combinação das técnicas descritas anteriormente. O CCA indica o meio como ocupado se, e somente se, detetar um sinal com as características de modulação e espalhamento espectral do IEEE 802.15.4 e com uma energia superior ao ED *threshold*.
- **Seleção do canal.** A norma IEEE 802.15.4 define 27 canais diferentes. A camada física deve ser capaz de sintonizar o transcetor no canal requerido por uma camada superior.

O IEEE 802.15.4 disponibiliza três bandas de frequência de operação distintas: 2.4 GHz, 868 MHz e 915 MHz. Na banda de 868 MHz existe somente um canal (canal 0), na banda de 915 MHz existem 10 canais (canais 1 a 10, não disponíveis na Europa) e, por fim, há 16 canais na banda de 2.4 GHz (canais 11 a 26), como mostra a Figura 7.2. Normalmente os dispositivos disponíveis no mercado para operação na banda de 2.4 GHz não operam nas outras bandas, e vice-versa. Todos esses canais operam com base na técnica de espalhamento espectral DSSS.

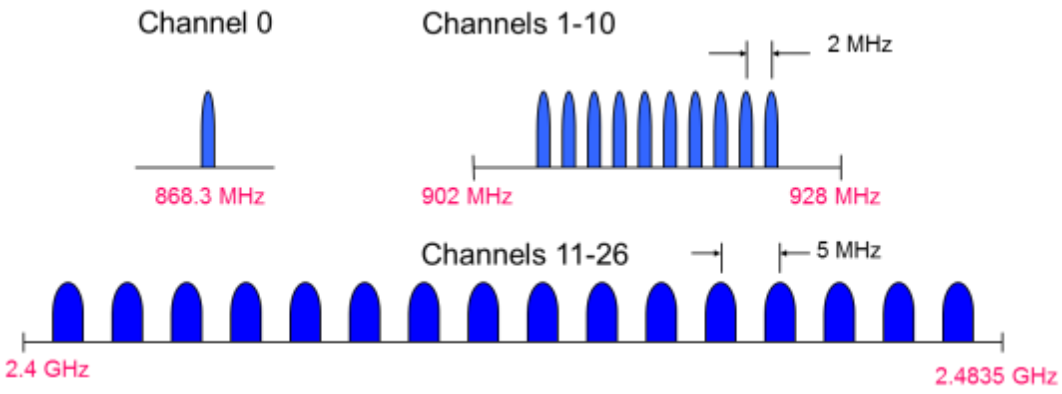

Figura 7.2: Canais de frequência do IEEE 802.15.4 [Schi04].

A frequência central para estes canais é definida da seguinte maneira:

$$F_c = 868.3\ \text{MHz}, \quad k = 0$$

$$F_c = 906 + 2(k-1)\text{MHz}, \qquad k = 1,2,\ldots,10$$

$$F_c = 2405 + 5(k-11)\text{MHz}, \qquad k = 11,12,\ldots,26$$

onde k é o número do canal.

No que diz respeito a taxas de transmissão, o IEEE 802.15.4 apresenta 20 kbps a 868 MHz, 40 kbps a 915 MHz e 250 kbps a 2.4 GHz. Devido a menores perdas de propagação, as frequências mais baixas são mais indicadas para transmissões a longa distância, proporcionando melhor sensibilidade e cobertura. Por outro lado, a taxa de transmissão mais alta a 2.4 GHz possibilita maior débito, menor latência e menor *duty cycle*. Um resumo das características associadas a cada banda de frequências é apresentado na Tabela 7.1.

Tabela 7.1: Características do IEEE 802.15.4 nas três bandas de operação [IEEE03].

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

O formato do pacote da camada física (PPDU) é apresentado na Figura 7.3. O SHR (*Synchronization Header*) permite a sincronização e delimitação do pacote, o PHR (PHY *Header*) contém a informação do tamanho do pacote, e o *payload* contém a trama da camada MAC.

Octets: 4	1	1		variable
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	PSDU
SHR		PHR		PHY payload

Figura 7.3: Formato do PDU da camada física [IEEE03].

7.3 Camada MAC

A camada MAC gere o acesso ao canal físico de rádio, sendo responsável pelas seguintes tarefas [IEEE06]:

- Gerar os *beacons*, caso o dispositivo seja um coordenador.
- Sincronização com os *beacons* da rede.
- Suporte à associação e a desassociação de dispositivos na PAN.
- Suporte de segurança no dispositivo.
- Implementação do mecanismo CSMA-CA para acesso ao canal.
- Gestão do mecanismo GTS (*Guaranteed Time Slot*).
- Garantir uma ligação fiável entre as camadas MAC de dois dispositivos.

A camada MAC do IEEE 802.15.4 suporta dois modos de operação:

- **Modo *beacon-enabled*.** Neste modo, *beacons* são gerados e enviados periodicamente pelo coordenador, a fim de sincronizar os restantes dispositivos ligados à rede e fornecer informação relacionada à PAN. O tempo é estruturado em supertramas, e pode haver períodos inativos para poupança de energia. Durante a supertrama, que inicia com a transmissão de uma trama *beacon*, o mecanismo *slotted* CSMA-CA é utilizado para troca de informação entre os dispositivos. Opcionalmente, pode ser utilizado também o mecanismo GTS.
- **Modo *non-beacon-enabled*.** Neste modo não existe uma estrutura em supertrama. Os dispositivos enviam pacotes utilizando o mecanismo *unslotted* CSMA-CA.

7.3.1 Modo *non-beacon-enabled*

Neste modo de operação não é feita a transmissão periódica de *beacons* e não existe a estrutura em supertrama. O controlo de acesso ao meio é efetuado com base no mecanismo *unslotted* CSMA-CA. Todos os pacotes devem ser transmitidos utilizando esse mecanismo, com exceção das tramas de reconhecimento positivo (ACK).

O algoritmo *unslotted* CSMA-CA do IEEE 802.15.4 está representado na Figura 7.4. Antes de obter o acesso ao meio, o dispositivo tem que aguardar um tempo aleatório, denominado intervalo de *backoff*, que está limitado entre 0 e 2^{BE}-1 períodos unitários de backoff (*unit backoff period*), onde *BE* (*backoff exponent*) inicialmente assume o valor *macMinBE*, e o período unitário de *backoff* tem a duração de *aUnitBackoffPeriod* símbolos. Após esse atraso aleatório, se a função CCA indicar que o canal está livre, o algoritmo termina com sucesso[21] e o dispositivo pode começar a sua transmissão (sendo para isso necessário antes comutar o rádio do estado de receção para o estado de transmissão). Por outro lado, se o canal estiver ocupado, o dispositivo adia a

[21] Sucesso neste caso significa que o dispositivo obteve permissão de transmissão, não significa necessariamente que a transmissão irá ser bem-sucedida.

sua transmissão e incrementa o número de tentativas de transmissão (*NB*) para o pacote que está a tentar transmitir. Caso *NB* ainda não tenha atingido o seu valor máximo (*macMaxCSMAbackoffs*), a variável *BE* também é incrementada (até ao limite *aMaxBE*), e um novo tempo aleatório de *backoff* é calculado. Se, por outro lado, o número máximo de tentativas for alcançado, o algoritmo declara uma falha no acesso ao meio.

Os valores dos parâmetros do *unslotted* CSMA-CA estão definidos na Tabela 7.2. Note-se que o parâmetro *aUnitBackoffPeriod*, que determina a duração do período unitário de *backoff*, não é fornecido em segundos, mas sim em *symbol periods* (SP). O período do símbolo é o inverso do *symbol rate*, cujo valor depende da banda de frequência utilizada, tendo os respetivos valores sido apresentados na Tabela 7.1. Sendo assim, no caso da banda de 2.4 GHz, por exemplo, o *symbol rate* é 62.5 ksymbols/s, pelo que SP = 16 µs e, portanto, *aUnitBackoffPeriod* corresponde a 320 µs.

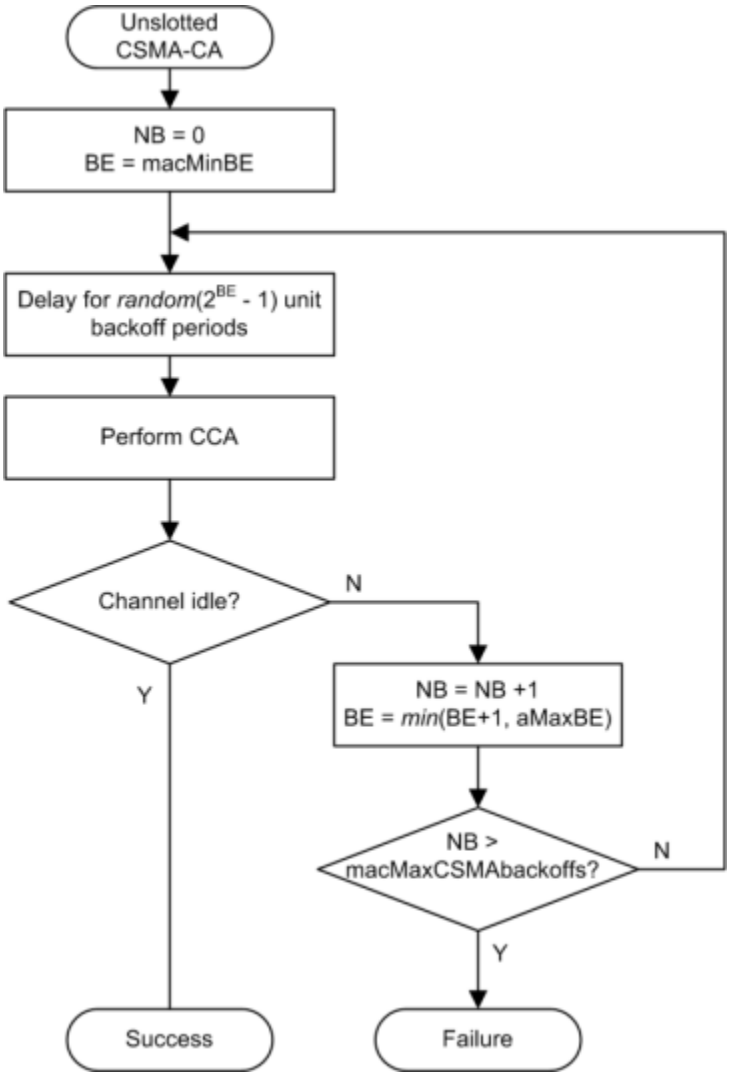

Figura 7.4: Algoritmo *unslotted* CSMA-CA do IEEE 802.15.4 [Lope12].

Tabela 7.2: Valores dos parâmetros do algoritmo *unslotted* CSMA-CA [IEEE06].

Parâmetro	Descrição	Valor
macMinBE	Valor mínimo do expoente de *backoff*	[0-3], por omissão = 3
aUnitBackoffPeriod	Duração do período unitário de *backoff* em número de *symbol period*s (SP)	20 SP
aMaxBE	Valor máximo do expoente de *backoff*	5
macMaxCSMAbackoffs	Número máximo de tentativas de *backoff*	[0-5], por omissão = 4

7.3.2 Modo *beacon-enabled*

No modo *beacon-enabled* do IEEE 802.15.4, o tempo é dividido em supertramas com a estrutura apresentada na Figura 7.5. Cada supertrama inicia com o *beacon* transmitido pelo coordenador da PAN. Além da parte ativa, em que ocorre a transmissão de dados, a supertrama pode conter uma parte inativa, na qual o coordenador pode entrar em modo de poupança de energia. A função dos *beacons* é a de sincronizar os dispositivos com o coordenador, identificar a PAN e descrever a estrutura da supertrama.

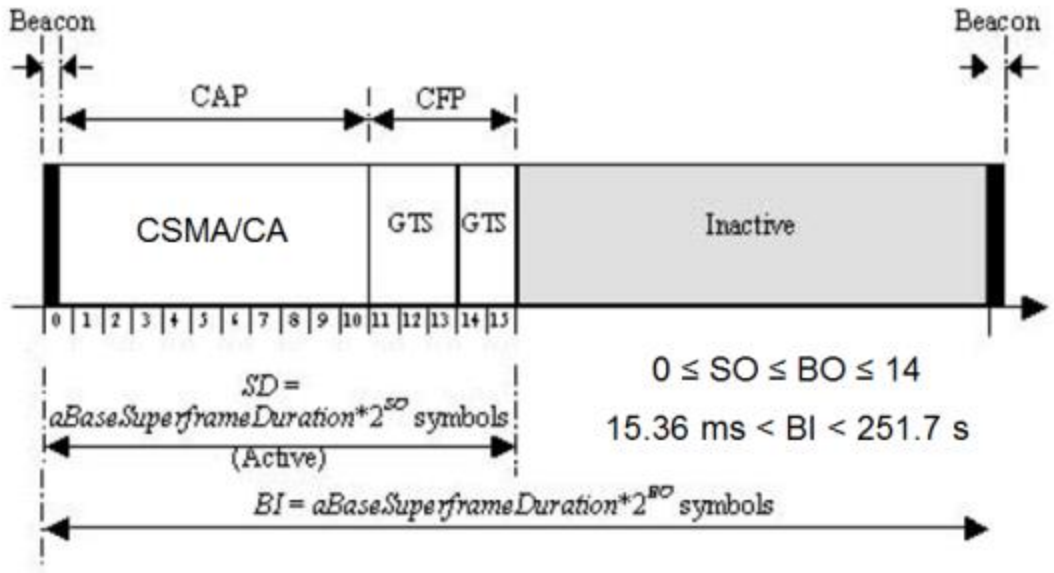

Figura 7.5: Estrutura da supertrama do modo *beacon-enabled* [IEEE03].

A seguir ao *beacon*, a parte ativa da supertrama (que é composta por 16 *slots* de igual duração) é dividida em um período de contenção (CAP - *Contention Access Period*), em que os dispositivos utilizam o mecanismo *slotted* CSMA-CA[22] para aceder ao meio, e um período livre de contenção (CFP - *Contention Free Period*), opcional, em que é utilizado o mecanismo GTS.

[22] O algoritmo *slotted* CSMA-CA [IEEE06] é semelhante ao *unslotted* CSMA-CA, mas contém alguns passos extras.

A duração da parte ativa da supertrama (SD - *Superframe Duration*) é função dos parâmetros *aBaseSuperframeDuration* e SO (*Superframe Order*), como mostra a figura. O intervalo entre os *beacons* (BI - *Beacon Interval*), que inclui a parte ativa e a parte inativa, é função dos parâmetros *aBaseSuperframeDuration* e BO (*Beacon Order*). Os valores de SO e BO seguem a relação $0 \leq SO \leq BO \leq 14$ e o valor de *aBaseSuperframeDuration* corresponde a 960 *symbol periods*. Sendo assim, na banda de 2.4 GHz, a duração da supertrama pode ser configurada entre um mínimo de 15.36 ms e um máximo de 251.7 s, em múltiplos de 2.

7.3.3 Modelos de transferência de dados

A norma IEEE 802.15.4 define três modelos de transferência de dados. O primeiro e o segundo modelo indicam como se transfere informação de um coordenador para um dispositivo e de um dispositivo para um coordenador, respetivamente. O terceiro modelo é usado para transferência de dados *peer-to-peer*. Nas redes baseadas em topologia em estrela são usados os dois primeiros modelos, enquanto nas redes *peer-to-peer* pode ser usado qualquer um dos modelos.

Os procedimentos utilizados variam conforme esteja a ser utilizado o modo *beacon-enabled* ou o modo *non-beacon-enabled*. A Figura 7.6 apresenta os procedimentos no caso da comunicação de um dispositivo para um coordenador. Quando um dispositivo pretender transmitir numa PAN em modo *beacon-enabled*, ouve o beacon, sincroniza-se com a supertrama e, no momento apropriado, transmite a informação utilizando o mecanismo *slotted* CSMA-CA. A seguir, o coordenador transmite o *acknowledgment*, caso seja pedido. Já quando um dispositivo quer comunicar numa PAN em modo *non-beacon-enabled*, simplesmente transmite o pacote de dados utilizando o mecanismo *unslotted* CSMA-CA. Da mesma forma, o coordenador responde com o *acknowledgment*, caso seja pedido. Os procedimentos de transferência de dados de um dispositivo para um coordenador assumem que o coordenador está sempre ativo e, desta forma, apto a receber pacotes dos dispositivos

durante todo o período ativo da supertrama, no caso do modo *beacon-enabled*, e durante todo o tempo, no caso do modo non-*beacon-enabled*.

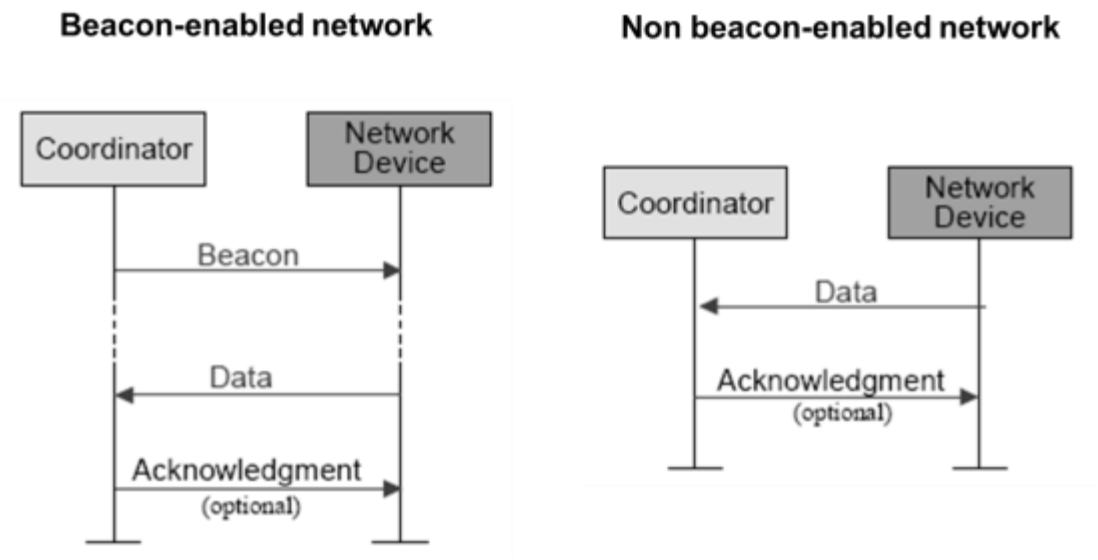

Figura 7.6: Comunicação de um dispositivo para o coordenador [IEEE06].

Na transferência de dados de um coordenador para um dispositivo, assume-se que o dispositivo pode estar em modo inativo (*sleep*) para poupar energia, não estando assim apto a receber pacotes. Desta forma, o coordenador armazena os pacotes pendentes e espera que seja o dispositivo a requisitá-los.

No modo *beacon-enabled*, o coordenador utiliza o *beacon* para indicar que existem dados pendentes para o dispositivo. O dispositivo acorda periodicamente e ouve o *beacon*. Caso haja dados pendentes, o dispositivo faz um pedido ao coordenador, utilizando um pacote *Data Request*, para que este lhe envie os dados Este pedido é feito no CAP, utilizando o *slotted* CSMA-CA. Tanto o coordenador como o dispositivo podem efetuar os respetivos *acknowledgments* dos pacotes trocados.

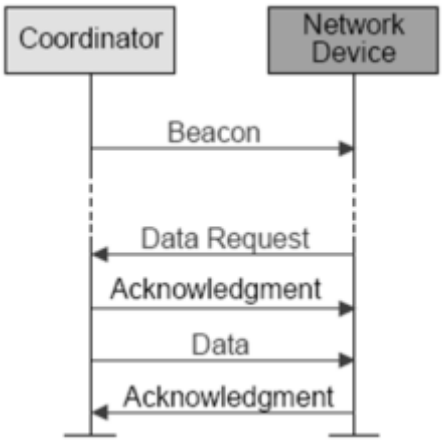

Figura 7.7: Comunicação de um coordenador para um dispositivo no modo *beacon-enabled* [IEEE06].

A transferência de dados de um coordenador para um dispositivo no modo *non-beacon-enabled* é semelhante à do modo *beacon-enabled*. A diferença é que o dispositivo não dispõe do *beacon* para saber se existem dados pendentes. Desta forma, o dispositivo utiliza um mecanismo de *polling* ao coordenador, pelo envio de pacotes *Data Request* de forma periódica. Caso existam dados pendentes, o coordenador responde ao *Data Request* com um *acknowledgment*, e envia de seguida os dados. Por fim, caso seja pedido, o dispositivo envia um *acknowledgment* ao coordenador. Por outro lado, quando não há dados pendentes, o coordenador envia um *acknowledgment* com esta informação ou então envia um pacote de dados com o *payload* vazio. Tanto o pacote *Data Request* quando o pacote de dados são transmitidos utilizando o protocolo *unslotted* CSMA-CA.

No caso da topologia *peer-to-peer*, cada dispositivo pode comunicar com todos os outros ao seu alcance. Para que a comunicação seja feita de forma eficaz, a norma define que os dispositivos que pretendem comunicar estejam aptos a receber durante todo o tempo ou sejam capazes de se sincronizar entre si. No primeiro caso, o dispositivo pode simplesmente transmitir os seus dados usando o *unslotted* CSMA-CA. No segundo caso, outras medidas devem ser tomadas de forma a conseguir a sincronização. No entanto, tais medidas são consideradas fora do âmbito da norma.

7.3.4 O mecanismo GTS

Conforme foi dito anteriormente, a parte ativa da supertrama do modo *beacon-enabled* é composta por 16 *slots* de igual duração. O mecanismo GTS (*Guaranteed Time Slot*) permite reservar na supertrama um conjunto de *slots* contíguos para transmissões associadas a um dispositivo, no sentido ascendente ou descendente, mediante um pedido efetuado pelo dispositivo.

A Figura 7.5 mostra um exemplo no qual estão feitas duas alocações GTS, uma de três *slots* e outra de dois *slots*. Uma rede IEEE 802.15.4 permite que até sete alocações GTS, no máximo, estejam ativas ao mesmo tempo. O GTS deve ser alocado antes de ser utilizado e pode ser desalocado a qualquer instante por iniciativa do coordenador da PAN ou do dispositivo.

A Figura 7.8 apresenta o formato do pedido de GTS (GTS *Request*), contendo as características do GTS, que é transmitido pelo dispositivo para o coordenador numa trama MAC. O campo *GTS Length* contém o número de *slots* que estão a ser pedidos. O campo *GTS Direction* especifica o sentido de transmissão dos dados neste GTS: o valor ‘1’ indica que o GTS é alocado para o dispositivo receber dados, enquanto o valor ‘0’ indica que o GTS é alocado com o propósito de transmissão de dados. O campo *Characteristic Type* indica que se trata de um pedido de alocação se o valor for ‘1’, e um pedido de desalocação se o valor for ‘0’. O pedido de GTS é feito durante o CAP, utilizando o mecanismo *slotted* CSMA-CA.

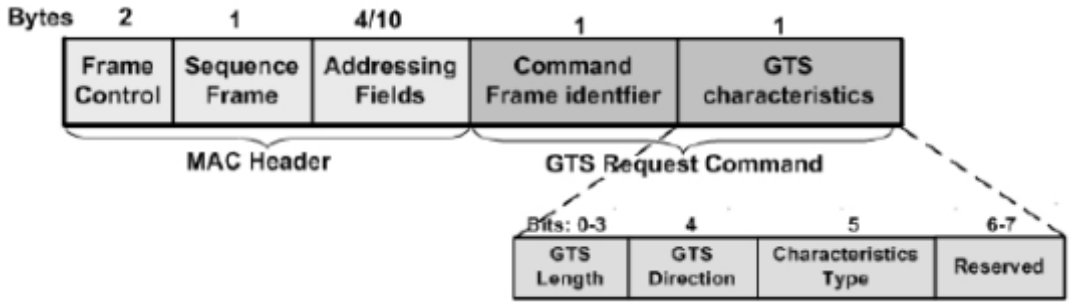

Figura 7.8: Formato da trama GTS Request [Koub05].

O resultado do pedido de GTS é comunicado ao dispositivo pelo coordenador utilizando o respetivo descritor GTS (GTS *Descriptor*), que é

inserido na trama beacon. O descritor GTS permanece na trama beacon durante um número *aGTSDescPersistenceTime* de supertramas consecutivas, sendo que a norma IEEE 802.15.4 define que o valor de *aGTSDescPersistenceTime* é 4. No decorrer da utilização GTS, caso um dispositivo não consiga receber corretamente o *beacon* no início de uma supertrama, não deve utilizar os GTS alocados naquela supertrama.

O formato do descritor GTS é apresentado na Figura 7.9, sendo composto pelo endereço de 16 bits do dispositivo, o *slot* inicial do GTS (GTS *Start Slot*), e o número de slots alocados (GTS *Length*). Um descritor GTS com GTS *Start Slot* igual a zero serve para indicar que o GTS foi desalocado.

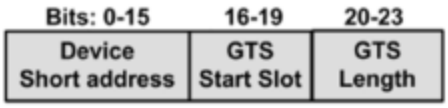

Figura 7.9: Formato do GTS *Descriptor* [Koub05].

A desalocação de um GTS pode fazer com que a supertrama fique fragmentada. Quando isso ocorre, o coordenador da PAN deve executar um processo de realocação de GTSs para eliminar os *gaps*, de modo a maximizar o comprimento do CAP. O processo de realocação consiste em mover para a direita os GTSs situados à esquerda do GTS desalocado, o que é feito pela inclusão dos descritores GTS correspondentes nas tramas *beacon*.

7.3.5 Tipos e formatos de tramas

A norma IEEE 802.15.4 define quatro tipos de tramas:

- **Trama *beacon***, utilizada por um coordenador para transmissão de beacons.
- **Trama de dados**, utilizada por todos tipos de dispositivos para as transferências de dados.
- **Trama de *acknowledgment***, utilizada para confirmar a receção bem-sucedida de uma trama.
- **Trama de comando MAC**, usada para sinalização de nível MAC.

A Figura 7.10 apresenta o formato da trama de dados. O cabeçalho da trama MAC (MHR - MAC *Header*) inclui os seguintes campos:

- *Frame Control*: contém informação sobre o tipo de trama e outras *flags* de controlo (*Security Enabled*, *Frame Pending*, *Acknowledgment Request*, etc.)
- *Sequence Number*: número de sequência de 8 bits.
- *Destination PAN Identifier*: campo de 16 bits que contém o identificador da PAN do destinatário da trama.
- *Destination Address*: endereço do destinatário da trama. Uma trama pode conter o endereço longo (64 bits) ou o endereço curto (16 bits), dependendo do valor do respetivo subcampo no campo *Frame Control*.
- *Source PAN Identifier*: campo de 16 bits que contém o identificador da PAN do dispositivo de origem da trama.
- *Source Address*: endereço de origem da trama. Uma trama pode conter o endereço longo (64 bits) ou o endereço curto (16 bits), dependendo do valor do respetivo subcampo no campo *Frame Control*.

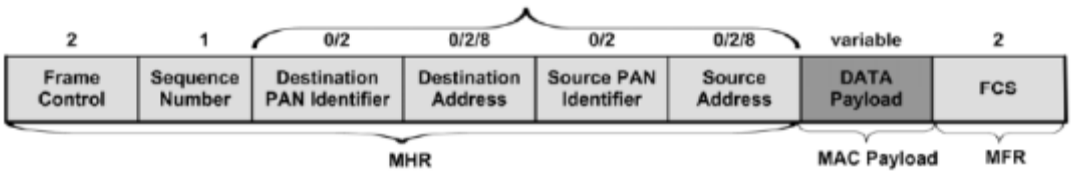

Figura 7.10: Formato da trama de dados [Koub05].

A cauda da trama MAC (MFR - MAC *Footer*) contém o campo FCS (*Frame Check Sequence*), que transporta um código CRC (*Cyclic Redundancy Code*) de 16 bits usado para a deteção de erros na trama.

O formato da trama beacon é apresentado na Figura 7.11. O *payload* desta trama contém a seguinte informação:

- *Superframe Specification*: Especifica os valores de diversos parâmetros relacionados com a supertrama: *Beacon Order, Superframe Order, Final* CAP *Slot, Battery Life Extension, PAN Coordinator* e *Association Permit*.

- *GTS field*: É um campo de tamanho variável que contém informação a respeito dos GTSs que estão a ser alocados.
- *Pending Address*: Campo de tamanho variável que contém informação sobre os dispositivos para os quais atualmente há dados pendentes armazenados no coordenador.
- *Beacon Payload*: Sequência opcional de bytes especificada para transmissão no *beacon* pela camada superior.

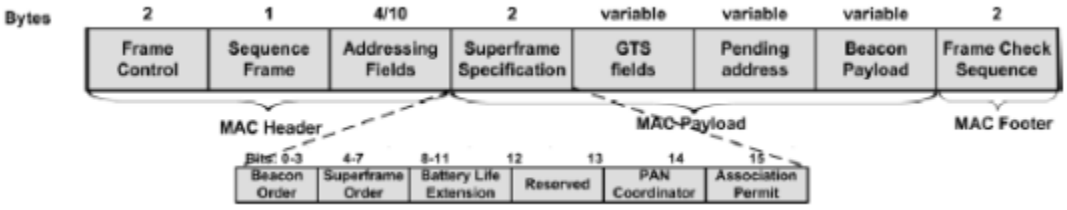

Figura 7.11: Formato da trama *beacon* [Koub05].

Referências

[IEEE03] IEEE Std 802.15.4-2003, “Part 15.4: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks”, October 2003.

[IEEE06] IEEE Std 802.15.4-2006, “Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”, September 2006.

[Koub05] A. Koubaa, M. Alves and E. Tovar, “IEEE 802.15.4 for Wireless Sensor Networks: A Technical Overview”, IPP-HURRAY Technical Report, HURRAY-TR-050702, July 2005.

[Lope12] H. F. López, J. A. Afonso, J. H. Correia, R. Simões, "Towards the design of efficient nonbeacon-enabled ZigBee networks", Computer Networks, Vol. 56, Issue 11, July 2012, pp. 2714–2725.

[Mace10] P. Macedo, “Desenvolvimento de Modelos de Simulação de Redes de Sensores sem Fios”, Dissertação de Mestrado, Mestrado

Integrado em Engenharia Eletrónica Industrial e Computadores, Universidade do Minho, Novembro de 2010.

8.ZigBee

8.1 Introdução

Hoje em dia as redes de comunicação sem fios estão por toda a parte, cobrindo as necessidades de variados tipos de aplicações. As redes ZigBee [ZigB04], ao contrário do Wi-Fi, em que um dos objetivos principais é disponibilizar elevadas taxas de transmissão de dados, são vocacionadas para aplicações nas quais o baixo consumo de energia, baixo custo e pequeno tamanho dos nós são normalmente prioritários, sendo assim adotadas tecnologias mais adequadas para satisfazer esses requisitos. Neste sentido, os dispositivos da rede utilizar costumam utilizar componentes (microcontroladores, transcetores, etc.) de baixo consumo, baixa complexidade e capacidade de processamento limitada, de modo a satisfazer os requisitos de baixo custo e elevada autonomia dos dispositivos alimentados por baterias.

Enquanto a maior parte dos tipos de redes de comunicação foram concebidas com o propósito de satisfazer as necessidades associadas à prestação de variados serviços de comunicação de dados entre utilizadores, o ZigBee foi concebido tendo em vista aplicações de monitorização e controlo nas quais grande parte dos dados transmitidos pela rede não são gerados por utilizadores, mas sim recolhidos do ambiente através de sensores. Essas redes também podem ser utilizadas para alterar parâmetros do ambiente, por intermédio de atuadores.

De modo a satisfazer os requisitos de baixo custo financeiro e energético, o ZigBee é uma tecnologia que utiliza potências de transmissão e taxas de transmissão de dados substancialmente menores do que redes de área local. Essas potências de transmissão mais reduzidas implicam que o alcance é menor; no entanto, o ZigBee suporta comunicações *multihop*, o que permite alargar a área abrangida pela rede. O ZigBee não necessita de altas taxas de transmissão de dados porque as aplicações típicas desse tipo de redes não

geram muito tráfego. Um exemplo extremo é um sistema simples formado por uma lâmpada e um interruptor que a controla, no qual podemos constatar que a quantidade de dados transportados pela rede será muito pequena, uma vez que o interruptor só necessita de gerar mensagens de controlo pequenas e de forma esporádica quando for ativado por um utilizador.

8.2 Pilha Protocolar

A estrutura da pilha protocolar definida na norma ZigBee é apresentada na Figura 8.1.

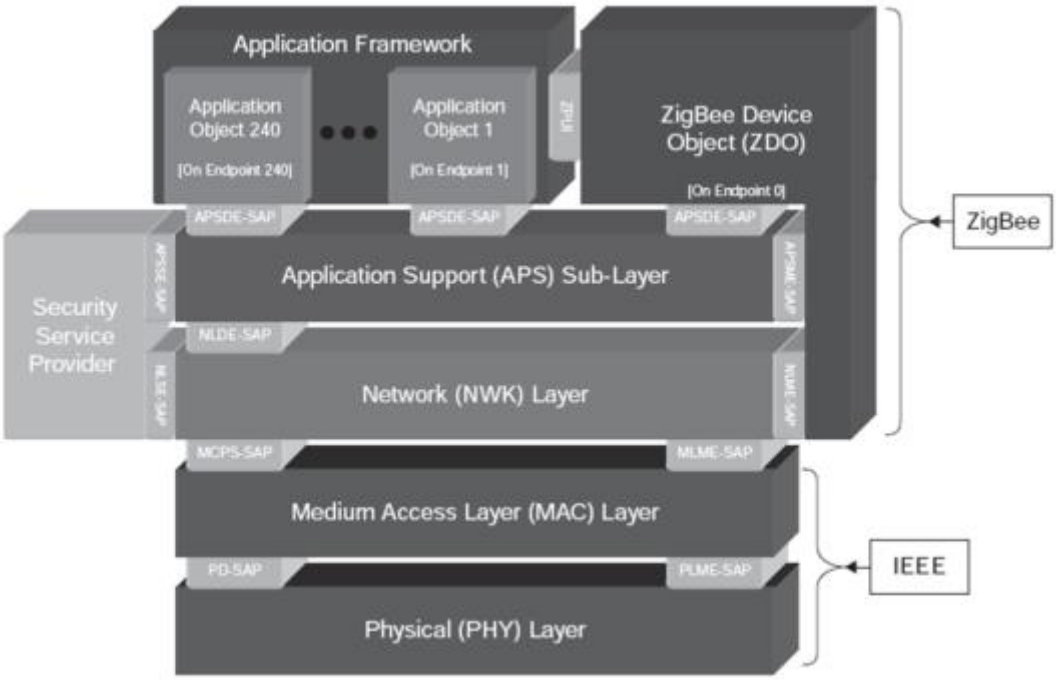

Figura 8.1: Pilha protocolar ZigBee [Gisl08].

Não se encaixando exatamente no modelo OSI de 7 camadas, o ZigBee contém alguns elementos correspondentes: a camada física (PHY), de ligação de dados (MAC) e a camada de rede (NWK). As funcionalidades das restantes 4 camadas (transporte, sessão, apresentação e aplicação) estão incluídas nas camadas APS (*Application Support Sublayer*) e ZDO (ZigBee *Device Object*) do modelo protocolar adotado pelo ZigBee.

Entre as camadas existem interfaces denominadas SAPs (*Service Access Point*). Cada interface está associada à respetiva API (*Application Programming Interface*), podendo-se assim abstrair o funcionamento de cada camada para as camadas superiores.

As duas camadas inferiores da pilha protocolar ZigBee, PHY e MAC, são definidas pela norma IEEE 802.15.4, versão 2003 [IEEE03]. A camada de rede (NWK) é responsável pelo encaminhamento, endereçamento de rede, *broadcasting*, e por garantir que os pacotes enviados chegam ao destino. Esta camada contém também um conjunto de comandos que permitem aos dispositivos efetuarem a associação (*joining*) ou reassociação (*rejoining*) à rede de maneira segura.

A camada APS é responsável pela gestão das aplicações que estão a correr sobre a mesma. Funciona como um filtro que tem a capacidade de distinguir *endpoints* e *clusters*, e de verificar se uma aplicação pertence a um determinado o perfil ou grupo. Assim, esta camada é capaz de identificar e entregar a informação à aplicação correta no destino, visto que podem existir várias aplicações a correr por cima desta camada. A APS filtra também pacotes duplicados e mantém uma tabela de *binding* que indica quais os outros nós na rede com que o nó está a comunicar.

O ZDO, que inclui o ZDP (ZigBee *Device Profile*), é responsável pela gestão do nó na rede. Para além disto, providencia também serviços que permitem descobrir outros nós e serviços na rede. A *Application Framework* (AF) é o local onde correm as aplicações.

8.3 PANs

Uma rede ZigBee formada é denominada *Personal Area Network* (PAN). O processo de formação de uma PAN é iniciado pelo coordenador ZigBee (ZC - ZigBee *Coordinator*). Os outros nós que se associam à rede podem ser de dois tipos: encaminhadores ZigBee (ZR - ZigBee *Router*) ou terminais ZigBee (ZED - ZigBee *End Device*).

O ZigBee usa o mesmo conjunto de canais especificado pela norma IEEE 802.15.4. Os canais 0 a 10 estão definidos para a banda sub-1GHz, enquanto na banda ISM de 2.4 GHz estes canais estão numerados de 11 a 26. Na banda de 2.4 GHz, estes canais estão espaçados de 5 MHz e disponibilizam uma taxa de transmissão de 250 kbps.

No processo de formação de uma rede ZigBee, o coordenador decide qual canal vai utilizar[23] com base na execução de dois procedimentos:

- Determinação se o canal está livre através da deteção de energia.
- Transmissão de um pacote *beacon request* em modo *broadcast* e verificação se há respostas de outros coordenadores, o que permite determinar se o canal está a ser ocupado por outras PANs.

Com base nesses procedimentos, o coordenador ZigBee seleciona o canal menos utilizado.

Para se associar a uma rede existente, um nó encaminhador ou terminal transmite primeiro um *beacon request*. Se existir alguma rede formada no canal, o nó irá receber um *beacon response* da parte do coordenador.

8.3.1 PAN IDs

Os PAN IDs são identificadores de 16 bits utilizados para diferenciar os pacotes pertencentes a redes ZigBee diferentes que possam operar na mesma área e no mesmo canal. O PAN ID é definido no momento em que a rede é criada, e permite a coexistência de múltiplas redes no mesmo canal. Naturalmente, neste caso, as redes têm que partilhar a largura de banda disponível no canal.

Os PAN IDs para uso privado são atribuídos de forma aleatória ou configurados manualmente pelo utilizador. Neste caso, estão disponíveis cerca de 16000 PAN IDs diferentes, pelo que o ZigBee assume que não existirão

[23] Com base na consulta de uma lista de canais selecionáveis, configurada pelo utilizador, que pode não incluir todos os canais suportados pelo dispositivo.

conflitos na atribuição dos identificadores. Isto deve-se ao facto de que, como estas redes são de curto alcance e geralmente não existe um número elevado de redes concentradas num mesmo local, a probabilidade de haver conflito é pequena. Duas redes com PAN IDs iguais podem coexistir sem problemas se estiverem em canais diferentes. Em perfis públicos, os identificadores estão normalizados, sendo atribuídos segundo o tipo de perfil utilizado.

8.3.2 Extended PAN IDs

Os Extended PAN IDs são identificadores únicos de 64 bits de uma PAN. O ZigBee utiliza o identificador de 16 bits da PAN para todas as comunicações exceto quando um nó se associa à rede. Neste caso, quando o nó transmite um *beacon request*, e na resposta é devolvido o Extended PAN ID, para dar garantias que o nó escolhe a rede correta.

8.4 Tipos de nós ZigBee

Noma rede ZigBee pode haver três tipos de nós: coordenador (ZC - ZigBee *Coordinator*), encaminhador (ZR - ZigBee *Router*) ou terminal (ZED - ZigBee *End Device*). Os ZC e ZR têm que ser necessariamente dispositivos FFD, conforme definido na norma IEEE 802.15.4, enquanto os ZED podem ser FFDs ou RFDs.

Os coordenadores ZigBee têm como principal tarefa a formação da rede. À parte disto, os ZCs tem funcionalidades semelhantes aos ZRs. É importante frisar que numa rede ZigBee só existe um único coordenador.

A principal função dos encaminhadores é permitir que o ZigBee possa funcionar em topologias *multihop*. Desta maneira, pode-se estender o alcance da rede. Este tipo de nó permite também que outros nós se associem à rede.

Os ZEDs são nós que, como o próprio nome indica, se encontram nos extremos da rede. Desta forma, por eles não pode passar informação destinada a outros nós na rede. São vocacionados para operar com alimentação de baterias, sendo portanto aqueles em que a economia de

energia é um fator crucial para maximizar a autonomia de funcionamento. Neste sentido, estes dispositivos são concebidos com a capacidade de poderem “dormir”, ou seja, entrar em modo inativo de baixo consumo de energia, e só acordarem periodicamente ou na ocorrência de um evento relevante, para aí sim agirem em conformidade.

A princípio, uma aplicação pode residir em qualquer um destes tipos de nós. Por exemplo, qualquer um deles pode servir para controlar uma lâmpada, efetuar a leitura um sensor de temperatura, etc. No entanto, dependendo das tarefas a desempenhar a nível da aplicação em cada caso, um tipo de nó pode ser mais recomendado do que outros.

8.5 Endereçamento

O endereçamento é a forma de identificação utilizada para que seja possível enviar informação de um ponto da rede para outro. No ZigBee, o endereçamento é feito a diferentes níveis, tendo em conta os parâmetros mostrados na Tabela 8.1.

Tabela 8.1: Parâmetros de endereçamento do ZigBee [Gisl04].

Name	Range	Description
Channel	11–26	A physical portion of the RF spectrum
PAN ID	0x0000–0x3fff	The address of a network within a channel
NwkAddr	0x0000–0xfff7	The address of a node within a network
Endpoint	1–240	The address of an application within a node
Cluster	0x0000–0xffff	The object within the application
Command	0x00–0xff	An action to take within the cluster
Attribute	0x0000–0xffff	A data item within the cluster

8.5.1 Endereço de Rede

O endereço de rede é um identificador de 16 bits que serve para identificar um nó em particular. O coordenador tem sempre o endereço de rede 0x0000. Para os restantes nós, o modo de atribuição de endereços depende

da versão da *stack* ZigBee utilizada. Quando um nó quer comunicar com outro, envia simplesmente os dados para o endereço correspondente.

8.5.2 Endereço MAC

O endereço MAC no ZigBee, também chamado de endereço IEEE ou endereço longo, é um identificador de 64 bits que é único para cada dispositivo IEEE 802.15.4 produzido, atribuído de fábrica. Os primeiros 24 bits correspondem ao identificador do fabricante (OUI - *Organizational Unique Identifier*) e os restantes 40 bits são geridos pelo fabricante (OEM - *Original Equipment Manufacturer*) para identificar os dispositivos que produz. Este endereço não tem qualquer relação com o endereço de rede. Quando um nó deixa a rede e volta a se associar, o endereço de rede pode mudar, mas o endereço MAC mantém-se sempre o mesmo.

O endereço MAC não está contido nos transcetores ZigBee. Em vez disso, é o fabricante do módulo (OEM) que é responsável por introduzir esse endereço na memória *flash* do microcontrolador do módulo. O OUI é requisitado ao IEEE, pelo pagamento de uma taxa (da ordem de US$1600 em 2004 [Gisl04]).

Alguns dispositivos ZigBee são comercializados sem um endereço MAC único atribuído, apresentando o endereço 0x0000000000000000. Neste caso, o procedimento consiste em gerar um endereço MAC aleatório para a operação do dispositivo numa rede. Estes dispositivos são destinados a desenvolvimento laboratorial e não são adequados para utilização posterior na implementação de soluções comerciais.

O endereço MAC é utilizado em troca de pacotes efetuadas antes da atribuição do endereço curto de 16 bits, que é dinâmico, ao nó. O endereço MAC também é utilizado em outras situações em que o uso de um endereço fixo único é apropriado.

8.5.3 Grupos

Um grupo representa um conjunto de dispositivos que são endereçáveis utilizando um único identificador. Desta forma, uma única mensagem pode ser enviada aos múltiplos dispositivos que formam um grupo. A funcionalidade de grupos é opcional na norma ZigBee, mas é obrigatória em alguns perfis, como é o caso do *Home Automation Profile*.

O conceito de grupo permite que um conjunto de dispositivos efetue uma ação em conjunto. Por exemplo, um sistema de *home theater* baseado em ZigBee pode reduzir a luminosidade, ligar o leitor de DVD, a televisão e as colunas, e baixar as persianas com um único comando.

8.5.4 Difusão

Difusão (*broadcast*) é o mecanismo utilizado para envio de informação a todos os nós da rede em simultâneo. Os endereços de difusão disponíveis no ZigBee são os seguintes:

- 0xffff – para todos os nós da rede;
- 0xfffd – para todos os nós que não estiverem em modo *sleep*;
- 0xfffc – para o coordenador e encaminhadores da rede.

Este modo de endereçamento é útil, por exemplo, em processos de descoberta de serviços na rede por parte das aplicações, e para os encaminhadores poderem descobrir rotas.

8.5.5 Endereçamento interno ao nó

Os mecanismos de endereçamento descritos anteriormente visam endereçar nós na rede. No entanto, devido ao facto de em cada nó poderem existir varias aplicações a funcionar em simultâneo, é necessário haver uma maneira de endereçar estas aplicações, de modo a ser possível encaminhar informação para a aplicação correta. O endereçamento interno ao nó tem em conta os componentes indicados abaixo. Esses endereços são transportados no cabeçalho do pacote da camada indicada entre parêntesis.

- PAN ID (Camada MAC);
- Endereço de rede (Camada de rede);
- *Endpoint* (Camada APS);
- *Profile* ID (Camada APS);
- *Cluster* ID (Camada APS);
- Comando e/ou atributos (ZCL).

Os *endpoints*, que são identificados com um número entre os valores 1 e 240, endereçam as aplicações a funcionar no nó, pelo que se pode concluir que um nó ZigBee pode executar múltiplas aplicações em simultâneo. Para além desses, existem alguns tipos de endereços especiais. O endereço 0 identifica uma aplicação especial em particular no nó, o ZDO (ZigBee *Device Object*). O endereço 255, por sua vez, corresponde ao endereço de difusão, ou seja, qualquer informação direcionada a este *endpoint* é entregue a todas as aplicações no nó.

Os *clusters* representam objetos e são definidos por um identificador de 16 bits. Semelhantes aos objetos usados em linguagens de programação orientadas a objetos, os *clusters* são constituídos por atributos e comandos. Os atributos podem representar o estado das variáveis do objeto, e os comandos representar funções sobre essas variáveis. Por exemplo, se uma lâmpada for representada por um *cluster* então os atributos podem representar o estado atual da lâmpada e os comandos as funções de ligar ou desligar. Os *clusters* só têm significado dentro de uma aplicação, e as ações tomadas quando são executados comandos têm que ser definidas.

Seguindo o exemplo de uma lâmpada, poderíamos associar-lhe o OnOff Cluster. Este *cluster* foi definido na ZigBee Cluster Library (ZCL) para ser o responsável por interagir com dispositivos em que a sua função é a de ligar ou desligar qualquer coisa. Para além dos *clusters* possuírem um identificador, possuem também uma direção. Esta característica é muito útil nos processos de descoberta de serviços na rede. Uma aplicação pode representar um interruptor num *cluster* OnOff de saída, e quando esta aplicação procurar na rede lâmpadas para controlar, vai ter que procurar pelos dispositivos que

tenham um *cluster* OnOff definido como *cluster* de entrada. Assim, definindo a direção podemos determinar quais os dispositivos que se podem controlar, por que não faz sentido que dois interruptores trocassem comandos um com o outro, visto que tanto lâmpadas como os switch são representados pelo mesmo tipo de *cluster*.

8.6 Perfis

Cada aplicação ZigBee tem associado um identificador de 16 bits (*Profile* ID) que serve para identificar o perfil da aplicação. Um perfil pode ser visto como um domínio de aplicações e dispositivos que estão relacionados. Os perfis estão divididos em duas classes: públicos e privados. Os perfis públicos recebem identificadores na gama entre 0x0000 e 0x7fff, enquanto aos perfis privados são atribuídos identificadores entre 0xbf00 e 0xffff. Os perfis públicos designam tipos de aplicações e dispositivos normalizados com o objetivo de garantir a interoperabilidade entre fornecedores de equipamentos. Os perfis públicos são especificados pela ZigBee Alliance, em oposição aos perfis privados, que são especificados pelos fabricantes individuais.

O Home Automation, por exemplo, é um perfil público que define um conjunto variado de dispositivos ZigBee para uso residencial, incluindo lâmpadas, interruptores, tomadas elétricas, termostatos, aparelhos de ar condicionado, e aquecedores. Qualquer fabricante que forneça equipamentos com aplicações do perfil público Home Automation tem que normalizar o seu produto de maneira a que este funcione com outros do mesmo perfil de fornecedores diferentes. A Tabela 8.2 apresenta alguns dos perfis públicos que se encontram definidos.

Tabela 8.2. Perfis públicos do ZigBee.

Profile ID	Profile Name
0101	Industrial Plant Monitoring (IPM)
0104	Home Automation (HA)
0105	Commercial Building Automation (CBA)
0107	Telecom Applications (TA)
0108	Personal Home & Hospital Care (PHHC)
0109	Advanced Metering Initiative (AMI)

8.7 Aplicações

Esta secção apresenta exemplos de aplicações baseadas em ZigBee que foram desenvolvidas no Departamento de Eletrónica Industrial da Universidade do Minho.

8.7.1 Monitorizador de consumo de eletricidade

No âmbito de um trabalho de dissertação realizado na Universidade do Minho [Pere11], foi desenvolvido um sistema que possibilita a monitorização remota do consumo dos diversos aparelhos elétricos distribuídos por uma residência ou indústria, bem como a deteção de eventos de qualidade de energia elétrica (QEE).

Este sistema adquire, por intermédio de nós sensores ZigBee (medidores) ligados aos aparelhos, os valores de diversas grandezas elétricas (corrente, tensão, frequência, energia ativa e energia aparente), e envia os dados recolhidos via rede sem fios para uma estação base, ligada a um computador pessoal, onde esses dados são apresentados utilizando um software com interface gráfica amigável (monitorizador). Os medidores são capazes também de atuar remotamente sobre o aparelho elétrico, cortando ou fornecendo alimentação, mediante um comando enviado pelo computador. O monitorizador inclui funções simples, de fácil utilização e interpretação, disponibilizando ao utilizador informação da data e hora da aquisição das grandezas elétricas, valores de fator de potência, potência ativa, eventos de

QEE, consumo energético em kWh, bem como o respetivo custo mensal e anual em Euros.

A implementação do sistema está estruturada em três partes: hardware do nó sensor para medição das grandezas elétricas; software embebido para aquisição e envio dos dados através da rede de sensores sem fios até o computador; e software para processamento e visualização dos dados adquiridos no computador.

A arquitetura do sistema é exemplificada na Figura 8.2. O sistema desenvolvido utiliza a topologia malha do ZigBee. O papel de estação base (EB) é desempenhado por um coordenador ZigBee, enquanto o papel de nó sensor (S) tanto pode ser desempenhado por um *router* como por um *end device*. No exemplo dado, o nó sensor S1 transmite os dados diretamente para a estação base. O nó sensor S2, por sua vez, envia os pacotes para um nó encaminhador (E), configurado como *router* ZigBee, que encaminha os pacotes para a estação base. De igual modo, o nó S3 encaminha para a estação base os pacotes enviados por S4. A diferença é que S3, sendo um nó sensor, também envia os seus próprios pacotes de dados para a estação base.

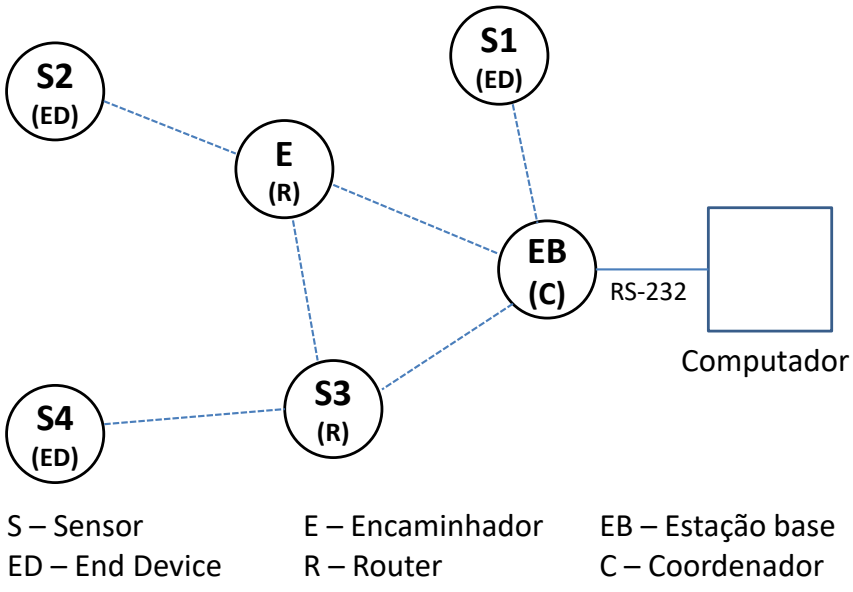

Figura 8.2. Arquitetura do sistema de monitorização de consumo elétrico.

O nó sensor contém um circuito integrado ADE7753, da Analog Devices, que processa os dados recebidos dos sensores de corrente e tensão, um relé,

um bloco de alimentação e um módulo CC2530EM, da Texas Instruments, que lê os dados recolhidos pelo ADE7753 utilizando a interface SPI (*Serial Peripheral Interface*) e os transmite pela rede ZigBee. A Figura 8.3 apresenta a vista superior da placa de circuito impresso do nó sensor.

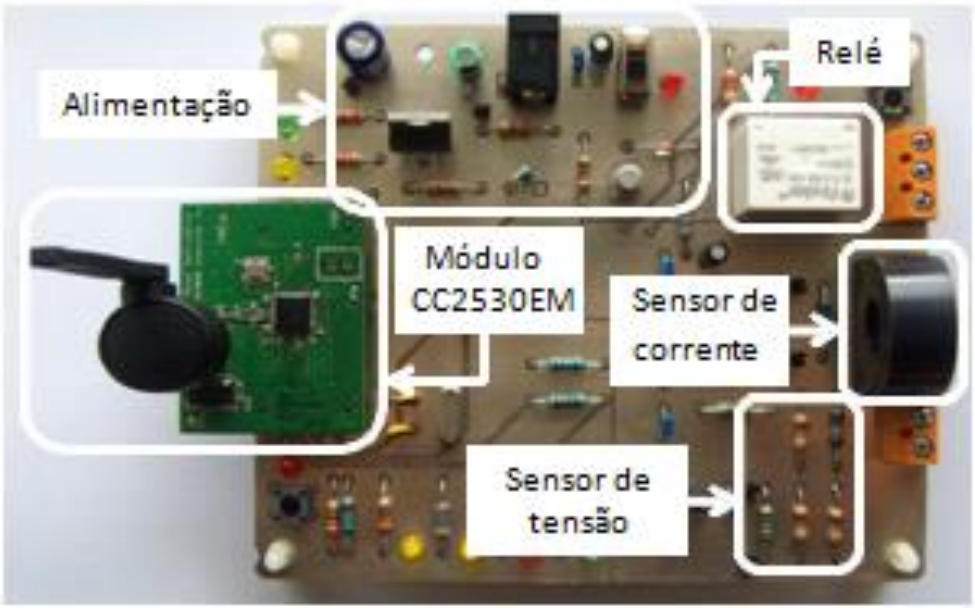

Figura 8.3. Vista superior do medidor de consumo elétrico [Pere11].

Os testes realizados ao medidor indicam que os erros de medição de corrente e de tensão situam-se abaixo do patamar de 1%, o que é bastante satisfatório.

8.7.2 Health Monitoring for All

O sistema HM4All (*Health Monitoring for All*) [Lope11] foi desenvolvido de forma a possibilitar que sinais fisiológicos de múltiplos pacientes possam ser monitorizados em tempo-real, de modo contínuo, com baixo custo e sem restringir a mobilidade dos utilizadores. Este sistema permite monitorizar sinais como a temperatura, ritmo cardíaco ou eletrocardiograma (ECG) de pacientes, tanto no hospital como na residência. Os sinais recolhidos são transmitidos para um servidor central por meio de uma rede de sensores sem fios implementada utilizando ZigBee/IEEE 802.15.4. O servidor central tem como função a gestão, armazenamento e disponibilização dos dados referentes quer

aos valores dos sinais medidos, quer a informações acerca dos pacientes, dos utilizadores do sistema ou dos sensores. Todas as informações do sistema podem depois ser acedidas através de dispositivos com ligação à Internet, como computadores pessoais ou dispositivos móveis (*smartphones* ou PDAs).

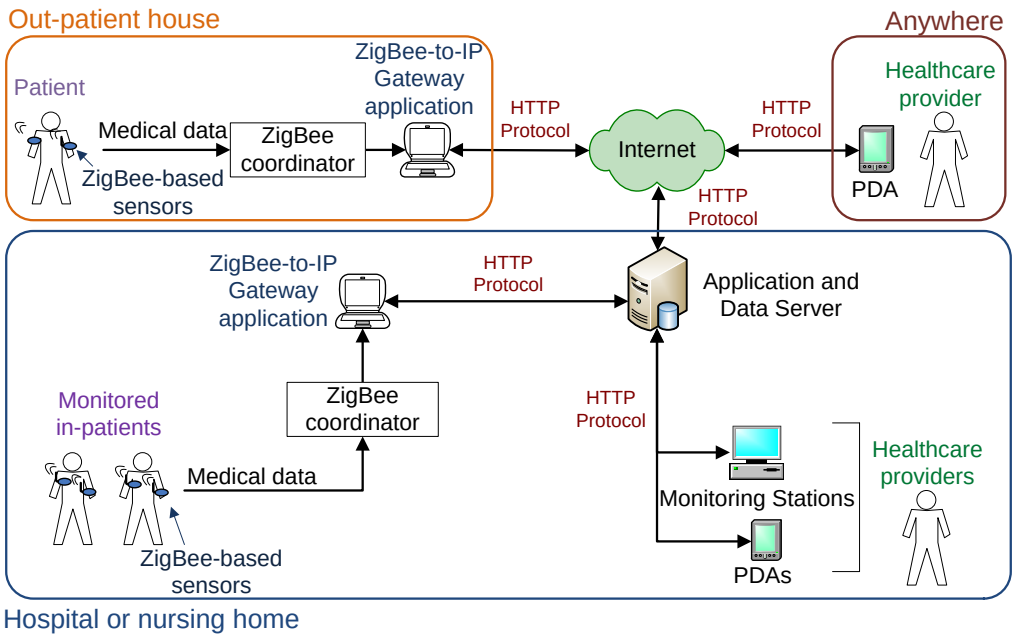

Figura 8.4. Arquitetura do sistema HM4All [Lope11].

Dois dispositivos sensores sem fios baseados em ZigBee foram desenvolvidos no âmbito deste projeto: um sensor de ECG, que fornece não só o sinal de ECG, mas também a informação do ritmo cardíaco, e um sensor de temperatura para ser utilizado na axila. Ambos os sensores são baseados no módulo ZigBee JN5139-M00, da Jennic.

O sensor de ECG que foi desenvolvido [Mato09] é apresentado na Figura 8.5. À esquerda é apresentado o lado dos elétrodos, que fica voltado para o paciente, enquanto à direita é apresentado o lado oposto, cuja caixa contém um desenho de um coração para indicar a orientação correta de colocação do sensor com relação ao tórax do paciente. Este sensor dispensa o uso de cabos: os três elétrodos descartáveis são encaixados diretamente no sensor, que é fixado a seguir no peito do paciente. Os testes efetuados indicam que o sensor apresenta uma autonomia de 70 horas em uso contínuo com uma pilha CR2.

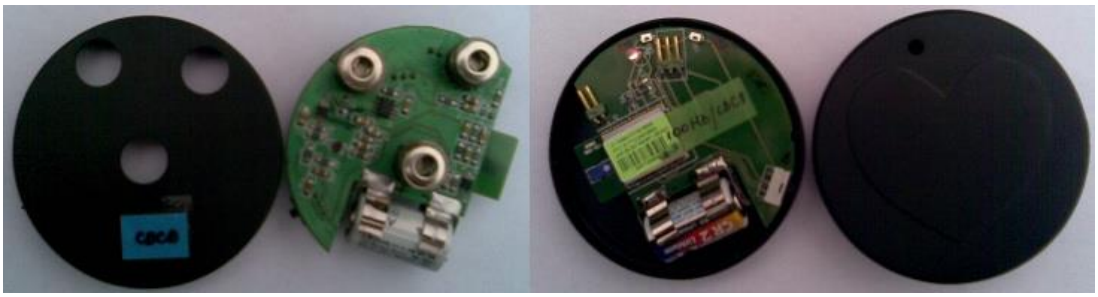

Figura 8.5. Sensor de ECG basado em ZigBee [Mato09].

O sensor de temperatura que foi desenvolvido [Lope11] utiliza um termístor médico para medir a temperatura da axila. Este sensor opera na gama entre 34℃ and 42℃ com precisão de ± 0.2℃ e resolução de 0.1 ℃. O sensor é alimentado por uma pilha botão CR2540 e apresenta uma autonomia de 241 dias em uso contínuo.

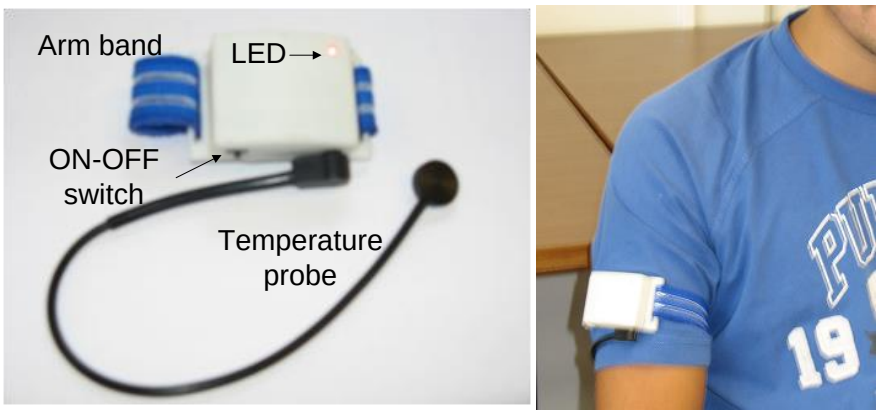

Figura 8.6. Sensor de temperatura baseado em ZigBee [Lope11].

Foram também desenvolvidas aplicações, tanto para computadores pessoais como para dispositivos móveis [Fern11], que permitem, por meio de uma ligação à rede local sem fios do hospital ou através da Internet, que os profissionais de saúde tenham acesso a diversas funcionalidades de monitorização e gestão do sistema: visualização em tempo real dos sinais dos pacientes; visualização de históricos dos sinais ao longo do tempo; geração de alarmes para valores fora dos limites definidos pela aplicação para cada paciente; representação do nível da bateria correspondente a cada sensor; gestão da informação dos pacientes e dos sensores (listar, inserir, editar e remover); e gestão da associação de sensores a pacientes.

A Figura 8.7 apresenta a janela de monitorização da aplicação que foi desenvolvida para o sistema operativo Windows Mobile, onde se pode observar valores reais recolhidos dos sensores de um paciente em tempo real: a forma de onda do sinal de ECG, o ritmo cardíaco em bpm e a temperatura em ºC, bem como o nível de bateria dos sensores.

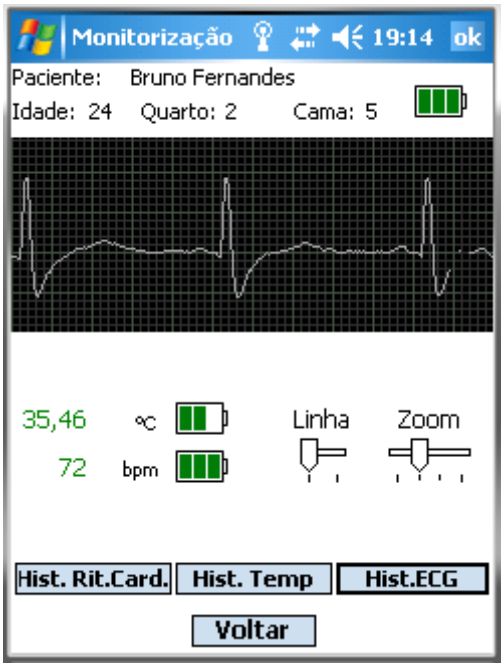

Figura 8.7. Janela de monitorização da aplicação de monitorização e gestão desenvolvida para dispositivos móveis [Fern11].

Este sistema foi extensivamente testado num piso de internamento do Hospital Privado de Guimarães. A Figura 8.8 apresenta a configuração utilizada nos testes de desempenho da rede ZigBee com a topologia em estrela com dois saltos. Outras configurações também foram testadas, bem como os efeitos do *clock drift* e de nós ocultos. A descrição dos testes efetuados e resultados obtidos está disponível em [Lope11] e [Lope12].

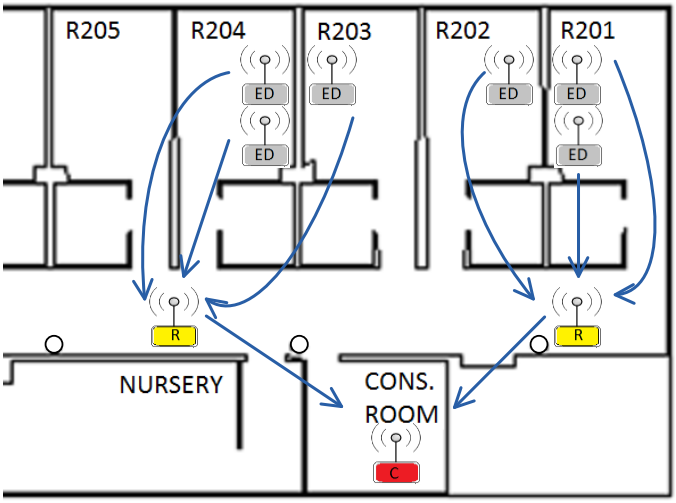

Figura 8.8. Configuração para os testes de desempenho da rede ZigBee em topologia estrela no piso de internamento do hospital [Lope12].

Referências

[Fern11] Bruno M. V. Fernandes, “Sistema de Monitorização e Gestão de Sinais Vitais baseado em Dispositivos Móveis”, Dissertação, Mestrado Integrado em Engenharia Eletrónica Industrial e Computadores, Universidade do Minho, Dezembro de 2011.

[Gisl08] D. Gislason, “ZigBee Wireless Networking”, Newnes, 2008.

[IEEE03] IEEE Std 802.15.4-2003, “Part 15.4: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks”, October 2003.

[Lope11] Helena Fernandez-López, “Remote Vital Signs Monitoring Based on Wireless Sensor Networks”, Tese de Doutoramento, Programa Doutoral LTI EDAM-MIT-Portugal, Dezembro de 2011.

[Lope12] H. F. López, J. A. Afonso, J. H. Correia, R. Simões, "Towards the design of efficient nonbeacon-enabled ZigBee networks", Computer Networks, Volume 56, Issue 11, Elsevier, pp. 2714–2725, July 2012.

[Mato09] Ana Carolina L. P. de Matos “Desenvolvimento de um sensor de electrocardiograma compatível com a tecnologia de redes sem fios

ZigBee", Dissertação, Mestrado Integrado em Engenharia Biomédica, Novembro de 2009.

[Pere11] Manuel A. P. C. Pereira, "Sistema Distribuído de Monitorização de Consumos e Qualidade de Energia Elétrica", Dissertação, Mestrado Integrado em Engenharia Eletrónica Industrial e Computadores, Universidade do Minho, Dezembro de 2011.

[ZigB04] ZigBee Specification, ZigBee Document 053474r06 Version 1.0, December 2004.

9. Redes de sensores sem fios

9.1 Introdução

Ao contrário das redes convencionais, cujo foco principal consiste na partilha de informação (e.g., dados, voz, vídeo) entre seres humanos, as redes de sensores sem fios (WSN - *Wireless Sensor Networks*) [Karl05] interagem com o ambiente físico, recolhendo informação através de sensores ou mesmo controlando variáveis ambientais por intermédio de atuadores.

Além da diferença apontada acima, as redes de sensores sem fios apresentam diversas outras características diferenciadoras das outras redes. Nas redes convencionais, muitos dispositivos operam ligados à rede elétrica, pelo que não apresentam restrições de energia, ao contrário de outros dispositivos, como os telemóveis, que operam com baterias. No entanto, mesmo estes últimos estão normalmente sempre junto ao utilizador, que efetua o recarregamento da bateria sempre que necessário. As redes de sensores, por outro lado, podem conter um grande número de nós alimentados por baterias (que podem chegar a milhares, nalgumas aplicações) distribuídos pelo ambiente, pelo que não é viável que uma pessoa se encarregue do recarregamento das baterias dos nós da rede neste caso. Sendo assim, uma das principais ênfases das redes de sensores sem fios é colocada no baixo consumo de energia dos nós, para possibilitar que estes operem com autonomia de meses ou anos sem necessidade de manutenção.

Várias medidas são necessárias para reduzir o consumo dos nós. Grande parte da energia é gasta com as comunicações sem fios, pelo que uma das características típicas dos nós das redes de sensores sem fios é a baixa potência de transmissão. Outra medida aplicada consiste em comutar o nó para um modo de muito baixo consumo de energia (*sleep*) sempre que possível, reativando o nó somente quando há uma tarefa a realizar. Esta

medida requer protocolos de comunicação eficientes do ponto de vista energético, concebidos especificamente para estas redes, de modo a coordenar quando o nó deve estar ativo e quando pode ficar em modo *sleep*. Esta coordenação não é uma tarefa simples, pois enquanto um nó está em modo *sleep* não está apto, por exemplo, a receber um pacote de outro nó. A percentagem resultante da divisão do tempo ativo pelo tempo total é chamada *duty cycle*. Naturalmente, quanto menor o *duty cycle*, maior será a eficiência energética do protocolo.

A baixa potência de transmissão implica que o alcance direto das transmissões dos nós também é pequeno. Sendo assim, para possibilitar o aumento do alcance da rede são utilizadas topologias *multihop*, nas quais os nós intermediários são utilizados para encaminhar os pacotes entre o nó de origem e o destinatário.

Como foi referido anteriormente, as redes de sensores sem fios podem ser formadas por um número muito grande de nós. Sendo assim, é desejável que esses dispositivos tenham um custo muito baixo. Este requisito, aliado à necessidade de baixo consumo de energia, leva a que os dispositivos dessas redes apresentem tipicamente pouca capacidade de processamento e memória.

Nas redes de sensores, os nós que pertencem a uma mesma rede cooperam para atingir um objetivo comum, definido pela aplicação desejada. Em grande parte das aplicações, a informação transmitida pela rede consiste em leituras esporádicas de dados adquiridos por sensores, pelo que o tráfego transportado pela rede é muito baixo quando comparado ao que é exigido das redes convencionais. Como consequência, as redes de sensores também costumam oferecer taxas de transmissão de dados muito inferiores às das outras redes.

9.1.1 Aplicações

As redes de sensores sem fios têm um enorme potencial e podem ser aplicadas em inúmeros cenários, aproveitando as capacidades inerentes dos sensores e atuadores. Estas redes podem ser usadas em áreas como:

Indústria – Aplicações que impliquem monitorização ou controlo em ambientes industriais, nas áreas de automação industrial e controlo de processos. Exemplos incluem a monitorização de uma linha de montagem; o controlo de um dispositivo mecânico, como um servo motor; ou ainda o acionamento de aparelhos elétricos por via de relés.

Agricultura e pecuária – Através da instalação de redes de sensores sem fios em ambientes agrícolas, pode ser obtida uma maior precisão, por exemplo, na irrigação dos campos se forem usados sensores de humidade no terreno. Um outro exemplo é o uso de sensores nos animais, podendo-se assim obter dados fisiológicos do seu corpo, como por exemplo a temperatura, aferindo-se assim o seu estado de saúde.

Prevenção de desastres – Monitorização de variáveis ambientais em florestas e cidades, como temperatura e humidade, tendo em vista aplicações como a prevenção de incêndios. Monitorização de vulcões.

Meio-ambiente – Monitorização da biodiversidade da fauna e da flora em *habitats* naturais. Monitorização da qualidade do ar e alerta da presença de substâncias poluentes no meio-ambiente.

Edifícios inteligentes – O uso destas redes permite aumentar o nível de conforto dos que habitam nestes edifícios e diminuir o seu consumo de energia. Isto é conseguido através da monitorização e controlo de parâmetros como a temperatura, humidade e fluxo de ar, o que permite eliminar possíveis gastos desnecessários.

Redes veiculares – Monitorização do tráfego em redes rodoviárias para prevenir acidentes e evitar engarrafamentos.

Medicina – Através de sensores colocados nos pacientes, é possível monitorizar o seu estado clínico (parâmetros como batimento cardíaco,

temperatura e pressão arterial) e enviar alertas para os prestadores de cuidados de saúde em caso de deteção de anomalias.

Segurança/Vigilância – Provisão de segurança e controlo de entrada em edifícios, estacionamentos e zonas urbanas, detetando, por exemplo, a entrada na zona de indivíduos ou objetos suspeitos.

Estruturas de engenharia civil – Monitorização de estruturas como pontes, túneis e monumentos tendo em vista a deteção precoce de falhas estruturais e a manutenção preventiva antes da ocorrência de acidentes.

9.1.2 Tipos, distribuição e interação entre os nós

Nas redes de sensores sem fios existem diferentes tipos de nós: nós sensores, que recolhem informação do ambiente; e nós aos quais se destina a informação recolhida da rede, como são o caso das estações base e dos nós atuadores. Podem ainda existir nós dedicados especificamente ao encaminhamento de informação na rede.

No que diz respeito à distribuição dos nós pela área de abrangência da rede, existem três possibilidades. No primeiro caso, os nós são distribuídos de forma aleatória. Um exemplo deste tipo é o lançamento dos nós sobre o terreno a partir de uma aeronave. O segundo caso consiste na distribuição planeada dos nós, por exemplo, a colocação de nós em posições estratégicas de uma ponte para a monitorização de sua integridade estrutural. No terceiro caso, os nós são móveis, como no caso de pacientes sendo monitorizados num hospital.

O padrão de interação existente entre os nós ajuda a caracterizar os tipos de aplicações numa rede de sensores sem fios:

Deteção de eventos: Os módulos sensoriais reportam à estação base assim que detectem eventos de interesse específico, por exemplo, quando os limites esperados de uma variável que está a ser monitorizada são ultrapassados, como a temperatura ou os níveis de humidade.

Medições periódicas: Os módulos sensoriais coletam e reportam dados do meio em que estão inseridos periodicamente, enviando os dados para a estação base a intervalos constantes. Por vezes, estas medições periódicas são iniciadas após a deteção de um evento.

Monitorização de posicionamento: A posição de um evento que se pretende monitorizar pode não ser fixa, como na localização de um indivíduo ao longo do tempo. Neste caso os nós da rede cooperam para determinar e reportar a posição.

9.1.3 Requisitos característicos das redes de sensores

Para o desenvolvimento e posterior instalação de uma rede de sensores sem fios, alguns requisitos devem ser levados em conta para que a rede possa satisfazer, com eficácia, as necessidades da aplicação que se deseja implementar.

A finalidade principal de uma rede convencional consiste na transmissão de dados entre dois ou mais pontos. Nas redes de sensores sem fios normalmente é desejado, para além disso, que estas forneçam respostas, associadas à medição de determinados processos físicos, que são dependentes da aplicação.

Dependendo da aplicação da rede de sensores, parâmetros de qualidade de serviço convencionais relacionados com o débito e o atraso podem não ser tão relevantes. Por outro lado, a fiabilidade não só das comunicações, como da própria deteção dos eventos, bem como o grau de exatidão e precisão das medições assume papel relevante.

No que diz respeito à tolerância a falhas, um nó alimentado por bateria tem um tempo de vida limitada, podendo ainda ser danificado de outras formas. A autonomia de nós individuais pode ser de menor importância se houver nós redundantes na vizinhança capazes de desempenhar a tarefa desejada em caso de falha de um nó.

Dado que uma rede de sensores sem fios pode ter que suportar um grande número de nós, os protocolos e arquiteturas da rede devem ser capazes de satisfazer este requisito de escalabilidade.

Além de processar a informação, pode ser necessário que os nós reajam, de forma flexível, a mudanças nas suas tarefas. Para isso, é desejável que seja possível a reprogramação dos nós durante a operação da rede, quando novas tarefas se tornam importantes.

É desejável também que a rede seja capaz de realizar tarefas de manutenção de si própria, de forma autónoma, por exemplo, adaptar-se a mudanças no ambiente e na própria rede, monitorizar o seu próprio estado (e.g., a carga restante da bateria dos nós) e incorporar novos recursos (e.g., novos nós).

9.1.4 Mecanismos para satisfação dos requisitos

Como foi referido anteriormente, o baixo consumo de energia é um requisito essencial para aumento da autonomia dos nós operados por baterias, o que requer otimizações do consumo a nível das comunicações, processamento, sensores e atuadores. A comunicação *multihop* também costuma ser necessária para aumentar o alcance da rede. Mecanismos de autoconfiguração também são necessários, uma vez que é esperado que a rede funcione sem necessidade de manutenção no local e com um mínimo de configuração manual.

A colaboração entre os nós e o processamento local são outros mecanismos desejáveis para aumentar a eficiência da rede, através do pré-processamento dos dados localmente, em cada nó ou entre um conjunto de nós vizinhos. Por exemplo, para determinar a temperatura média numa zona, em vez de enviar as leituras individuais de cada nó para um destinatário remoto, o cálculo e envio de um único pacote com a média das leituras dos nós daquela zona é mais eficiente do ponto de vista do tráfego gerado na rede.

9.1.5 Desenvolvimentos tecnológicos associados

A proliferação das redes de sensores sem fios depende dos avanços tecnológicos que vêm sendo realizados numa séria de áreas. Para a diminuição dos custos dos nós colaboram os avanços no desenvolvimento das comunicações sem fios, processadores, sensores e baterias, bem como a economia de escala obtida à medida que a proliferação destes componentes aumenta.

Os avanços na miniaturização dos componentes contribuem para a redução do tamanho e peso dos nós, tornando a sua utilização mais conveniente e contribuindo também para a redução dos custos.

Para o aumento da autonomia dos nós existe ainda a possibilidade dos mesmos extraírem energia do ambiente, num processo de recolha de energia denominado em inglês por *energy harvesting* ou *energy scavanging*, o que pode se feito de diferentes formas (energia solar, vibração, gradiente térmico, etc.).

Por fim, o desenvolvimento na área das redes de sensores sem fios é conseguido através da conceção e implementação de novos protocolos de comunicação e pela especificação de novas normas na área.

9.2 Arquitetura dos nós da rede

Os componentes tipicamente presentes num nó de uma rede de sensores sem fios são apresentados na Figura 9.1.

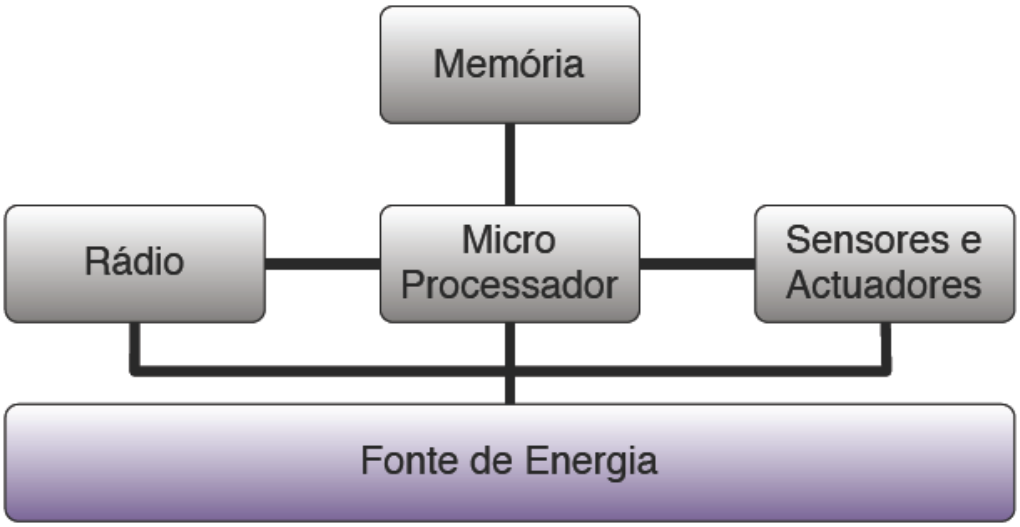

Figura 9.1. Componentes de um nó de rede de sensores sem fios.

A unidade de comunicação (rádio) é o componente que permite efetuar a comunicação entre os nós, possibilitando a transmissão e a receção de dados pelo meio sem fios.

A unidade de processamento, coordena a atividade no módulo, determinando quando e como adquirir dados dos sensores, pré-processar os dados, transmitir pacotes para o destinatário, armazenar ou ler dados da memória, entre outras tarefas. Tipicamente, a unidade de processamento consiste num microprocessador de uso geral otimizado para aplicações embebidas (microcontrolador) e com baixo consumo de energia. Em aplicações específicas, outras opções podem ser tomadas, como o uso de um DSP (*Digital Signal Processor*) quando o processamento de sinal intensivo é necessário, um FPGA (*Field-Programmable Gate Array*), cujo circuito pode ser reprogramado, ou um ASIC (*Application-Specific Integrated Circuit*), que possibilita maior desempenho, mas sem flexibilidade e apresenta maiores custos de desenvolvimento.

Os sensores convertem parâmetros físicos medidos no ambiente (e.g., temperatura, humidade, aceleração) em sinais elétricos que são recolhidos pelo processador. Os atuadores (e.g., relé, motor), por outro lado, permitem converter um sinal elétrico numa ação sobre o meio no qual estão inseridos.

Quanto à fonte de energia, os nós são normalmente alimentados por baterias, podendo em alguns casos contar com energia adicional recolhida do ambiente. Alguns nós da rede, como por exemplo a estação base, podem ser alimentados pela rede elétrica, não tendo assim as mesmas limitações no consumo de energia dos outros nós, o que possibilita ter mais recursos em termos de processamento e hardware, permanecer mais tempo em atividade e utilizar maior potência de transmissão.

9.2.1 Unidade de comunicação

A unidade de comunicação utilizada nas redes sem fios geralmente é um transcetor (*transceiver*) de rádio. O motivo é que o uso de sinais de radiofrequência permite alcances relativamente longos com elevadas taxas de transmissão, quando comparado a outras alternativas, além de não requerer linha de vista entre o emissor e o recetor.

Refira-se, no entanto, que alguns meios de transmissão alternativos podem ser vantajosos em determinados nichos de aplicação. As alternativas incluem o uso de comunicações óticas, ultrassons (adequados para comunicações subaquáticas) e de indutância magnética (em casos específicos para pequenas distâncias).

Um transcetor pode ser colocado em diferentes estados de operação. O conhecimento desses estados e do consumo de energia associado a cada um é fundamental para a redução do consumo do transcetor, que tem um impacto significativo no consumo do nó. Os quatro estados básicos são:

Transmissão (TX) – O nó está efetivamente a transmitir um pacote.

Receção (RX) – O nó esta efetivamente a receber um pacote.

Idle – O nó está pronto a receber dados , mas não se encontra a receber no momento. Por vezes, algumas partes do hardware podem ser desligadas, reduzindo o ligeiramente o consumo.

Sleep – Neste caso, partes significativas do hardware do transcetor são desligadas. Neste estado, o transcetor não é capaz de receber dados.

O consumo do transcetor nos estados de transmissão, receção e *idle* é alto, e costuma ser da mesma ordem de grandeza. Por outro lado, o consumo no modo *sleep* costuma ser muito inferior. Desta forma, é desejável que o transcetor comute para o modo *sleep* quando não estiver a transmitir ou receber dados. No entanto, pode não valer a pena entrar no modo *sleep* por períodos muito curtos, porque a mudança de estado também consome algum tempo e energia. Como o transcetor não é capaz de receber dados no estado *sleep*, é necessário que o protocolo de controlo de acesso ao meio utilizado implemente mecanismos de coordenação entre os nós que evitem que isso aconteça.

Além do conhecimento do consumo do transcetor nos diferentes estados, o projetista da rede deve ter conhecimento de diversas outras características do transcetor, como as bandas de frequência e canais de operação, a taxa de transmissão de dados, a potência de transmissão, o alcance típico e a gama de tensões de alimentação.

9.2.2 Fonte de energia

O objetivo de uma fonte de energia para um nó de uma rede de sensores sem fios consiste em fornecer o máximo de energia possível com o menor custo, volume e peso.

Existem duas opções de baterias para estes nós, dependendo a hipótese de recarregamento:

- Baterias primárias – não recarregáveis;
- Baterias secundárias – recarregáveis, sendo usadas em conjunto com algum mecanismo de recolha de energia do ambiente.

Requisitos para as baterias utilizadas incluem:

- Alta capacidade por volume (J/cm3) – dado que se deseja que os nós sejam de pequenas dimensões.
- Capacidade sob carga – o nó pode estar sujeito a diferentes níveis de consumo e apresentar consumo elevado em alguns modos de operação.

- Baixa taxa de auto-descarga – a quantidade de carga perdida pela bateria quando esta não se encontra em funcionamento deve ser baixa, para não comprometer a autonomia desejada de meses ou anos de funcionamento sem substituição da bateria.
- Recarregamento eficiente, mesmo com baixas correntes – a corrente fornecida por mecanismos de recolha de energia do ambiente tende a ser baixa e intermitente, pelo que a bateria deve ser eficiente nessas condições e não sofrer do efeito memória.
- Estabilidade de tensão.

9.3 Protocolos MAC para redes de sensores

O controlo dos instantes de envio e receção de pacotes é uma das tarefas mais importantes numa rede de comunicação sem fios, sendo fundamental no caso das redes de sensores sem fios, uma vez que o protocolo MAC tem grande influência no consumo de energia do nó ao controlar os estados de operação referidos na secção 9.2.1. Desta forma, um protocolo MAC concebido para uma rede de sensores deve ter em consideração as características destas redes em geral e da aplicação desejada em particular, além de enfatizar a operação eficiente do ponto de vista do consumo de energia. Além disso, é desejável que a solução concebida tenha baixa complexidade, uma vez que os nós da rede possuem capacidades de hardware e processamento limitadas.

Como foi referido na secção 4.3, a implementação de protocolos MAC em redes sem fios impõe alguns desafios adicionais não existentes em redes cabladas. A deteção de colisão é inviável devido ao fenómeno de *self-interference*. A potência do sinal recebido em meio livre decresce com o quadrado da distância. A taxa de erros num meio sem fios é maior e mais variável que nos meios cablados. Além disso, para o sucesso de uma transmissão, o que conta é a interferência sobre o recetor, que pode ser muito diferente da observada pelo emissor, dando origem ao problema da estação oculta referido na secção 4.3.1.

Como foi referido na secção 9.2.1, a transmissão e a receção de dados tem custos energéticos elevados nas redes de sensores sem fios. O consumo no estado *idle* pode ser ligeiramente menor, mas costuma ser da mesma ordem de grandeza. Somente no modo *sleep* é que o consumo é substancialmente inferior. Tendo isso em consideração, uma das principais tarefas de um protocolo MAC para redes de sensores sem fios consiste em eliminar as fontes de desperdício de energia referidas abaixo:

- **Colisões** – Colisões representam um desperdício óbvio de energia, uma vez que os nós emissores consumiram energia para a transmissão de dados que não chegaram em condições ao(s) recetor(es).
- ***Idle listening*** – Como o nome diz, este fenómeno consiste em desperdiçar tempo, e consequentemente energia, a escutar o meio (portanto, com o transcetor ativo) sem que estejam a ser recebidos dados.
- ***Overhearing*** – Este fenómeno consiste na receção de dados que estão a ser enviados para outro nó, o que representa um desperdício de energia uma vez que a receção é inútil neste caso.
- ***Overheads* do protocolo** – Esta parcela engloba os tempos associados à transmissão e receção pacotes de controlo e cabeçalhos dos pacotes de dados, bem como os tempos mortos entre pacotes (*gaps*, períodos de *backoff*), que consomem energia, mas não são efetivamente utilizados para a transmissão dos dados associados ao *payload* da aplicação.

9.3.1 Categorias de protocolos MAC

Tal como foi feito na secção 4.2.2, os protocolos MAC para redes sem fios podem ser divididos em duas categorias no que concerne à coordenação do acesso ao meio: controlo centralizado e controlo distribuído. No primeiro caso, existe um nó, o controlador central, que controla quando os outros nós podem aceder ao meio, enquanto no segundo caso, os nós coordenam o acesso ao meio de forma distribuída. O controlo centralizado não é viável para redes formadas por uma grande quantidade de nós espalhados por uma área extensa, mas pode ser implementado se a rede for dividida em áreas menores,

denominadas *clusters*. Neste caso, em cada *cluster* passa a haver um nó que controla o acesso dos nós vizinhos pertencentes ao mesmo *cluster*.

Dos tipos de protocolos mencionados na secção 4.2.2, os protocolos de *polling* não costumam ser utilizados em redes de sensores sem fios porque requerem que o nó esteja ativo à espera de receber um pacote de interrogação do controlador central para poder enviar os seus dados, o que causa desperdício de energia devido ao *idle listening*. Os protocolos de reserva dinâmica implícita também não são utilizados porque não há lugar à transmissão de pacotes de voz e porque estes protocolos requerem a escuta constante do meio. Sendo assim, os dois tipos básicos de protocolos MAC em redes de sensores sem fios são:

- **Protocolos baseados em escalonamento** – Correspondem aos protocolos centralizados de reserva (fixa ou dinâmica) referidos anteriormente. A operação destes protocolos é baseada na reserva de recursos, como frequências de transmissão e *slots* temporais, para a transmissão ou receção de pacotes. Sendo assim, o desperdício de energia associado a colisões, *overhearing* e *idle listening* é eliminado. Por outro lado, estes protocolos exigem a renovação periódica da sincronização temporal na rede, devido ao *clock drift* dos nós, para evitar que os nós transmitam fora dos limites dos *slots* atribuídos. Além disso, o escalonamento dos recursos numa rede *multihop* não é uma tarefa simples. Essas duas tarefas também introduzem *overhead* adicional que tem impacto no consumo dos nós.
- **Protocolos baseados em contenção** – Correspondem aos protocolos de acesso aleatório referidos anteriormente. Nestes protocolos, o risco de colisão existe. Por outro lado, a complexidade em termos de sincronização e coordenação do acesso ao meio é menor, pelo que o *overhead* com a execução destas tarefas tende a ser inferior.

9.3.2 Problema da estação oculta

Os nós dos protocolos baseados em contenção geralmente utilizam o mecanismo de deteção da portadora (*carrier sense*) para adiar a transmissão quando outra transmissão em curso é detetada, de forma a evitar a colisão. Porém, a deteção de portadora pode falhar quando existem nós ocultos na rede. Sendo assim, vários mecanismos foram propostos na literatura para reduzir o impacto no desempenho dessas redes provocado pelo problema da estação oculta. A seguir são descritas três categorias de soluções propostas para este problema, baseadas em tom de ocupado, RTS/CTS e agrupamento de nós.

Nos mecanismos baseados em tom de ocupado (*busy tone*), o recetor informa aos nós na sua vizinhança que o meio está ocupado durante a receção do pacote. Isso possibilita adiar potenciais transmissões de outros nós, mesmo quando estes não conseguem detetar diretamente a transmissão em curso. Este aviso é feito através do envio de um sinal de aviso em simultâneo com a receção do pacote. Como já vimos anteriormente, um nó de uma rede sem fios não consegue transmitir e receber ao mesmo tempo na mesma frequência, devido ao fenómeno de *self-interference*. Sendo assim, o sinal de aviso tem que ser transmitido num outro canal específico para o efeito. A desvantagem destes mecanismos é a necessidade de hardware adicional nos módulos para transmissão e receção do sinal de ocupado, bem como correspondente acréscimo no consumo de energia dos nós.

Nos mecanismos baseados RTS/CTS, por outro lado, o recetor informa aos nós na sua vizinhança que o meio estará ocupado antes da receção do pacote de dados propriamente dito. Isso é feito utilizando os pacotes de controlo RTS e CTS. O funcionamento deste tipo de protocolos é descrito com mais detalhes na secção 4.3.1. A principal desvantagem destes mecanismos é o *overhead* introduzido pelos pacotes de controlo, que é particularmente relevante nas redes de sensores sem fios, visto que os pacotes de dados transmitidos por essas redes tendem a ser pequenos.

Os mecanismos baseados em agrupamentos de nós [Koub09] foram propostos para reduzir os efeitos dos nós ocultos em redes de sensores sem fios. A ideia consiste em separar os nós em grupos, de modo a não haver nós ocultos num mesmo grupo. Após isso, são atribuídos períodos separados para cada grupo fazer as suas transmissões. A principal desvantagem deste mecanismo é a complexidade e os respetivos custos em termos de consumo, processamento e largura de banda associados à identificação dos nós ocultos e a formação e atualização dos grupos de nós visíveis.

9.3.3 Protocolo S-MAC

Nos protocolos baseados em contenção convencionais, uma estação tem que estar continuamente a escutar o meio para saber se outra estação começou a transmitir um pacote para ela, o que leva ao desperdício de energia devido ao *idle listening*. Como foi visto anteriormente, as redes IEEE 802.11 (secção 5.1.5) e IEEE 802.15.4 (secção 7.3.3) definem mecanismos semelhantes que permitem a um dispositivo entrar em modo *sleep*, para poupar energia, sem o risco de perder pacotes destinados ao mesmo. Para isso, os pacotes pendentes para esses dispositivos são armazenados até que o dispositivo acorde e peça o seu envio. No entanto, esse modelo de comunicação assimétrico requer a existência de dispositivos com capacidade energética muito maior, como pontos de acesso ou coordenadores, para efetuar o armazenamento dos pacotes e atendimento dos pedidos conforme as necessidades dos dispositivos com limitações energéticas.

Esta seção apresenta um exemplo de um protocolo baseado em contenção concebido para redes de sensores sem fios, denominado S-MAC [Ye02], no qual todos os dispositivos envolvidos na comunicação têm limitações energéticas. Este protocolo assume que a quantidade de tráfego trocada pelos nós é pequena. Sendo assim, conforme ilustra a Figura 9.2, a ideia adotada pelo protocolo S-MAC para minimizar o *idle listening* consiste em sincronizar as transmissões/receções de dados entre nós vizinhos de forma que estas ocorram de forma periódica (*wakeup period*) durante curtos períodos (*active*

period). Consequentemente, fora desses períodos, os nós podem passar o resto do tempo (*sleep period*) a “dormir” para economizar energia.

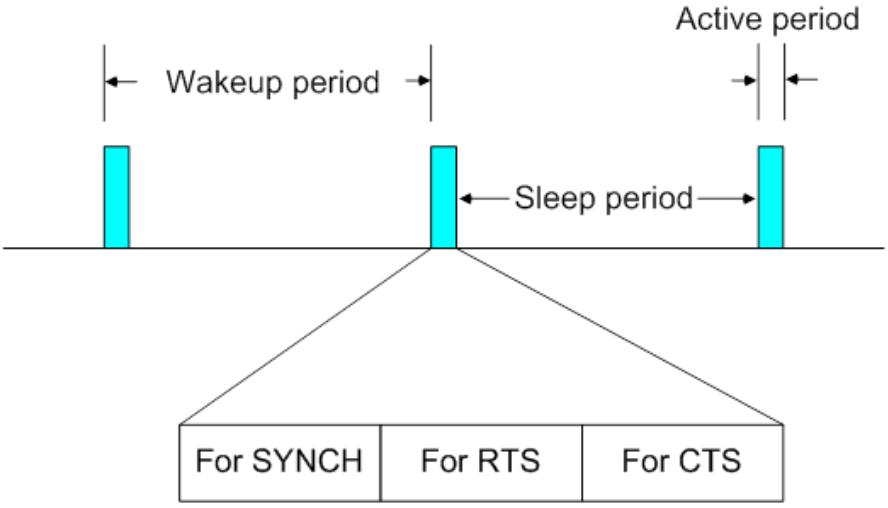

Figura 9.2. Princípio de funcionamento do protocolo S-MAC [Karl05].

Para o protocolo funcionar, os nós têm que difundir pacotes de sincronização, para que os nós vizinhos possam tomar conhecimento do escalonamento adotado, que especifica o momento de início de cada período ativo. Estes pacotes necessitam de ser enviados periodicamente, caso contrário o sincronismo seria perdido em pouco tempo devido ao *clock drift* dos nós.

Durante os períodos ativos, a transmissão do pacote de dados é precedida pelos pacotes de SYNCH, RTS e CTS. Os nós que seguem o mesmo escalonamento competem pelo envio de pacotes de SYNCH e RTS utilizando um algoritmo CSMA. O pacote CTS é transmitido a seguir à transmissão de um pacote RTS pelo destinatário dos dados. Caso um nó não tenha um pacote de dados a receber, pode voltar imediatamente a “dormir”, caso contrário, fica “acordado” até ao fim do recebimento do pacote.

A área abrangida e a quantidade de nós existentes numa rede de sensores sem fios podem ser muito grandes, pelo que não é viável existir um único escalonamento dos períodos ativos para toda a rede, mas sim vários escalonamentos disjuntos seguidos por conjuntos diferentes de nós, criando o que pode ser chamado de ilhas de sincronização.

O processo de definição dos escalonamentos utilizados, de modo a possibilitar a comunicação entre os nós, começa com a escuta do meio pelo nó, quando este inicia a sua operação na rede. Decorrido algum tempo, se o nó não ouviu nenhum pacote de sincronização, define o seu próprio escalonamento e passa a difundi-lo para outros nós durante o período ativo. Os nós que procedem desta forma recebem a denominação de sincronizadores (*synchronizers*) no protocolo S-MAC.

Se, por outro lado, o nó detecta um pacote de sincronização de outro nó durante o processo de escuta inicial, adota esse escalonamento. Estes nós são denominados seguidores (*followers*).

À medida que outros nós começam a operar na rede, alguns podem detetar dois escalonamentos adotados por grupos diferentes de nós. Para servir de intermediário entre essas ilhas de sincronização, possibilitando assim a comunicação entre os dois grupos, o nó tem que seguir ambos os escalonamentos.

9.3.4 Protocolo LEACH

Esta seção apresenta um exemplo de um protocolo baseado em escalonamento para redes de sensores sem fios, denominado LEACH (*Low-Energy Adaptive Clustering Hierarchy*) [Hein00]. Este protocolo assenta em dois pressupostos: todos os nós da rede estão ao alcance direto de uma estação base afastada, ao qual enviam os seus dados; e todos os nós da rede são homogéneos e possuem restrições em termos energéticos.

O funcionamento do LEACH assenta na divisão dos nós da rede num conjunto de *clusters*, em que cada *cluster* possui um nó, denominado *cluster-head* (CH), que funciona como controlador central para este *cluster*. O *cluster-head* é responsável por criar e manter um escalonamento TDMA, para receber os pacotes dos nós associados ao *cluster*, agregar e comprimir os dados recebidos e enviar o pacote resultante para a estação base. Sendo assim a topologia da rede é uma árvore com dois saltos.

Se os *cluster-heads* fossem fixos durante todo o período de funcionamento da rede, os nós escolhidos rapidamente ficariam sem energia, uma vez que a comunicação entre um *cluster-head* e a estação base é bastante dispendiosa em termos energéticos, além de que o CH tem que permanecer muito mais tempo ativo do que os outros nós do *cluster*. Isto faria com que o CH deixasse de funcionar, impedindo a comunicação dos outros nós com a estação base. Sendo assim, o papel de CH é distribuído por todos os nós da rede ao longo do tempo, tornando mais uniforme a distribuição do consumo de energia.

O protocolo LEACH é organizado por rondas, sendo que cada ronda é subdividida numa fase de configuração (*setup*), onde os *clusters* são formados, e numa fase estacionária (*steady-state*), quando ocorrem transferências de dados para a estação base, como é ilustrado na Figura 9.3.

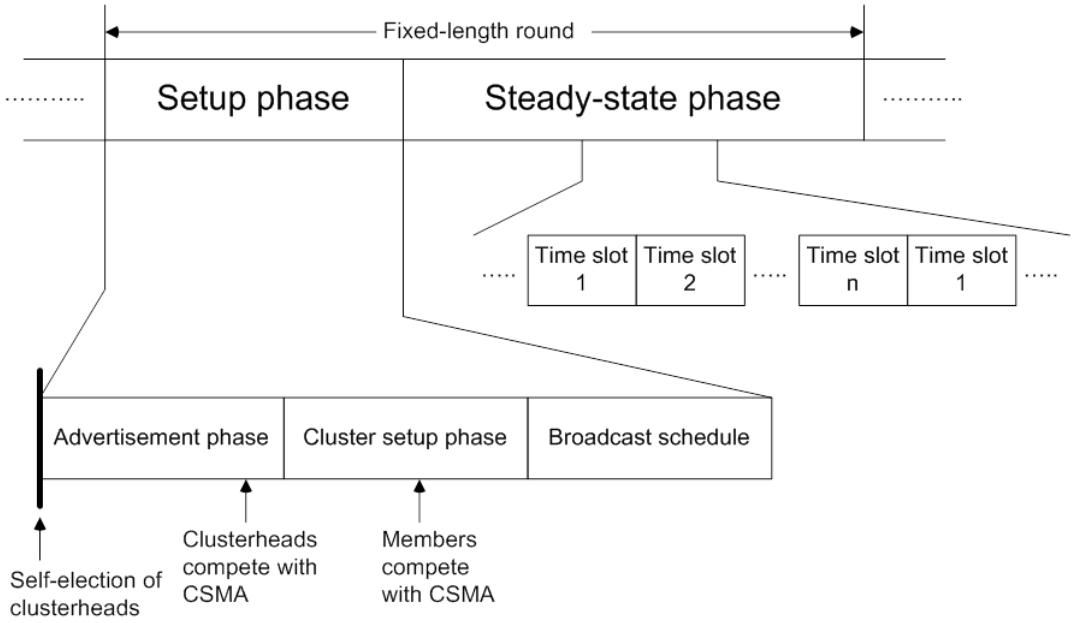

Figura 9.3. Fases do protocolo LEACH [Karl05].

A fase de configuração é ela própria dividida em várias etapas. Na primeira etapa, todos os nós da rede executam um mesmo algoritmo para determinar se serão (ou não) *cluster-heads* naquela ronda, com base numa certa probabilidade e na função desempenhada em rondas anteriores. Na etapa seguinte (*advertisement phase*), cada *cluster-head* eleito difunde essa informação aos seus vizinhos, e cada nó que não tenha sido eleito CH na ronda

determina a que *cluster* quer pertencer, pela escolha do CH do qual recebeu o sinal com maior intensidade. Na etapa seguinte (*cluster-setup phase*), cada nó associa-se ao CH escolhido, usando para isso o protocolo CSMA. Depois de receber todos os pedidos de associação ao seu *cluster*, o CH define um escalonamento TDMA fixo e difunde essa informação para todos os nós pertencentes ao *cluster*.

Com os *clusters* organizados, a transmissão de dados propriamente dita pode começar, entrando-se assim na fase estacionária. De modo a minimizar o *overhead* associado ao processo de formação dos *clusters*, a fase estacionária é longa comparada com a fase de configuração. Os nós enviam seus dados periodicamente, nos respetivos *slots* alocados pelo CH, a cada trama TDMA. O transcetor de cada nó que não seja CH pode permanecer desligado até o momento de enviar os dados, enquanto o CH deve manter o seu rádio ligado para receber os pacotes de todos os nós do *cluster* e para enviar a seguir os dados comprimidos para a estação base. Uma vez que todos os *clusters* utilizam o mesmo meio para comunicar, as transmissões de um *cluster* podem interferir com a comunicação de um outro cluster nas proximidades. Para reduzir essas interferências cada *cluster* no LEACH comunica usando um código CDMA diferente. A Figura 9.4 apresenta um exemplo de uma rede a operar com base no protocolo LEACH numa dada ronda. A composição dos *clusters* varia de ronda para ronda em função dos CHs eleitos na ronda e da proximidade entre os dispositivos envolvidos.

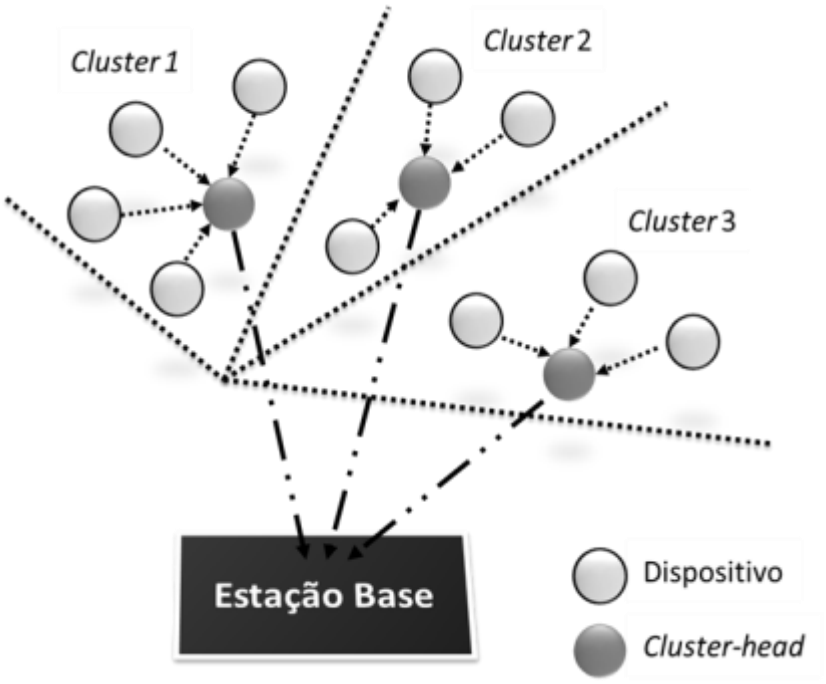

Figura 9.4. Exemplo da configuração dos *clusters* de uma rede para uma ronda do protocolo LEACH [Mace10].

Em [Hein02], os mesmos autores apresentam uma versão aprimorada deste protocolo, denominada LEACH-C (*Low-Energy Adaptive Clustering Hierarchy-Centralized*). Ao contrário do algoritmo distribuído para eleição dos CHs utilizado pelo LEACH, que pode levar a formações imperfeitas de *clusters*, no protocolo LEACH-C a formação dos clusters é centralizada, sob o controlo da estação base. No protocolo LEACH-C a fase estacionária é igual à do protocolo LEACH, o que difere é a fase de configuração. Nesta fase, cada nó envia para a estação base informação quanto à sua localização e nível de energia que apresenta no momento. Com base nesta informação a estação base determina quais são os melhores candidatos a serem *cluster-heads*, organiza os *clusters* de forma a distribuir os gastos energéticos por todos os nós da rede, e envia uma mensagem de difusão contendo a identificação dos *cluster-heads*.

Em ambos os protocolos, a eficiência na redução do consumo energético em comparação com outras alternativas é fortemente dependente da

compressão dos dados que é efetuada nos *cluster-heads* e da localização afastada da estação base em relação aos nós da rede.

9.4 Análise do consumo de energia

Atualmente existe um grande interesse na investigação e desenvolvimento de transcetores de rádio com baixo consumo de energia, dada a limitação energética dos dispositivos operados por baterias. Diferentes pressupostos a respeito das características do rádio, incluindo a energia consumida nos estados de transmissão e receção, podem levar a diferentes resultados na avaliação do desempenho de redes e protocolos de comunicação, pelo que o modelo utilizado na avaliação deve procurar fornecer uma representação fiel da realidade. Esta secção considera o modelo de consumo de energia de rádio apresentado em [Hein00], que é descrito a seguir.

9.4.1 Modelo de consumo de energia do rádio

Este modelo assume que a energia consumida é proporcional ao número de bits transmitidos ou consumidos, e não ao tempo decorrido. Desta forma, tudo se passa como se o rádio esteja desligado fora dos períodos de transmissão e receção, ou seja, não há energia desperdiçada devido ao *idle listening*. Conforme ilustrado na Figura 9.5, o modelo assume que a eletrónica do recetor consome uma energia fixa por cada bit recebido, sendo o parâmetro associado expresso em J/bit. Por exemplo, um rádio que opere a 250 kbps com uma tensão de alimentação de 3.0 V e com uma corrente no estado de receção de 25 mA apresenta um consumo da eletrónica do recetor ($E_{rx\text{-}elec}$) igual a 300 nJ/bit.

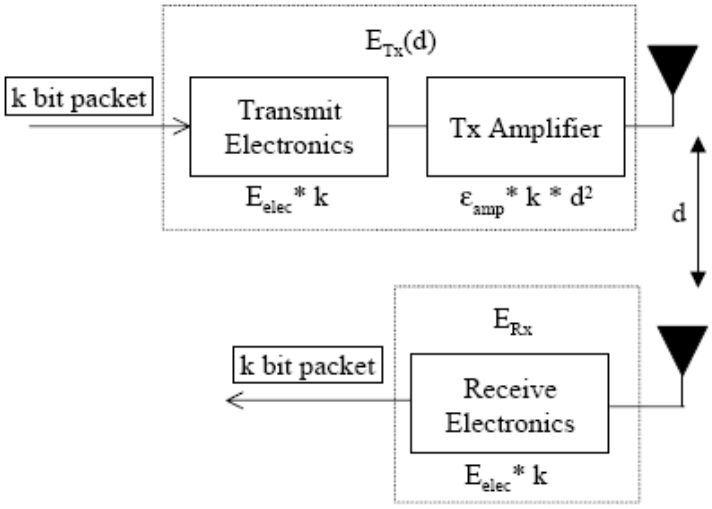

Figura 9.5. Modelo de consumo de energia do rádio [Hein00].

No transmissor, por sua vez, além de uma parcela de consumo por bit associada à eletrónica do transmissor ($E_{tx\text{-}elec}$), o modelo inclui outra parcela associada ao amplificador de transmissão (ϵ_{amp}), necessária para alcançar-se um valor aceitável de E_b/N_0. Esta parcela é proporcional ao quadrado da distância (d) entre o emissor e o recetor, o que está de acordo com a perda em espaço livre expressa na equação 2.1. No resto desta análise, assume-se que $E_{tx\text{-}elec} = E_{rx\text{-}elec} = E_{elec}$. A Tabela 9.1 apresenta um exemplo de valores atribuídos aos parâmetros deste modelo.

Tabela 9.1. Valores atribuídos aos parâmetros do modelo.

Operação	**Energia consumida**
Eletrónica do transmissor ($E_{tx\text{-}elec}$)	50 nJ/bit
Eletrónica do recetor ($E_{rx\text{-}elec}$)	
$E_{tx\text{-}elec} = E_{rx\text{-}elec} = E_{elec}$	
Amplificador de transmissão (ϵ_{amp})	100 pJ/bit/m^2

Conforme ilustrado na Figura 9.5, a energia consumida na transmissão é dada pela expressão:

$$E_{tx}(k,d) = k(E_{elec} + \epsilon_{amp} \times d^2)$$

A energia dissipada na receção, por sua vez, é dada por:

$$E_{rx}(k) = k \times E_{elec}$$

9.4.2 Análise de estratégias de encaminhamento

Esta secção analisa e compara o consumo de energia de uma rede na utilização de duas estratégias de encaminhamento diferentes. Na estratégia de comunicação direta, cada nó da rede envia os seus dados diretamente para a estação base. Se a distância entre o nó e a estação base for grande, a comunicação direta vai exigir uma grande quantidade de energia para transmissão por parte dos nós, fazendo com que a carga da bateria se esgote rapidamente. Por outro lado, a receção é feita na estação base, que não apresenta limitações energéticas, pelo que esta pode ser a melhor estratégia quando as distâncias envolvidas são pequenas ou a energia requerida pela eletrónica de receção é elevada.

Na estratégia alternativa considerada nesta secção, denominada MTE (*Minimum Transmission Energy*), os pacotes são encaminhados de nó em nó, desde o nó de origem até a estação base, através dos nós mais próximos no caminho. Neste caso, cada nó intermediário consome energia para receber o pacote e encaminhá-lo para o nó seguinte. Alguns protocolos que foram propostos na literatura ignoram o consumo associado à eletrónica do transmissor e do recetor, considerando somente o consumo devido ao amplificador de transmissão. Neste caso, a estratégia MTE seria sempre vantajosa em relação à comunicação direta, bastando para isso que, para cada nó B intermediário utilizado no caminho entre dois nós A e C, a seguinte relação fosse válida:

$$d_{AB}{}^2 + d_{BC}{}^2 < d_{AC}{}^2,$$

o que ocorreria sempre que os nós estivessem minimamente alinhados.

Porém, na prática temos que considerar o consumo da eletrónica, pelo que a melhor estratégia irá depender da distância entre os nós e a estação base,

bem como das caraterísticas específicas dos rádios utilizados no que concerne ao consumo da eletrónica do transmissor, do recetor e do amplificador de transmissão. Para facilitar a análise, vamos considerar a rede simples, com os nós alinhados, apresentada na Figura 9.6. A rede é formada por um número (*n*) variável de nós operados por baterias (*n* = 5 no exemplo da figura), e a distância entre nós consecutivos (*r*) é igual. O nó mais afastado está situado à distância *d* da estação base, sendo válida a relação *d* = *nr*.

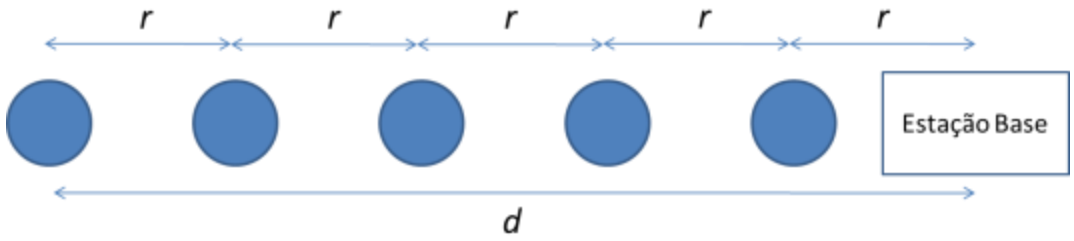

Figura 9.6. Rede linear simples.

Estamos interessados em saber o consumo total dos nós da rede (excluindo a estação base, visto que esta não possui limitações energéticas) para a transmissão de um pacote de tamanho *k*, com origem no nó mais afastado e tendo como destino a estação base. Para a comunicação direta, a energia consumida é:

$$E_{dir} = E_{tx}(k, d) = k(E_{elec} + \epsilon_{amp} \times d^2)$$

Já para a estratégia MTE, a energia consumida é:

$$E_{MTE} = n \times E_{tx}(k, r) + (n - 1) \times E_{rx}(k)$$

Através de manipulação algébrica, é possível chegar à conclusão de que $E_{MTE} < E_{dir}$ somente se a seguinte condição for satisfeita:

$$n < \frac{\epsilon_{amp}}{2E_{elec}} \times d^2$$

Por essa equação, podemos chegar à mesma conclusão alcançada anteriormente de que a estratégia MTE seria mais vantajosa para qualquer número de nós se a energia da eletrónica (E_{elec}) fosse zero. Na prática, porém, se obtivermos $n < 2$ na equação para um determinado conjunto de valores dos

parâmetros, isso significa que a estratégia de comunicação direta será mais vantajosa neste caso[24].

Outra análise interessante consiste em determinar o número ótimo de nós (*n*) para a estratégia MTE, ou seja o valor de *n* com o qual o consumo para esta estratégia é mínimo. Isso pode ser feito tendo como ponto de partida a aplicação da derivada à expressão do consumo de energia da estratégia MTE. Como resultado final, obtém-se a seguinte expressão:

$$n = d \times \sqrt{\frac{\epsilon_{amp}}{2E_{elec}}}$$

A análise teórica feita nesta secção assumiu o modelo linear simples representado na Figura 9.6 para tornar suficientemente simples a manipulação matemática necessária para obtenção dos resultados. Porém, na prática, geralmente os nós da rede apresentam uma distribuição geográfica mais complexa. Para possibilitar a avaliação e obtenção de resultados em cenários mais complexos, como neste exemplo, normalmente recorre-se à simulação computacional.

Referências

[Hein00] W. B. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks”, *Proceedings of 33rd Annual Hawaii Internacional Conference on Systems Sciences*, Maui, Hawaii, USA, 2000.

[Hein02] W. B. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, “An Application-Specific Protocol Architecture for Wireless Microsensor Networks”, IEEE Transactions on Wireless Communications, Vol. 1(3), pp. 660-670, October 2002.

[24] Note que com *n* = 1 não há encaminhamento, e a estratégia MTE passa a ser idêntica à comunicação direta.

[Karl05] H. Karl and A. Willig, “Protocols and Architectures for Wireless Sensor Networks”, John Wiley & Sons, 2005.

[Koub09] A. Koubâa et al., “Improving Quality-of-Service in Wireless Sensor Networks by Mitigating Hidden-Node Collisions”, IEEE Transactions on Industrial Informatics, Vol. 5, No. 3, August 2009.

[Mace10] P. Macedo, “Desenvolvimento de Modelos de Simulação de Redes de Sensores sem Fios”, Dissertação de Mestrado, Mestrado Integrado em Engenharia Eletrónica Industrial e Computadores, Universidade do Minho, Novembro de 2010.

[Ye02] W. Ye, J. Heidemann and D. Estrin, “An Energy-Efficient MAC Protocol for Wireless Sensor Networks”, *Proceedings of IEEE INFOCOM 2002*, pp. 1567-1576, 2002.

10. Redes de área corporal

10.1 Introdução

Uma rede de área corporal (BAN - Body Área Network) ou redes de sensores corporal (BSN - Body Sensor Network) é uma categoria particular de rede de sensores sem fios em que os dispositivos da rede (sensores, atuadores, *routers*, estação base) situam-se no interior, sobre ou em torno do corpo humano. Exemplos do primeiro tipo incluem dispositivos implantáveis e cápsulas endoscópicas. Já no caso dos dispositivos colocados sobre o corpo, estes podem ser incorporados na própria roupa do utilizador (*wearable*) ou fixados ao corpo por outro método.

As redes de área corporal possuem diversas aplicações nas áreas dos cuidados de saúde, desporto e entretenimento. No primeiro caso, estas redes podem ser utilizadas para monitorização contínua de sinais fisiológicos de pacientes, como eletrocardiograma (ECG), temperatura, oximetria, pressão arterial, eletroencefalograma (EEG), eletromiograma (EMG), nível de glicose no sangue, etc., sem restrição à mobilidade e à realização das tarefas normais diárias. Estas redes têm o potencial de deteção precoce e prevenção de patologias, o que não só resulta em benefícios para a saúde do utilizador, mas também permite evitar o recurso a tratamentos mais onerosos numa fase mais avançada. Por exemplo, muitas doenças cardíacas são associadas a anomalias esporádicas, como alterações transitórias na pressão arterial ou arritmias, que muitas vezes não são detetadas com a utilização de equipamentos de monitorização convencionais [Lo05]. Outro exemplo consiste na deteção e prevenção de quedas com base no uso de acelerómetros e outros sensores.

Na área do desporto, sensores podem ser utilizados para monitorizar parâmetros como o ritmo cardíaco e a atividade biomecânica (por exemplo,

pelo uso de sensores de postura [Afon08]) durante a atividade física, permitindo avaliar o estado de saúde e auxiliar na melhoria do desempenho. Na área do entretenimento, estas redes podem ser utilizadas, por exemplo, para captura de movimentos e controlo em videojogos, bem como para transmissão de vídeo, áudio e dados para dispositivos do tipo *wearable*.

10.2 Arquiteturas de comunicação

As redes de área corporal podem ser implementadas com base em diferentes arquiteturas. Em [Chen11], é feita uma divisão da arquitetura destes sistemas em três camadas: a primeira camada (intra-BAN), envolve a comunicação entre os dispositivos da BAN no corpo de um utilizador e um dispositivo pessoal que também é transportado pelo utilizador. O dispositivo pessoal tanto pode ser um dispositivo móvel de uso geral, por exemplo, um *smartphone*, como pode ser um dispositivo concebido especificamente para essa função. A segunda camada (inter-BAN) envolve a comunicação sem fios entre o dispositivo pessoal e um ponto de acesso ou estação base instalado fora do corpo. Nesta camada podem ser utilizadas tecnologias como Wi-Fi, Bluetooth, ZigBee, 3G, etc., sendo que uma mesma rede pode abranger múltiplos utilizadores. A terceira camada (beyond-BAN) visa proporcionar o acesso e armazenamento remoto da informação, por exemplo, via Internet.

No que concerne à primeira camada, existem três arquiteturas básicas:

a) Ligação por fios entre os dispositivos da BAN e o dispositivo pessoal;
b) Comunicação sem fios entre os dispositivos da BAN e o dispositivo pessoal;
c) Comunicação direta entre os dispositivos da BAN e o ponto de acesso (ou a *routers* fora do corpo), integrando assim as duas primeiras camadas e dispensando a necessidade do dispositivo pessoal.

A Figura 10.1 apresenta um exemplo de arquitetura do primeiro tipo, que consiste numa rede de área corporal desenvolvida no Departamento de Eletrónica Industrial da Universidade do Minho tendo em vista a utilização em sessões de hidroterapia e reabilitação em piscinas [Silv07]. Esta BAN integra

um sensor de ritmo cardíaco (*ear clip*), um sensor de frequência respiratória (*respiratory belt*) e diversos módulos de monitorização da postura (*sensing modules*). Todos esses dispositivos estão inseridos num fato de banho e são ligados por fios ao dispositivo pessoal (*floating device*), que é anexado ao fato e fica a flutuar sobre a superfície da água. O dispositivo pessoal agrega os dados de todos os sensores e envia para uma estação base utilizando o protocolo LPRT (Low Power Real Time), que também foi desenvolvido no DEI. O dispositivo pessoal e a estação base são baseados em módulos MICAz, cujo hardware é compatível com a norma IEEE 802.15.4 na banda de 2.4 GHz. Ao nível da camada MAC, no entanto, o protocolo IEEE 802.15.4 foi substituído pelo LPRT, que permite que a rede sem fios possa monitorizar múltiplos utilizadores ao mesmo tempo de forma eficiente e com suporte de qualidade de serviço.

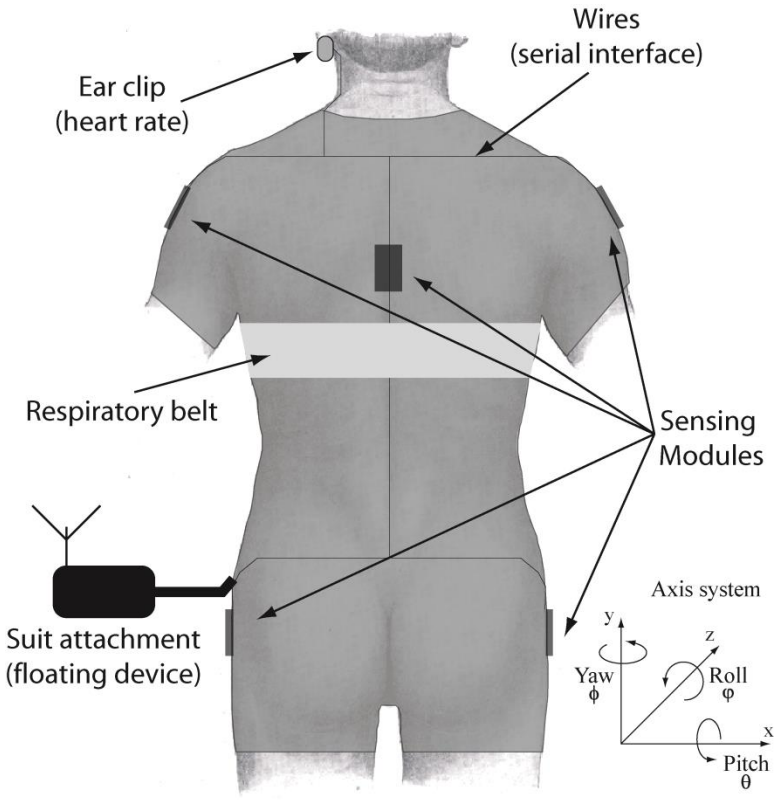

Figura 10.1. Exemplo de arquitetura de BAN com ligação por fios entre os dispositivos sensores e o dispositivo pessoal [Silv07].

Um exemplo da arquitetura do seguindo tipo é apresentado em [Fare08]. Neste sistema, múltiplos sensores enviam os sinais corporais para o dispositivo pessoal (*gateway*) utilizando o transcetor sem fios RFM TR1001, que opera na banda de 868 MHz com uma taxa de transmissão máxima de 100 kbps. O *gateway*, por sua vez, encaminha os dados recebidos dos sensores para equipamentos externos (e.g., um computador pessoal) utilizando uma das interfaces que disponibiliza, como por exemplo Bluetooth, RS-232 ou Ethernet.

Um exemplo de arquitetura do terceiro tipo é o sistema HM4All (*Health Monitoring for All*) [Lope11]. Neste sistema, sinais fisiológicos como a temperatura, ritmo cardíaco ou eletrocardiograma (ECG) são adquiridos por sensores colocados em um ou mais pacientes, em ambiente hospitalar ou doméstico. Estes sinais são transmitidos diretamente para *routers* ou um coordenador ZigBee nas proximidades. Este sistema é descrito com maior detalhe na secção 8.7.2. A principal vantagem deste tipo de arquitetura consiste em eliminar a necessidade de o utilizador ter que carregar um dispositivo extra para além dos sensores (o dispositivo móvel). A comunicação direta para o exterior também diminui o número de ligações sem fios necessárias, em relação ao segundo caso, de duas para uma. Este sistema é flexível de forma a poder passar a utilizar um dispositivo móvel para armazenamento dos dados e transmissão via 3G ou Wi-Fi quando o utilizador se encontra na rua fora do alcance da infraestrutura da tecnologia de rede sem fios utilizada pelos sensores.

Outro exemplo de arquitetura do terceiro tipo é o sistema de monitorização de postura sem fios WPMS (*Wireless Posture Monitoring System*) [Silv11], que é uma evolução do sistema apresentado na Figura 10.1. Neste sistema, ilustrado na Figura 10.2, os módulos de monitorização da postura (*sensor nodes*) comunicam sem fios diretamente com a estação base utilizando uma versão aprimorada do protocolo LPRT, denominada eLPRT (*Enhanced Low Power Real Time*) [Afon11]. Estes módulos são baseados no circuito integrado CC2530, que integra um microcontrolador baseado no 8051 e um transcetor compatível com a norma IEEE 802.15.4 no mesmo chip. Ao dispensar as

ligações por fios entre os dispositivos, o sistema torna-se mais cômodo para o utilizador e mais flexível, pois o número de módulos sensores utilizados e a sua posição no corpo podem ser facilmente alterados consoante as necessidades de cada aplicação em particular.

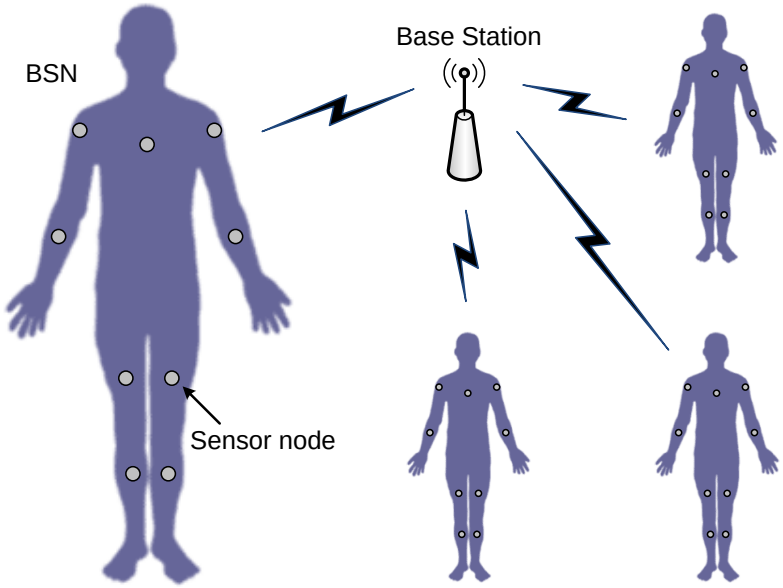

Figura 10.2. Exemplo de arquitetura de BAN com comunicação direta entre os nós sensores e a estação base [Silv11].

10.3 Características das BANs

As redes de área corporal (BAN) são um tipo de rede de área pessoal (PAN), e estão relacionadas com as redes de sensores sem fios (WSN). Apesar dessa relação, existem algumas diferenças entre BANs e WSNs a nível das características e requisitos das aplicações, o que pode fazer com que algoritmos e protocolos concebidos para WSNs não sejam adequados no âmbito das BANs. A seguir são apresentadas algumas características das BANs e suas diferenças com relação às características típicas das WSNs.

- Os dispositivos sensores das BANs normalmente apresentam características heterogéneas em termos de taxa de transmissão de dados, consumo de energia e requisitos de qualidade de serviço (e.g., um sensor

de ECG e um sensor de temperatura). Os nós das WSNs, por outro lado, geralmente possuem características semelhantes.

- No caso da monitorização de sinais fisiológicos, as BANs normalmente geram tráfico periódico. As WSNs, por outro lado, muitas vezes geram tráfego assíncrono em resposta a ocorrência de eventos.
- Os dispositivos sensores das WSNs normalmente geram tráfego de muito baixo débito. Nas BANs, enquanto alguns sensores geram tráfego de muito baixo débito (e.g., temperatura), outros sensores geram sinais com débito muito mais elevado (e.g., ECG, EEG, sensores de postura, etc.).
- Os dispositivos sensores nas BANs são colocados em locais estratégicos no corpo humano, de forma a possibilitar a monitorização adequada do parâmetro desejado em cada caso. Já no que concerne às WSNs, em algumas aplicações os dispositivos são distribuídos de modo aleatório pela área a ser monitorizada.
- Os dispositivos nas BANs podem mudar de posição de acordo com os movimentos do utilizador, pelo que a sua posição relativa pode mudar frequentemente. Além disso, a intensidade dos sinais recebidos também podem ser afetadas pelo corpo humano. Sendo assim, as BANs devem proporcionar os meios necessários para garantir a robustez das comunicações perante mudanças na topologia e nas condições de propagação de sinais provocadas por esses efeitos. Nas WSNs, por outro lado, os dispositivos são normalmente estáticos.
- As BANs utilizam uma quantidade pequena de dispositivos sensores por utilizador, em comparação com o número de dispositivos normalmente presentes numa WSN. No entanto, em algumas aplicações, como a monitorização hospitalar, múltiplos utilizadores podem estar a ser monitorizados ao mesmo tempo.
- Como foi visto na secção anterior, as BANs são normalmente implementadas em arquiteturas de comunicação multicamadas, ao contrário das WSNs.
- Nas WSNs, há o interesse em limitar a potência de transmissão para reduzir o consumo dos nós, de forma a aumentar a sua autonomia. Nas BANs, a

necessidade de utilizar baixas potências de transmissão está associada também, por razões de segurança, a imposição de restrições às emissões de energia eletromagnética nas proximidades do corpo humano.

- O consumo de energia é um aspeto importante tanto nas WSNs como nas BANs. No caso de sensores utilizados sobre o corpo humano, a substituição ou recarga da bateria pode ser uma opção viável, mas é desejável que este processo ocorra com pouca frequência, para minimizar os inconvenientes ao utilizador. Já no caso de sensores implantados, essa questão é mais problemática.
- A segurança das comunicações é essencial nas BANs, pelo que a informação transmitida deve ser protegida do acesso e alteração por parte de utilizadores não autorizados. Os requisitos de segurança devem ser compatíveis com as necessidades de confidencialidade, integridade, disponibilidade e controlo de acesso.

Referências

[Afon08] J. A. Afonso, J. H. Correia, H. R. Silva, L. A. Rocha, “Body Kinetics Monitoring System”, International Patent WO/2008/018810, February 2008.

[Afon11] J. A. Afonso, H. D. Silva, P. Macedo, L. A. Rocha, “An Enhanced Reservation-Based MAC Protocol for IEEE 802.15.4 Networks”, Sensors, Vol. 11, Issue 4, pp. 3852-3873, April 2011.

[Chen11] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao and V. C. M. Leung, “Body area networks: A survey,” Mobile Networks and Applications, vol. 16(2), pp. 171–193, 2011.

[Fare08] E. Farella et al., “Interfacing human and computer with wireless body area sensor networks: the WiMoCA solution”, Multimedia Tools and Applications 38(3), pp. 337-363, 2008.

[Lo05] B. Lo and G. Z. Yang, “Key technical challenges and current implementations of body sensor networks,” in Proc. BSN 2005, London, UK, April 2005.

[Lope11] Helena Fernandez-López, “Remote Vital Signs Monitoring Based on Wireless Sensor Networks”, Tese de Doutoramento, Programa Doutoral LTI EDAM-MIT-Portugal, Dezembro de 2011.

[Silv07] H. R. Silva, L. A. Rocha, J. A. Afonso, P. C. Morim, P. M. Oliveira, J. H. Correia, “Wireless Hydrotherapy Smart-Suit Network for Posture Monitoring”, Proceedings of IEEE International Symposium on Industrial Electronics - ISIE 2007, Vigo, Spain, June 2007.

[Silv11] H. D. Silva, P. Macedo, J. A. Afonso, L. A. Rocha, “Design and Implementation of a Wireless Sensor Network applied to Motion Capture”, Proceedings of 1st Portuguese Conference on Wireless Sensor Networks (CNRS 2011), Coimbra, Portugal, March 2011.