Rui Paulo do Nascimento Gomes

UMA PLATAFORMA PARA REDES DE SENSORES SEM FIOS EM INSTRUMENTAÇÃO INDUSTRIAL

Dissertação de Doutoramento na área científica de Física, especialidade Física Tecnológica, orientada pelo Senhor Professor Francisco José de Almeida Cardoso e apresentada ao Departamento de Física da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Setembro de 2012

· U C ·

Universidade de Coimbra

· U C ·

FCTUC FACULDADE DE CIÊNCIAS
E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

Rui Paulo do Nascimento Gomes

Uma Plataforma para Redes de Sensores Sem Fios em Instrumentação Industrial

Dissertação de Doutoramento na área científica de Física, especialidade Física Tecnológica, apresentada ao Departamento de Física da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Orientador: Prof. Doutor Francisco José de Almeida Cardoso

Coimbra, 2012

Este trabalho foi desenvolvido com base numa parceria entre o Laboratório de Automação e Instrumentação Industrial do Centro de Instrumentação do Departamento de Física da Faculdade de Ciências e Tecnologia da Universidade de Coimbra e a empresa Eneida, Lda.

O projecto foi co-financiado pelo POPH - QREN - Tipologia 4.1 - Formação Avançada, comparticipado pelo Fundo Social Europeu e por fundos nacionais do MCTES, através da Bolsa de Doutoramento em Empresa com a referência SFRH / BDE / 33437 / 2008.

Imagem da capa: "*Oil Refinery at dusk*", por J. K.

Agradecimentos

Agradeço ao meu Orientador, o Professor Francisco Cardoso, por me ter proposto em 2008 o projecto que vim a desenvolver, e pelo seu aconselhamento ao longo dos últimos quatro anos.

Agradeço ao Eng. Carlos Teixeira, Director da empresa Eneida, Lda., por me ter possibilitado aplicar o trabalho desenvolvido num ambiente real, ao implementá-lo para as soluções da empresa.

Ao Engenheiro Ricardo Mendão, pelo apoio prestado no aprofundamento de conhecimentos relacionados com o protocolo de comunicações *6LoWPAN*.

Aos trabalhadores da Eneida, Lda. nas suas diferentes áreas, um grande agradecimento pela saudável colaboração e apoio na instalação dos sistemas desenvolvidos, por vezes com maior necessidade de acompanhamento e esforço da sua parte, pela sua condição piloto dos sistemas.

Um grande agradecimento aos meus colegas de trabalho no Grupo de Sensores Inteligentes da Eneida, Lda., a quem já posso chamar de amigos: o Engenheiro José Oliveira, o Engenheiro Sérgio Faria e o Engenheiro António Silva, pelos anos de trabalho conjunto, discussões e conselhos, que levaram às soluções que reconhecemos como as melhores que conseguimos desenvolver.

E, muito especialmente, às pessoas sem as quais não estaria a escrever este texto, os meus amigos e família.

Agradeço aos meus amigos mais próximos Zé, Miguel, Sílvia, Paulo, Alberto, Idália, Inês V., Rita, Maria João, Gito, Hélder, João, Teresa, Tiago, Rita F., Inês P., Cláudio, por no meio de todos os trabalhos em que todos estivemos envolvidos, termos conseguido estar juntos e apoiar-nos. Aos meus amigos de infância, ao João e ao Sérgio.

À minha família, que manteve sempre a paciência e apoio, a Filomena, o Paulo, a Sofia, a Aurora, o José, o Fernando e a Glória. Ainda à madrinha Salete.

Finalmente, obrigado Andreia, por estares sempre comigo em todos os momentos passados, hoje, e no futuro.

Índice

Índice de Figuras

Índice de Tabelas

Índice de Equações

Índice de Fluxogramas

Resumo

Apresenta-se nesta dissertação o percurso de desenvolvimento de uma plataforma de comunicações modular para redes de sensores sem fios, direccionada especificamente para aplicações industriais. A base do desenvolvimento prendeu-se com a criação de um módulo de comunicações, tanto do ponto de vista físico – *hardware* – como virtual – *software* – altamente versátil, para sua introdução em dispositivos sensores e encaminhadores de dados (vulgo *Routers*) em ambiente industrial, ou seja, para a criação de uma rede de sensores sem fios, congregando os diferentes tipos de dispositivo necessários: um ponto de acesso, *Routers* e sensores. Na realidade, com base nos mesmos princípios desenvolveram-se duas plataformas: primeiro uma com base no protocolo *ZigBee PRO* – na gama dos 2.4 GHz –, com vista à sua compatibilização com outros sistemas, uma vez que se trata de um protocolo de comunicações para redes de sensores sem fios largamente divulgado e aplicado, e posteriormente uma outra plataforma, com base num protocolo proprietário, desenvolvido no âmbito deste trabalho tendo como base o protocolo *SimpliciTI*, na gama dos 433 MHz, para cumprir com critérios de relevância maior na área industrial, nomeadamente um maior alcance nas comunicações entre nós da rede.

Com base nos referidos módulos, criaram-se redes de comunicações suportadas sobre um dispositivo com funções de gestão e de ponto de acesso, com uma interface com um *backbone* de uma rede de campo, esta baseada no protocolo *CANbus*. As referidas redes de comunicações têm uma natureza híbrida, uma vez que não só integram sensores sem fios, como sensores de vibrações e temperatura e de alinhamento e temperatura, como dispositivos que executam funções de reencaminhamento de dados como de integração na rede sem fios de sensores com capacidades de comunicação sobre uma rede *CANbus*, ao terem uma interface para aquele protocolo, para criar uma maior versatilidade no que toca às diferentes aplicações que o sistema enfrentou.

Assim, apresentando as diferentes opções de *software* e *hardware* tomadas, revelam-se de seguida as aplicações que os sistemas desenvolvidos tiveram, nomeadamente a monitorização de pontos quentes em barramentos de alta tensão (com base numa rede *ZigBee*) e a monitorização de equipamentos em subestações eléctricas, mais concretamente em parques de linhas com base numa rede 433 MHz.

Os sistemas desenvolvidos possibilitaram a criação de redes com elementos modulares dedicados à área industrial da Gestão de Activos, ao facilitarem a monitorização de equipamentos industriais como transformadores ou disjuntores, apoiando a Produção e facilitando a Manutenção.

Abstract

It is presented in this thesis the course of the development of a modular communications platform for wireless sensor networks, specifically directed for industrial applications. The basis of this development is bound with the creation of a communications module, from the physical perspective – its hardware – and from the virtual perspective – the software it runs – which is highly versatile, so it can be inserted into sensor devices and data *router*s in industrial environment, i.e., for the creation of a wireless sensor network, which encloses different types of devices: access point, sensors and *router*s.

In fact, two platforms were created based under the same framework: first a platform based on *ZigBee PRO* protocol – in the 2.4 GHz range – in order to be compatible with other systems, for this is a highly disclosed communications protocol for wireless sensor networks. After this first system was created, a second platform was developed, communicating on the 433 MHz range and based on the *SimpliciTI* protocol, to fulfill other relevant criteria for communications in an industrial environment, namely a larger range between network nodes.

Based on the referred devices, communications networks were created, supported by a device with managemenent and access point functionalities, with an interface with a *fieldbus* network *backbone*, the latter one based on the *CANbus* protocol. The referred wireless communication networks have therefore a hybrid nature, for they not only integrate wireless sensors, such as vibration and temperature sensors and alignment and temperature sensors, as well as devices that have functions of routing and integration in the wireless network of *CANbus* based sensors, through a *CANbus* interface. This functionality permits a higher versatility regarding the different applications which the developed systems have faced.

After presenting the different software and hardware options which have been taken, applications for the developed systems are revealed, namely the monitoring of hot spots in high power buses based on a *ZigBee PRO* communication network and the monitoring of equipments in electrical power stations, based on a 433 MHz network.

The developed systems allowed the creation of networks with modular elements dedicated to the industrial area of Asset Management, by facilitating the monitoring of industrial equipments such as high power transformers or switches, supporting Production and favoring Maintenance areas.

1. Introdução

1.1. Enquadramento e Oportunidades

A Instrumentação Industrial é a área da Engenharia dedicada à medida e controlo automático. A sua aplicação é transversal, sendo de extrema importância no controlo de parâmetros de processo na Indústria.

A monitorização de variáveis de processo, grandezas que permitem conhecer o estado actual de cada processo de fabrico sob controlo, tem como finalidade não só esse conhecimento por si só mas também a possibilidade de, partindo do mesmo, tomar acções de controlo sobre o sistema em questão. Assim, é possível ver como a Instrumentação Industrial e o Controlo Automático – a resposta programada a alterações em variáveis – estão intimamente ligados.

A evolução da Instrumentação Industrial tem-se dado no mesmo sentido que outras áreas da Engenharia, congregando conhecimentos tecnológicos que permitam melhorar a performance dos sistemas utilizados, baixando custos e perdas, e introduzindo novas capacidades.

Ao longo da última década têm ocorrido uma série de desenvolvimentos que inserimos na área dos Sistemas Embebidos. Estes avanços consistem sucintamente (i) no aumento das capacidades de microprocessadores, tipicamente de 8 ou 16 bit, chegando actualmente a frequências na ordem das dezenas de MHz, (ii) o baixo custo desses mesmos microprocessadores, que permitem fabricar mais unidades que os integram, (iii) o avanço das tecnologias de comunicação sem fios, mais concretamente na área das redes locais, com o aparecimento de unidades rádio mais capazes e com alcances de comunicação tipicamente até 300 m em linha de vista, (iv) um baixo consumo energético tanto de unidades rádio como de microprocessadores, que permite que os sistemas sejam alimentados a bateria (v) decorrente dos 4 avanços anteriores, o desenvolvimento de protocolos de comunicação dirigidos às redes locais sem fios. A existência de gamas livres de frequência do espectro electromagnético, algumas aplicadas mundialmente, – as chamadas bandas rádio Industriais, Científicas e Médicas (ISM, do inglês *Industrial, Scientific and Medical*) – tornou possível que estas tecnologias se desenvolvessem e se tornassem acessíveis a qualquer integrador de sistemas, tendo em conta que este não terá depois um custo adicional associado à utilização do espectro electromagnético, como acontece no caso das transmissões rádio na gama do VHF (onde existe uma série frequências utilizadas para transmissões televisivas e de rádio – som – que estão restritas a operadores legalizados).

A existência de componentes electrónicos destinados a comunicações sem fios de baixo custo e reduzido tamanho possibilitam que a geração anterior que entrou no mercado da Instrumentação

Industrial, a de sensores inteligentes integrados em rede através de tecnologias *Fieldbus*, como o CAN, o HART ou o PROFIBUS/PROFINET (1),(2) – cabladas – sofra um progresso que permite a remoção desses mesmos cabos e a sua substituição por ligações sem fios, permitindo o avanço das Redes de Sensores Sem Fios (WSN, do inglês *Wireless Sensor Networks*) em ambiente industrial.

Esta oportunidade é extremamente interessante se tivermos em conta que grande parte dos custos de instalação e manutenção deste tipo de sistemas estão associados aos cabos de comunicação e alimentação das unidades remotas – sensores e actuadores, que se estendem por quilómetros, numa nave industrial.

Por outro lado, a comunicação sem fios como alternativa à baseada em cabos traz mais vantagens do que a simples remoção de cabos, considerando as actuais instalações. Permite instalar dispositivos em pontos onde antes não era possível, por serem demasiado inacessíveis para a instalação de cablagens ou situados em partes móveis. Além disso, a poupança em termos de manutenção também é significativa, pois a substituição de cabos danificados é evitada.

À parte dos factores práticos vantajosos, a área das tecnologias sem fios ainda tem uma taxa de penetração relativamente baixa em ambiente industrial (como se verá no capítulo seguinte), existindo portanto mercado para a introdução de novas soluções. A baixa presença de comunicações sem fios em ambiente industrial reflecte também o recente aparecimento da tecnologia e a desconfiança associada que ainda existe para com este tipo de solução.

Esta última tem sido o grande obstáculo à entrada das soluções baseadas em comunicação sem fios no mercado industrial, pois o facto de a tecnologia ser recente e portanto não tão testada e reconhecida quanto as que se encontram instaladas há décadas constitui uma razão bastante forte para que os decisores desta área prefiram manter e continuar a instalar sistemas baseados em cabos até que uma nova tecnologia "amadureça", ou seja, que mais instalações sejam divulgadas – e consequentemente que possíveis erros sejam corrigidos – para demonstrar o seu bom funcionamento. Este obstáculo foi sentido na comunicação com potenciais clientes dos sistemas desenvolvidos no âmbito deste trabalho, que na sua maioria, e apesar de considerarem a colocação de dispositivos sem fios nas suas instalações, rejeitam à partida que esses mesmos dispositivos cumpram quaisquer funções de controlo – associadas à Produção –, pretendendo apenas que executem funções de monitorização.

Apesar de tudo, o ambiente industrial não está totalmente vedado às comunicações sem fios, existindo já aplicações típicas para as quais tem havido espaço para a aplicação deste género de sistemas.

O "segredo" por trás dessas aplicações – e que permite uma maior aceitação desta tecnologia em mercados conservadores – está principalmente relacionado com as novas possibilidades que trazem, com diferentes funcionalidades que as tecnologias cabladas não permitem. São exemplos as aplicações móveis, como os Sistemas de Localização em Tempo-Real (RTLS, do inglês *Real Time Location Systems*) e os sistemas de monitorização de apoio à Manutenção, que trazem novas capacidades de Gestão de Activos sem a necessidade de alteração da infrastrutura, bem como da monitorização de novos pontos, até agora inacessíveis.

A primeira possibilidade traz valências extremamente importantes em termos de segurança de recursos humanos e também activos móveis, sendo a partir daqui possível localizá-los dentro das naves industriais, evitando assim casos como atropelamentos (ao monitorizar pessoas e veículos), colisões (monitorizando veículos), perdas (reconhecendo sempre a localização de itens importantes) e sendo um óptimo auxiliar em situações de emergência (conhecimento da localização de pessoas ou bens).

Por outro lado, traz vantagens do ponto de vista da normal Gestão de Activos, tornando-se mais fácil localizar e seguir tanto meios de transporte como *stocks*.

As aplicações do segundo tipo não estão normalmente associadas a Controlo Automático, consistindo em sistemas de monitorização. Um caso bastante frequente, e no qual as redes de sensores sem fios tiveram (e continuam a ter) uma enorme oportunidade de penetração no mercado industrial é o de sistemas concebidos para Gestão de Activos, mais concretamente relacionados com a Manutenção de Estado Técnico (ou *Condition-based Monitoring* – CbM – em Inglês, como é mais conhecida).

A oportunidade identificada está relacionada com uma perspectiva associada à Manutenção de Activos, que ultrapassa o paradigma da Manutenção Preventiva. A concepção de sistemas que permitem o conhecimento do estado de funcionamento actual de um dado activo de uma nave fabril, como um motor ou um transformador, permite que a manutenção seja feita apenas quando necessária, evitando parar uma linha de produção apenas por prevenção de falha de um dos seus componentes ou, no caso do extremo oposto, da falha desse mesmo componente, por desconhecimento da sua condição. Apesar de já existirem há largos anos dispositivos que cumprem estas funções, a facilidade de instalação de dispositivos sem fios permite, tal como já foi referido, que sejam instalados em novos pontos, levando ao seguimento do estado de equipamentos que até aqui era desconhecido ou monitorizando mais pontos, e a um conhecimento mais completo.

Assim, tendo em conta que este tipo de função (apesar de bastante importante) não é muitas vezes considerado vital para o normal funcionamento das linhas produtivas, tem sido dado

espaço para a instalação de sistemas de monitorização com comunicação sem fios, muitas vezes criando novas capacidades de conhecimento do estado de activos mas também substituindo outros sistemas já instalados.

Os requisitos necessários para os sistemas desenvolvidos provieram das necessidades de empresas da área da Pasta e Papel, Produção de Energia e Geração de Energia, nas quais ocorreram as instalações dos sistemas desenvolvidos.

Com tudo isto em mente, e tendo em conta as oportunidades de mercado existentes, foi a pretensão deste trabalho a de criar e conceber plataformas para redes de sensores sem fios, tanto do ponto de vista do *hardware* como do *software*, desde a sua concepção à prototipagem, seguida da introdução em diferentes produtos (como sensores e *Routers* de dados), continuando para o teste e validação de produto e consequente produção.

As plataformas foram concebidas de forma a se inserirem facilmente em produtos pertencentes ao *portfolio* da empresa Eneida, Lda. na qual foi feito todo o trabalho de desenvolvimento, pelo que foi necessário que esse trabalho incluísse também etapas de concepção de *hardware* e *software* de interface para os respectivos produtos.

1.2. Objectivos

Considerando o estado actual do mercado da Instrumentação e Automação Industrial, e vislumbrando as oportunidades apresentadas, podemos considerar o desenvolvimento de sistemas de suporte à Gestão de Activos, concretamente para Manutenção segundo Estado Técnico, dotados de comunicações locais sem fios.

Assim, é do mais alto interesse a aplicação dos desenvolvimentos tecnológicos recentes já considerados, criando uma nova plataforma de comunicação para redes de sensores sem fios, tendo em conta os seguintes princípios directores:

(i) descentralização de funções, tornando os elementos do sistema tão autónomos em relação aos outros elementos da rede quanto possível, uma medida que possibilita diminuir o número de mensagens a percorrer a rede;

(ii) modularidade, criando componentes do sistema – tanto *hardware* como o *software* correspondente – que possam ser aplicados aos diferentes dispositivos constituintes da rede;

(iii) comunicações sem fios de baixa potência, utilizando uma ou várias bandas rádio livres do Regulamento Rádio da União de Telecomunicações Internacional (agência das Nações Unidas);

(iv) compatibilização com tecnologia *IP*, sobre diferentes bases possíveis: *GPRS*, *Ethernet*, *Wi-fi*;

(v) definição de funções locais (referentes à rede local do conjunto de dispositivos dedicados à instrumentação e comunicações numa dada instalação) que poderão ser invocadas partindo do exterior, tanto através de uma interface de utilizador como a partir de cenários pré-programados, ou do interior da rede, localmente (para cada dispositivo ou elemento constituinte) ou numa unidade gestora de rede, e que são solicitados automaticamente;

(vi) integração da rede sem fios num *backbone* local, uma rede cablada com comunicação através de um protocolo *Fieldbus* – norma em instalações industriais;

(vii) baixo consumo, tornando unidades totalmente desprovidas de cabos – tanto para comunicação como para alimentação – altamente duradouras, reduzindo custos de manutenção;

(viii) compatibilidade com outros sistemas, através da normalização do protocolo, sempre que esta não comprometer a performance pretendida do sistema.

(ix) preço de sistema competitivo;

(x) cumprimento de requisitos legais e imperativos nos ambientes considerados, como compatibilidade electromagnética, impermeabilidade do invólucro contra água e pó (índice IP elevado);

(xi) A aplicação de sistemas sem fios em ambiente industrial, criando uma plataforma modular que servirá de base a uma nova geração de dispositivos para este meio, que virão a substituir os actuais, baseados unicamente em comunicações cabladas;

(xii) Criando sistemas altamente embebidos no ambiente em que são instalados, que se insere nas aspirações descritas no documento – também da ITU – "*The Internet of Things*", que pode assim ter a sua versão em ambiente industrial.

Com tudo isto em mente, o objectivo geral prende-se com o desenvolvimento de dispositivos sensores e de redes sem fios que os integram com todas as características acima elencadas – equilibradas entre si – de forma a criar sistemas inovadores para redes de sensores sem fios para instrumentação industrial, criando bases que permitirão levar à automação industrial. A razão pela qual foi usado o plural prende-se com um certo conhecimento em retrospectiva de decisões que foram tomadas ao longo do trabalho de desenvolvimento. Tal como se verá, com base num único conceito de rede de comunicações, desenvolveram-se dois diferentes tipos de rede de sensores sem fios, com base em duas tecnologias de camada física, para a frequência dos 2,4 GHz e dos 433 MHz. Ainda assim, será ao longo dos capítulos referido como o "sistema desenvolvido", tendo em conta que, apesar de baseado em duas diferentes tecnologias que cumprem diferentes propósitos, o seu conceito de base é o mesmo.

Este sistema é inovador tanto do ponto de vista do conjunto das suas características técnicas, *hardware* e *software* desenvolvido, como do ponto de vista das aplicações para as quais foi desenvolvido, tendo sido feitas instalações destinadas a Subestações eléctricas, Refinarias ou instalações de geração de energia, como barragens.

1.3. Desenvolvimento em ambiente empresarial

Um dos factores que mais marcaram este trabalho está ligado ao facto de todo o desenvolvimento ter sido feito a pensar na produção de produtos, e na aplicação industrial dos sistemas constituídos por esses mesmos produtos. Este factor consiste no facto de este Doutoramento ter sido feito no seio da empresa Eneida, Lda., e de todas as plataformas desenvolvidas, bem como os produtos que integraram, terem efectuado todo um percurso de desenvolvimento que chegou até ao fabrico de pré-série, tornando-se assim produtos constituintes da gama de sistemas de monitorização da empresa.

Este trabalho de concepção e desenvolvimento constitui não só um processo mais longo do que o desenvolvimento de um sistema modelo ou protótipo, englobando outras fases associadas principalmente a:

- pesquisa de componentes, de forma a cumprir com custos máximos pré-estabelecidos;
- programação das diferentes aplicações que implementam as plataformas de comunicações (programação de API de sensores, *Routers*, …)
- desenho de plataformas físicas (placas de circuito impresso, interfaces);
- compatibilização com equipamentos e protocolos de comunicações pré-existentes;
- concepção e desenvolvimento de componentes associados, como invólucros dos dispositivos;
- configuração de mecanismos de configuração / instalação simples e amigável para o utilizador;
- teste dos produtos – como a validação de conformidade electromagnética;
- teste em ambiente real, denominado de instalação piloto;
- passagem para produção – preparação de documentação ;
- cumprimento requisitos de qualidade.

Deste modo, não só se trata de um processo mais longo, como os constrangimentos de tempo despendido em fase de desenvolvimento e custo associado à produção devem ser tidos em conta, influenciando assim todo o processo de desenvolvimento.

Naturalmente, não se pretende com este elenco indicar que todos os tópicos associados ao trabalho executado de concepção e desenvolvimento de produtos em ambiente empresarial serão abordados nesta dissertação, pois não se cumpririam preceitos de brevidade e confidencialidade.

Serão abordados principalmente tópicos associados com questões de índole técnica, e pretende-se com este rol de tarefas transmitir a ideia de que as decisões de projecto tomadas constituem a melhor opção vislumbrada, que equilibra a melhor performance com o custo e o tempo despendido em desenvolvimento, que influencia fortemente o tempo que uma solução leva a ser criada até que é introduzida no mercado (designado de *time-to-market*). Ao longo de vários capítulos desta dissertação, principalmente os capítulos 2 a 5, associados ao estado da arte, e arquitectura de sistema e apresentação das características técnicas dos sistemas desenvolvidos (em termos de *hardware* e *software*), serão avaliados sistemas ou justificadas opções tomadas à luz de um desenvolvimento de equipamentos que se pretendem com um custo e um *time-to-market* tão baixos quanto possível, sem comprometer a performance pretendida.

1.4. Estrutura

Esta dissertação está dividida em 8 diferentes capítulos - incluindo esta introdução –, que podemos dividir em 4 grandes partes: uma primeira onde é discutida a situação actual dos ambientes que vamos tratar e da área tecnológica na qual este trabalho se insere, no capítulo 2; uma segunda parte, referente aos capítulos 1 e 3, onde é apresentada a especificação dos sistemas desenvolvidos, bem como a sua arquitectura – no fundo, a apresentação e explicação das decisões tomadas em termos de arquitectura de sistema; a terceira parte – nos capítulos 4 e 5 – onde é apresentada a implementação técnica da arquitectura descrita nos capítulos anteriores, em termos de protocolo de comunicações, *software* de dispositivo, em termos da sua aplicação, e *hardware* relacionado com diferentes tipos de aplicação e questões mais práticas, referentes nomeadamente à passagem para produção de unidades, e a quarta e última parte, alusiva aos capítulos 6 e 7, descrevendo os testes feitos aos sistemas, as instalações piloto e os resultados obtidos. Finalmente, no capítulo 8, é feita a crítica aos sistemas desenvolvidos, bem como uma conclusão e a apresentação de um rumo para o trabalho futuro.

No capítulo 2, é realizada uma apresentação do geral para o particular, que se inicia com a descrição dos mercados de interesse para os sistemas criados, passando para as principais necessidades e condições-fronteira dos ambientes industriais referentes a esses mercados de interesse, e daí passando para características mais práticas, no que toca às restrições que sistemas de comunicações sem fios deverão ter em conta ao operar em ambientes industriais. De seguida, são apresentadas soluções existentes no mercado que se inserem na mesma categoria daquelas que foram desenvolvidas, iniciando-se aqui a apresentação do estado da técnica. Seguidamente, e como introdução, são representadas as características de base para redes de

sensores sem fios, sendo que depois são apresentadas as principais normas concorrentes de protocolos para redes de sensores sem fios, que já estavam no mercado na altura do início desta dissertação, e que foram opções possíveis. Neste ponto, é feita uma introdução relativa às condicionantes existentes na área dos protocolos para WSN, para indicar a importância que tem a utilização de protocolos modelo reconhecidos, bem como a implementação que esses mesmos protocolos têm no mercado, no ponto de vista de uma empresa de desenvolvimento. Os diferentes protocolos modelo são apresentados tendo em conta as funcionalidades que dispõem por camada protocolar, bem como pelas ferramentas e componentes que existem no mercado para a sua adaptação e criação de novas soluções das quais são base. Ainda neste capítulo, são apresentadas as características físicas de dispositivos rádio para as gamas de frequência tidas em conta, bem como questões de alimentação de dispositivos sensores de baixa potência.

No capítulo 3, referente à Arquitectura de Sistema, são apresentados os cenários de aplicação nos quais se pretende operar, passando-se de seguida para uma descrição da rede de sensores sem fios integrada na rede geral de comunicações, uma rede que congrega diferentes tipos de protocolos e no qual a rede de sensores sem fios se inclui. Finalmente, são expostos os protocolos sob os quais foi feito o desenvolvimento de soluções, quais as razões para a sua escolha, e a forma segundo a qual se integram na solução pretendida. São ainda apresentadas as principais funcionalidades de rede sem fios que ambos os protocolos partilham, e segundo as quais foram escolhidos e desenhados.

O capítulo 4 consagra a implementação dos dois diferentes protocolos por camada protocolar, sendo que é feita a subdivisão por função: como exemplo, a camada de rede do protocolo *ZigBee* é dividida em topologia, associação de dispositivos à rede, formação de rede, encaminhamento de mensagens e comunicação com dispositivos adormecidos. Ainda no mesmo capítulo, são descritas as API para o módulo controlador de comunicações do protocolo 433MHz: para a interface com o respectivo controlador de aplicação e para a interface com a unidade rádio. Como conclusão, é apresentada a estrutura do *firmware* do controlador de comunicações 433 MHz. Este capítulo contém ainda a implementação do ponto de vista de *software* das aplicações desenvolvidas, no âmbito de um sistema de monitorização de equipamentos numa subestação eléctrica sobre o protocolo 433 MHz e de um sistema de monitorização de vibração e temperatura em ambientes industriais, sobre *ZigBee*. A implementação é descrita no ponto de vista da arquitectura geral das aplicações, das funções constituintes do *firmware* e do programa de controlo dos vários controladores de aplicação.

O capítulo 5 contém a matéria técnica referente à implementação física dos diferentes sistemas de monitorização e de comunicações, sendo apresentadas as soluções escolhidas em termos de *hardware*: microcontroladores, sensores, reguladores de tensão, fontes de alimentação e

componentes associados à transmissão sem fios, bem como as placas de circuito impresso desenhadas e os respectivos esquemáticos. São ainda referidas as principais decisões de desenho de PCB tomadas.

O capítulo 6 descreve os testes executados, tanto em laboratório, a características específicas dos dispositivos, como de validação, referentes a testes de conformidade que os dispositivos deverão cumprir, executados por laboratórios externos. São acompanhados pelos respectivos resultados.

No capítulo 7 são apresentadas as instalações piloto terreno em empresas clientes, bem como outras que foram planeadas, servindo como exemplo da variedade de aplicações que a plataforma permite, sendo apresentados os locais de instalação, as suas características, os diferentes pontos de monitorização e a sua razão de ser, a estrutura da rede instalada, entre outras características descritivas da instalação, bem como os principais resultados obtidos.

A dissertação é encerrada no capítulo 8, onde são discutidas as opções tomadas e os resultados obtidos, as linhas orientadoras para o melhoramento dos sistemas desenvolvidos, bem como uma conclusão de todo o trabalho.

2. Redes sem fios na Indústria: oportunidades e tecnologias

2.1. Contextualização no âmbito da Instrumentação Industrial

A implementação de Instrumentação em meio Industrial teve um impacto significativo nas primeiras décadas do século XX, primeiro na Europa, com maior incidência na Inglaterra e na Alemanha, e posteriormente nos EUA, com a instalação de dispositivos de medida de temperatura, pressão e fluxo, vitais para muitas áreas industriais (3). Inicialmente puramente mecânicos, os equipamentos de medida seguiram os principais desenvolvimentos tecnológicos, com indicadores locais, e naturalmente adoptando métodos baseados em variáveis eléctricas, tendo nesta área encontrado a base das comunicações industriais – que nos interessa para este tema –, e que tiveram como grande primeira tecnologia globalmente implementada (baseada em variáveis eléctricas) o *loop* de corrente – forma de comunicação analógica, mais conhecido como *4-20 mA* (os valores mínimo e máximo permitidos a percorrer o par de fios) – que é ainda muito comum em instalações (4).

Com os desenvolvimentos na área da computação, foi possível ter capacidade de tomada de decisão automática por um computador central, através de ligações entre os sensores com saída em *loop* de corrente e um computador programado para "interpretar" os dados recebidos, ao executar automaticamente uma medida de resposta à alteração na sua entrada, através do comando de um outro componente do sistema – um actuador.

Inicialmente, tratava-se apenas de um único computador – peça central dum sistema dito centralizado e monolítico – que recebia a informação proveniente de todos os sensores e accionava todos os actuadores de uma instalação fabril, estando as funções de processamento e apresentação da informação, bem como de comando delegadas a esta unidade.

Com o aparecimento do microprocessador, foi possível distribuir as funções de controlo, em arquitecturas do tipo DCS (do inglês *Distributed Control System*), onde vários controladores se encontram ligados através de um barramento, sendo que cada um tem o seu próprio conjunto de sensores e actuadores e executa as suas próprias funções de controlo automático (5). Uma PLC (do inglês *Programmable Logic Controller*) pode ser considerada uma peça integrante de um

DCS, uma vez que consiste num dispositivo que contém diversas entradas e saídas, para ligação de sensores e actuadores, bem como um microcomputador programável para cumprimento das funções de controlo automático.

Com o desenvolvimento do microprocessador, estas tecnologias desenvolveram-se igualmente, levando a capacidade de controlo ao nível do dispositivo sensor, criando-se a possibilidade de sistemas distribuídos e descentralizados. Essa capacidade ao nível do dispositivo sensor ou actuador levou à necessidade do desenvolvimento de redes comunicações industriais mais capazes e com características próprias, com o aparecimento das Redes de Campo (do inglês *Fieldbus*). A progressão desta tecnologia permitiu atingir o ponto em que é possível distribuir capacidades de processamento e tomada de decisão pelos próprios sensores e actuadores que pertencem a uma rede de comunicações, existindo um microprocessador em cada ponto de aquisição de dados ou actuação, descentralizando e distribuindo o sistema de Controlo Automático.

É este o princípio do dispositivo inteligente, ou no caso das aplicações desenvolvidas, do sensor inteligente, constituído pelo elemento sensor – ou transdutor, normalmente convertendo a variável de interesse para uma variável eléctrica – e por uma unidade que executa, por exemplo, funções como armazenamento, processamento/cálculo, alteração de parâmetros de aquisição por alteração de condições de entrada.

A mais recente clivagem em termos de desenvolvimento e de novas tecnologias, que tem provocado discussões sobre a sua fiabilidade em ambiente industrial e, consequentemente, sobre a sua aplicabilidade, tem ocorrido em torno das comunicações industriais sem fios. Foi em meados da década de 1990 que ocorreram os primeiros progressos numa área que se viria a denominar de "Redes de Sensores sem Fios". As aplicações que foram criadas nessa altura prendiam-se com a capacidade de monitorizar parâmetros de interesse em ambientes remotos ou inóspitos, como um habitat natural de animais (6) ou a cratera de um vulcão em actividade (7), que se tornavam de difícil acesso para observação humana. Assim, as tecnologias existentes para instrumentação, baseadas no microprocessador, e as tecnologias de comunicação sem fios, baseadas em unidades rádio de baixo custo e dimensão, permitiram criar sistemas pouco intrusivos constituídos por pequenas unidades sensor capazes de comunicar entre si, abrindo caminho à comunicação e processamento em rede.

Os consequentes desenvolvimentos desta tecnologia em termos de *hardware* e de protocolo de comunicação criaram espaço para que outras áreas da engenharia a adoptassem, sendo exemplos a Domótica ou a Instrumentação Industrial, que nos interessa neste tema.

No caso da Instrumentação Industrial, os principais interesses são óbvios: a possibilidade de remoção de dispendiosos cabos de comunicação, a monitorização de pontos remotos ou o seguimento contínuo de bens móveis. Por outro lado, existe ainda o receio de que esta tecnologia não esteja suficientemente amadurecida para que possa já ser aplicada ao exigente ambiente industrial, e este afunilamento tem atrasado a sua disseminação total na Indústria. Veja-se que a própria tecnologia *Fieldbus*, que neste momento não é posta em causa, demorou cerca de 25 anos desde a sua criação a tornar-se uma tecnologia considerada totalmente fiável por parte dos agentes decisores na Indústria.

Daí que não estejamos neste momento a debater sobre a aplicação de redes de sensores sem fios ao Controlo Automático, em típicas aplicações de Produção ou Operação em Indústria. A inclusão destas tecnologias em malhas de controlo é ainda muito rara, estando de momento afastadas das aplicações mais comuns da Instrumentação Industrial. As redes de sensores sem fios, no presente momento, conseguiram apenas entrar na área industrial através da Gestão de Activos, em aplicações de Manutenção Preditiva, onde servem propósitos de monitorização contínua de equipamentos fabris.

Assim, e tendo em mente as oportunidades apontadas anteriormente, interessa-nos nomear os principais mercados de interesse, dentro do mundo industrial, bem como quais os tipos de soluções existentes nesses mesmos mercados. Esta informação permite apontar para o grande desafio das redes sem fios quando aplicadas ao ambiente industrial: como entrar no mercado e ganhar o seu lugar como uma solução robusta e prática, que a longo prazo permite a poupança de milhões de euros, e que não traz inconvenientes graves quando comparada com as suas congéneres cabladas, que já ganharam o seu espaço no mercado, e que têm a comprovação de anos em instalações de campo.

Criando-se a oportunidade de entrada no mercado, será possível provar através da prática que as tecnologias sem fios são funcionalmente equivalentes às tecnologias anteriores. Deste modo, neste capítulo definir-se-ão os mercados de interesse, bem como as tecnologias de ponta existentes para resolver as suas diferentes necessidades.

Para além disso, apresentar-se-ão as tecnologias que se encontram actualmente em desenvolvimento, e que ainda não fizeram uma entrada efectiva no mercado, podendo estar bem integradas dentro de alguns anos.

As áreas referidas ao longo desta dissertação têm uma série de características em comum: compreendem ramos de negócio do Sector Primário, nomeadamente as indústrias extractoras, ligadas à exploração mineira ou de pedreiras, mas principalmente ao Sector Secundário da

Economia, ligado às indústrias transformadoras, sendo óptimos exemplos a Pasta e Papel, a Química, a Petroquímica, a Energia, a Têxtil ou a da Electrónica (Produção).

Todos estes mercados têm uma taxa lenta para a aceitação de novos produtos, principalmente quando estes são constituídos na sua base por tecnologias novas. Tomando o exemplo das comunicações sem fios, peça central deste estudo, é facilmente reconhecível que esta tecnologia já entrou em grande escala noutros mercados, sendo comum em ambiente doméstico e também empresarial.

Isto deve-se principalmente ao facto de existirem factores a ter em conta num sentido mais restrito, quando pensados para o ambiente industrial. São esses factores a robustez – principalmente ligada à resistência a factores ambientais extremamente agressivos, a fiabilidade/integridade de dados, a segurança – associada, por um lado, à impossibilidade falha ou erro na comunicação – que poderia levar a interrupções ou acidentes – e, por outro, à máxima impenetrabilidade das redes de comunicações, e a alimentação – associada á performance –, relacionada não só com a capacidade de manter os diferentes dispositivos da nave fabril ligados, mas também com a necessidade de, em algumas instalações, estes terem a obrigatoriedade de cumprir requisitos de segurança intrínseca.

Fazendo uma descrição mais elaborada de cada uma destas características imperativas num sistema de comunicações industrial, é mais fácil compreender as decisões tomadas ao desenvolver um novo sistema baseado em tecnologias sem fios para a Indústria.

Ao longo dos textos desta dissertação existirão referências aos "decisores" da Indústria. Com este termo, pretende-se nomear quadros qualificados em posições de gestão nas diferentes indústrias nomeadas, normalmente engenheiros que progrediram na carreira, tendo inicialmente ocupado cargos com grande componente técnica associada ao processo, e que actualmente gerem áreas da Manutenção ou de diferentes áreas da Produção. Os indivíduos que se pretende indicar são assim conhecedores das tecnologias que foram e poderão continuar a ser usadas na área que gerem, sendo responsáveis pela tomada de decisão sobre a instalação de novos equipamentos.

Muitas vezes, a prospecção de novos sistemas é feita por engenheiros do mesmo departamento que, estando mais ligados ao processo, fazem a selecção dos sistemas actualmente no mercado, tomando assim um conhecimento mais profundo sobre as suas capacidades e vantagens. É por isso que, em reuniões de apresentação de produto, ocorre com frequência que o interlocutor seja um engenheiro de processo ou de manutenção, que terá um maior conhecimento da tecnologia envolvida, e que por isso estará interessado em conhecer as funcionalidades de mais "baixo nível", diga-se assim, do sistema.

Tendo em conta este contexto, é importante detalhar quais as características que os definem, e que, consequentemente, os sistemas de comunicações sem fios devem ter para que possam ser instalados em ambiente industrial, factores que são mais importantes neste ambiente do que no residencial, onde não estão em risco centenas de milhar a milhões de euros, como na paragem de uma linha de produção por avaria de um dos seus componentes, cuja condição era desconhecida.

Deste modo, é necessário ter em conta factores já nomeados, como a robustez contra agentes externos, nomeadamente ruído electromagnético ou alta humidade, a fiabilidade ou integridade de dados entre a sua fonte e o seu consumidor, a segurança ou impenetrabilidade da rede de comunicações e a alimentação ou questões associadas ao consumo dos dispositivos.

Distinguindo as diferentes indústrias nomeadas pelos ambientes que criam, devido aos processos que envolvem, podemos criar três grupos, com diferentes tipos de agentes agressivos e de configuração espacial:

- **Fabril**: unicamente áreas do sector secundário, com instalações onde ocorre a preparação de matérias-primas e a sua transformação em produto final. Dependendo da área em questão, o *shop-floor* fabril poderá ser mais ou menos agressivo, mas é de esperar que existam óleos, pós, ruído electromagnético, ruído sonoro ou vibrações em elevados níveis.

  Para além destes factores, é de ter ainda em conta as movimentações de material entre diferentes áreas da fábrica, envolvendo assim ainda meios de transporte em movimentação pela fábrica, tarefas comuns neste tipo de indústrias. Apesar da existência de muitos agentes agressivos, estes devem-se principalmente devido a factores internos ou inerentes ao trabalho da fábrica, e esta é na sua maioria própria para a permanência de pessoas a trabalhar no seu interior, sendo portanto protegida de agentes naturais exteriores e com temperatura amena. Exceptuam-se desta regra, naturalmente, os pontos de monitorização de maquinaria, onde as temperaturas poderão ser elevadas.
- **Indústria de Processos e de Produção de Energia**: nesta designação incluem-se as áreas *industriais* que normalmente envolvem fluidos, como combustíveis, sendo as suas instalações no exterior, desabrigadas de agentes naturais – como sol intenso, chuva, granizo, gelo ou vento –, e em muitos casos os bens com que lidam são voláteis ou explosivos, e que obrigam a características especiais que os dispositivos ali instalados deverão ter.

  Por outro lado, as bombas e motores necessários para o bombeamento dos fluidos em questão geram ruído electromagnético, com o qual deverá ser necessário contar.

As instalações deste tipo são normalmente mais extensas que as do tipo anterior, tendo os seus activos localizações mais remotas, sendo portanto necessário adaptar a rede de comunicações a essa necessidade. Em muitos casos, como em refinarias, existe uma grande quantidade de áreas com ambientes ditos classificados, sendo um dos exemplos a presença de atmosferas explosivas nesses mesmos locais. Para este tipos de ambientes, os dispositivos usados devem ter características que impedem a criação de arcos eléctricos, e portanto a possibilidade de uma explosão.

- **Mineira**: a Indústria Mineira merece uma distinção dos outros tipos por as suas instalações terem características especiais diferenciadoras dos outros dois tipos, juntando a grande quantidade de factores nocivos, como pós e humidade, com as movimentações de veículos de transporte e de extracção de grandes dimensões, no interior de galerias que são especialmente danosas para a propagação de sinais sem fios. É um ambiente no qual as comunicações sem fios devem ser tratadas com maior cuidado, optimizando o alcance de comunicação das diferentes unidades espalhadas pela mina, para que o impacto das reflexões ocorridas nas paredes das galerias seja minimizado.

É necessário ter especial atenção a alguns dos factores apresentados, que afectam fortemente a performance, tanto em termos de alcance como de taxa de erros, de uma rede de comunicações sem fios.

A Fiabilidade é uma das questões mais importantes associadas a redes de comunicação sem fios, senão o factor essencial que possibilitará a sua maior aceitação em meios mais conservadores. A prova de que a rede é fiável consiste neste âmbito em que a sua probabilidade de falha é extremamente baixa.

Considerando o controlo de um processo, se o dispositivo é dotado das capacidades de medição e de actuação, adicionando-lhe a capacidade de decisão sob uma dada acção de controlo, não existe qualquer problema em caso de falha da rede de comunicações, pois este é independente, do ponto de vista do controlo, não ocorrendo assim paragem no processo. Ainda assim, qualquer rede de comunicações deve ser capaz de detectar falhas na sua estrutura.

No caso de as capacidades de medição e controlo estarem espalhadas por diferentes dispositivos da rede, então a sua fiabilidade tem uma importância ainda maior, e os aspectos associados à fiabilidade devem ser discutidos e tidos em conta com maior cuidado.

Em redes de comunicação cabladas, uma maior fiabilidade pode ser alcançada utilizando componentes de melhor qualidade, como cabos, conectores ou terminações. É um compromisso entre o grau de fiabilidade que se pretende ter e o custo que se está disposto a pagar.

Em redes de comunicação sem fios, também é importante o uso de componentes de melhor qualidade, que permitam ao desenvolvedor ou instalador ter uma maior confiança no material que está a instalar. É por isso relevante ter especial cuidado na selecção de componentes electrónicos vitais para o dispositivo, antenas, cabos de interligação e conectores, bem como às baterias utilizadas (considera-se esta a forma de alimentação por ainda ser largamente a mais comum).

Veja-se que a questão da alimentação é importante para esta discussão, no caso de a própria rede de comunicações depender de unidades alimentadas a bateria. Outro factor relacionado apenas com comunicações sem fios é o da propagação do sinal, que poderá ser afectada ao usar conectores ou antenas de menor qualidade.

Uma medida fulcral a ser usada na arquitectura de uma rede sem fios é a da implementação de características de tolerância a falhas, que permitam que, no caso de um dispositivo fulcral para a manutenção da comunicação entre todos os dispositivos da rede falhar, a própria rede disponha de mecanismos que criem alternativas e possibilitem que a ligação se mantenha.

Para isso, é necessário que algoritmos de pesquisa de rede sejam implementados em caso de falhas de ligação. Tanto quanto possível, esta capacidade deve estar presente em todos os dispositivos, para que mais facilmente se detectem falhas e se implementem as consequentes medidas. Quanto maior for a liberdade de ligações entre os diferentes dispositivos de rede, isto é, quanto mais complexa for a rede, do ponto de vista da sua topologia, maior é a sua tolerância a falhas.

Uma das questões interessantes associadas à discussão de prós e contras às comunicações sem fios para ambiente industrial, principalmente quando comparadas à versão cablada, está relacionada com a possibilidade de intrusão, muito maior quando a capacidade teórica de aceder a uma rede se torna real, ao estar ao acesso de alguém nas suas proximidades. Uma rede cablada, isolada do mundo exterior, é virtualmente inatingível a alguém que não tenha um contacto físico.

Este ponto fraco das redes sem fios, que é absolutamente inerente ao seu princípio de funcionamento e portanto impossível de eliminar, obriga a que sejam tomadas medidas especiais do ponto de vista da segurança da rede, usando técnicas de encriptação de dados que tornem mais difícil a descodificação de dados permutados.

A segurança da rede é um dos pontos essenciais para que as redes sem fios vinguem no mundo industrial, pois trata-se também de um dos pontos que levantam mais dúvidas em relação ao sem fios, por parte dos agentes decisores da indústria.

Enquanto a utilização das redes sem fios se cingir unicamente a aplicações ligadas à Gestão de Activos, seja do ponto de vista da localização de bens móveis ou da monitorização do seu estado, esta questão parece não ter um papel de extrema importância, tendo em conta que um ataque do exterior nunca poderá ter acesso a acções de controlo. Ainda assim, o desenvolvimento do mercado das soluções sem fios terá inevitavelmente de chegar à automação industrial, e portanto é imperativo que estas sejam vistas como seguras, pelo que as medidas para que o sejam devem ser tomadas logo à partida.

Por outro lado, é necessário ter em conta a questão da Privacidade, que deve ser separada do tópico da Segurança pela razão de que normalmente se considera como segurança de uma rede a sua capacidade de impedir acesso ou intromissões ao seu domínio por parte de agentes externos. Estes agentes externos são considerados como pessoas ou sistemas fora da organização detentora da rede, e que assim pretendem lesar ou obter informação dessa mesma organização.

Este tipo de protecção pode ser entendido como do âmbito da privacidade, mas esse tópico deve ir mais além, e estar principalmente relacionado com questões do foro do controlo de acessos. Mesmo indivíduos ou sistemas pertencentes à rede geral da organização (da qual também fará parte a rede de sensores que estamos a considerar) devem estar habilitados ou não a aceder a dados ou comandos dessa mesma rede. Este controlo de acessos impede, por exemplo, que comandos que percorram toda a rede (denominados *broadcast*) e que habitualmente não estão relacionados com a área da instrumentação sejam transmitidos para os dispositivos de campo. Este tipo de segurança é habitualmente legado às *firewall*, que apenas admitem a comunicação com um conjunto de unidades cujo identificador é permitido na rede local.

O planeamento da alimentação em rede, ou dos dispositivos constituintes de uma rede, parecendo demasiado específica para se considerar nas questões gerais que um sistema sem fios para ambiente industrial deverá ter, é uma das principais preocupações de um desenvolvedor desta área, sendo em qualquer sistema um compromisso que deve tomar, entre o consumo dos seus dispositivos e a sua performance associada.

Numa rede cablada, os dispositivos de campo são alimentados recorrendo ao caminho usado pelos cabos de comunicação, estando os fios de alimentação geralmente integrados no mesmo cabo. Esta característica possibilita que quaisquer questões associadas à alimentação sejam habitualmente de menor importância, pois tipicamente um dispositivo de campo não tem um consumo minimamente comparável ao do equipamento que monitoriza, e de onde poderá ser retirada a fonte de alimentação.

Na rede sem fios, o mesmo já não pode ser dito, pois para um dispositivo ser verdadeiramente sem fios, não poderá ter cabos de comunicação ou alimentação ligados, sendo necessário adoptar outros métodos para o alimentar.

Esta necessidade de alimentação local condiciona fortemente decisões associadas à performance do dispositivo – pois para que todos os seus componentes estejam activos continuamente (esta questão, sobre o que poderá significar "continuamente" será discutida mais tarde), o tipo de alimentação local terá de variar, principalmente em tamanho – o que poderá também não ser viável. A solução mais comum, actualmente, é a utilização de baterias, que serão secundárias em soluções móveis, possibilitando uma reutilização mais prática, ou primárias em soluções definitivas, que sofrem manutenção para a sua substituição.

Outras soluções têm aparecido ao longo dos últimos anos, associadas ao aproveitamento de energia proveniente do ambiente em redor, na forma de luz, gradiente térmico, vibração ou campo magnético, considerando apenas alguns exemplos. Denomina-se este tipo de técnica de Captura Energética.

Se é verdade que estas metodologias permitem a criação de sistemas puramente sem fios, é ainda necessário melhorar a sua performance para que seja equivalente à de um dispositivo alimentado pela rede eléctrica (esta afirmação é sustentada pelo estudo apresentado na secção Alimentação de dispositivos de baixa potência, deste mesmo capítulo). Esse impedimento tem afectado a topologia das redes de sensores sem fios, levando a que as redes de sensores sem fios sejam híbridas no ponto de vista da alimentação, existindo dispositivos ligados à rede eléctrica, quando as suas funções obrigam a que o consumo exceda rapidamente o de uma bateria, e dispositivos alimentados localmente, através de baterias ou captura energética, quando as suas funções são esporádicas ou de baixa frequência.

Relativamente à comparação do preço de um sistema sem fios com o preço de um sistema cablado equivalente deve ser tida em conta, visto que é tomada como uma das vantagens dos sistemas sem fios o facto de poupar a instalação do cabo, e portanto o seu preço.

No entanto, para podermos ter uma melhor análise da diferença de preços, é necessário considerar o custo de equipamentos e materiais, e o custo de mão-de-obra para a sua instalação.

Quanto aos materiais usados, é fácil fazer o cálculo do custo do sistema cablado, pois é a soma dos custos em cabos, fichas (ou conectores) e interfaces de rede. Relativamente à instalação, trata-se de um processo algo demorado, sendo obrigatório criar o caminho de cabo e tratar da sua fixação às estruturas pré-instaladas, bem como da ligação entre o cabo e as fichas que serão introduzidas nas interfaces de comunicação dos dispositivos. Ainda associada à mão de obra,

está a manutenção da rede, principalmente ligada à substituição de cablagens ou fichas (que sofrerão maior ou menor desgaste consoante a severidade do ambiente onde estão instaladas.

Num sistema sem fios, o custo provém das interfaces de rede, das unidades alimentadas pela rede eléctrica (ou permanente) e da respectiva cablagem de alimentação e fichas, sendo que o custo destas torna-se equivalente ao custo de um sistema cablado e, para as unidades sem fios, nada mais para além do que o bloco de alimentação, que poderá consistir simplesmente num elemento armazenador, como uma bateria (ainda de longe a solução mais utilizada, ou num elemento de captura energética (como um painel solar ou uma espira condutora, para indução electromagnética) e elemento armazenador associado, que poderá ser uma bateria recarregável ou um supercondensador. Quanto aos custos associados a mão-de-obra, para unidades com alimentação permanente o custo é igual ao de um sistema cablado, e para unidades totalmente sem fios, o custo é simplesmente o da instalação no local. A manutenção é mais regular para um sistema sem fios, visto que é necessário que as baterias sejam substituídas em períodos de tempo regulares, associados à performance requisitada ao dispositivo. Para dispositivos alimentados através de captura energética, o potencial é bastante grande, tendo em conta que virtualmente não necessitam de alimentação (a não ser aquando da falha de algum componente interno).

2.2. Tecnologias de Radiofrequência

Tal como foi apresentado nas secções anteriores, existem algumas características intrínsecas aos sistemas baseados em comunicações sem fios que podem criar desvantagens quando comparados com os sistemas cablados. Nesta secção, interessa apresentá-las, bem como às possíveis soluções para as minimizar ou evitar, pretendendo-se demonstrar que o equilíbrio entre os vários pontos fracos das comunicações sem fios e das suas vantagens quando comparadas com sistemas cablados cria ainda uma oportunidade interessante nesta tecnologia.

2.2.1. Partilha do espectro electromagnético

A partilha do meio físico de comunicação, característica inerente às comunicações sem fios, poderá ser encarada como uma desvantagem para com as redes cabladas, tendo em conta que a interferência provocada entre diferentes redes é praticamente inexistente no cabo e um factor a ter em conta quando é feita a passagem para o sem fios.

Tal como foi indicado anteriormente, esta área das comunicações restringe-se a algumas gamas do espectro electromagnético denominadas de "livres", as gamas de frequência que não necessitam de licença por parte do Estado no qual são feitas, as frequências ISM.

Este facto fez com que todas as entidades criadoras de normas para comunicações e, ao mesmo tempo, OEM de componentes (*Original Equipment Manufacturer* – fabricantes de componentes modulares, para inclusão em outros produtos, que habitualmente fazem parte dessas mesmas entidades associadas a normas) se tenham centrado nestas frequências, sendo as mais utilizadas as que têm como frequências centrais 433,92 MHz, 868 MHz (na Europa), 915 MHz (nos Estados Unidos) e 2,4 GHz. Esta última é a que mais normas para comunicações sem fios tem gerado, sendo os principais exemplos o *Wi-Fi*, o *Bluetooth* e o *ZigBee*.

A definição de gamas de frequência de uso livre tem ainda alguns requisitos, não sendo assim possível transmitir qualquer tipo de sinal nestas frequências. Cada país tem legislação relativa à utilização do espectro electromagnético, sendo na União Europeia a entidade criadora de regulamentos a ETSI (*European Telecommunication Standards Institute*), e nos Estados Unidos a FCC (*Federal Communications Commission*).

Uma curta nota sobre a legislação existente relativamente à utilização do espectro electromagnético: qualquer dispositivo electrónico criado deve ser sujeito a testes de "compatibilidade electromagnética", onde deverá, em termos gerais: (i) cumprir limites de potência (da radiação) emitida numa parte considerável do espectro electromagnético (tipicamente os testes são feitos entre os 300 KHz e os 2,5 GHz); (ii) manter o correcto funcionamento após ser sujeito a uma fonte de ruído electromagnético; (iii) manter o correcto funcionamento após sofrer uma descarga instantânea (de uma fracção de segundo) de uma tensão elevada, tal como está definido nas normas associadas à Directiva Europeia de Compatibilidade Electromagnética (8) – que para a área dos PLC toma a forma da norma IEC 61131-2 (9), parte que se dedica aos requisitos e testes aplicáveis a PLC e periféricos associados (como HMI), em termos de compatibilidade electromagnética, segurança eléctrica, documentação e requisitos normais de funcionamento. Além deste regulamento, os fabricantes de equipamentos rádio devem ainda testar os dispositivos segundo as normas definidas na Directiva Europeia de Equipamentos de Rádio e Terminais de Telecomunicações (R&TTE) (10). O procedimento associado a esta última directiva é necessário para a comercialização de unidades de comunicações rádio de OEM, pelo que qualquer destes dispositivos disponível no mercado estará já conforme a directiva, sendo essa informação disponibilizada pelo fabricante.

Esta legislação permite que, do ponto de vista do normal funcionamento, todos os dispositivos a sair para o mercado sejam inerentemente incapazes de provocar interferências que levem à falha de outros e, por outro lado, que sejam suficientemente robustos para suportar um valor considerado mínimo de ruído.

A necessidade de alguma normalização, para que diferentes sistemas sejam compatíveis, cria este "afunilamento" das frequências utilizadas, o que pode gerar a situação de, num local onde

existam diferentes redes – que servem variadas finalidades –, estas provoquem interferências entre si. Assim, ao desenvolver ou ao instalar um sistema sem fios, é importante ter em mente questões protocolares, associadas à camada de acesso ao meio, física e questões de performance, ao nível do rádio seleccionado. São exemplos o método de modulação, o canal usado, a sensibilidade ou a taxa de rejeição de canal adjacente da unidade rádio, que lhe poderão dar uma melhor performance em ambientes ruidosos.

2.2.2. Atenuação e distorção de sinal

Uma característica igualmente óbvia inerente às comunicações sem fios é a de que o ar não é o melhor meio para a propagação de um sinal. É portanto importante, principalmente aquando da instalação mas também do desenvolvimento de dispositivos para comunicações sem fios, avaliar os factores de propagação de ondas electromagnéticas no ar, como a atenuação de sinal e a distorção multi-caminho.

Relativamente à atenuação de sinal, esta é inversamente proporcional, em segunda ordem, à distância entre o ponto emissor e o ponto receptor. Outros factores influenciam a atenuação que um sinal sofre ao longo de um dado percurso, sendo a relação que permite o cálculo da atenuação – *L,* em *dB* – ao longo de um percurso a equação de *De Friis*, que pode ser escrita na seguinte forma:

$$L = 20\log_{10}\left(\frac{4\pi \cdot d}{\lambda}\right)$$

Equação 1 - Relação de *De Friis*, da qual resulta a atenuação na amplitude de uma onda electromagnética para uma distância *d* (em linha de vista e no espaço livre).

Onde d é a distância entre os dois pontos e λ o comprimento de onda do sinal. Esta equação pode ser escrita numa forma mais simples, que envolve os parâmetros físicos da antena transmissora e da antena receptora, e que permite o cálculo, em *dB*, da potência medida no ponto receptor:

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

Equação 2 - Equação de *De Friis* para a potência do sinal medida pelo receptor (em linha de vista e no espaço livre), a uma distância *d*.

Apesar de, através da equação de *De Friis*, ser possível estimar a potência recebida num dado ponto, e assim poder projectar os locais onde serão instalados os vários nós de uma rede, é também importante ter em mente que esta equação considera um caso ideal, para uma propagação no vazio e em linha de vista, para antenas perfeitamente isotrópicas e sem perdas

nas interfaces com a unidade rádio, e que não tem em conta possíveis interferências provocadas por multi-caminho ou outras fontes de sinal ou ruído.

Estas formas de atenuação provocam frequentemente a existência de pontos onde seria suposto, com base nos resultados da equação, existir comunicação. Na realidade, a comunicação poderá não existir por o sinal do emissor não atingir o receptor, ou a mensagem chegar corrompida devido a, por exemplo, interferências, sendo as principais razões de falha as que se apresentam de seguida.

A distorção multi-caminho (do inglês *multipath distortion*) é provocada por refracções e reflexões da onda transmitida que atingem o receptor, provocando interferência que poderá ter um efeito construtivo ou destrutivo, de acordo com a fase que a onda refractada ou reflectida tem com a onda original que atingiu o receptor. O ambiente industrial é especialmente propício para este tipo de fenómeno, pelo tipo de construção das instalações e maquinaria existente, tipicamente metálicas, que proporcionam a reflexão do sinal.

Por estas razões, é especialmente importante uma boa adaptação do protocolo de comunicação a um ambiente ruidoso e altamente reflector, através da utilização de algoritmos e mecanismos que oferecem resistência à distorção de sinal, nomeadamente através do método de modulação de sinal e da selecção de componentes com boas características de filtragem. Estes mecanismos serão revistos em maior detalhe mais adiante neste capítulo.

2.2.3. Mecanismos de modulação

De forma a não realizar uma apresentação exaustiva de todos os tipos de modulação conhecidos, são apenas apresentados brevemente os esquemas de modulação digital implementados pelos protocolos que serão posteriormente discutidos e desenvolvidos.

2.2.3.1. FSK, 2-GFSK e 4-GFSK

O esquema de modulação FSK, ou *Frequency Shift Keying,* é um tipo de modulação em frequência, em que a informação é codificada através de alterações da frequência do sinal. O esquema FSK consiste na modulação de bits 0 e 1 na frequência da portadora, que altera a sua frequência de acordo com o bit transmitido. A modulação GFSK (*Gaussian Frequency Shift Keying*) constitui um caso restrito da modulação FSK em que é usado um filtro Gaussiano sobre o sinal de saída para reduzir os desvios de frequência. A forma descrita é a mais simples, designando-se de modulação 2-GFSK, onde são usadas duas frequências, para codificar o bit 0 e o bit 1. A modulação 4-GFSK possibilita a codificação de vários bits por cada símbolo, uma vez que compreende quatro diferentes frequências (ou símbolos), codificando cada uma dois bits (11, 10, 01, 00).

2.2.3.2. PSK e QPSK

O mecanismo de modulação PSK – *Phase Shift Keying* – baseia-se na transmissão de informação baseada na variação da fase de um sinal de base.

Na forma mais simples da técnica de modulação, o *Binary Phase Shift Keying*, existem dois valores de fase entre os quais o sinal oscila, para codificar o bit 0 ou o bit 1, sendo a relação entre bit e símbolo de 1:1 (11).

O mecanismo *Quaternary Phase Shift Keying* implementa uma técnica em que é possível codificar dois bits por símbolo, através da variação entre quatro diferentes fases. Modelando este mecanismo, consideram-se quatro diferentes sinais com quatro fases distintas. O fluxo de dados vai chegando ao modulador e é separado em dois outros fluxos (que serão as portadoras), sendo que uma portadora contém os bits pares e a outra portadora os bits ímpares.

Na Figura 1 apresenta-se um sinal original e a sua divisão em portadora I e portadora Q. Veja-se que os sinais I e Q são transmitidos ao mesmo tempo, sendo isso possível através da razão de ortogonalidade que existe entre os dois.

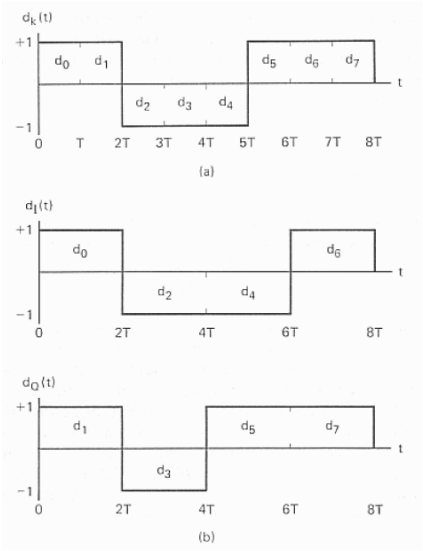


Figura 1 - Sinal original (dK), sinal da portadora I (dI) e sinal da portadora Q (dQ).

Deste modo, é possível duplicar a taxa de transmissão sem alterar a largura de banda, utilizando o esquema apresentado à esquerda na Figura 2. Veja-se nesta figura que cada uma das 4 possíveis fases de portadora representa um conjunto de dois bits, levando a dois bits por símbolo ou fase. Como é representado, o mecanismo QPSK possibilita a transição entre quaisquer estados de codificação.

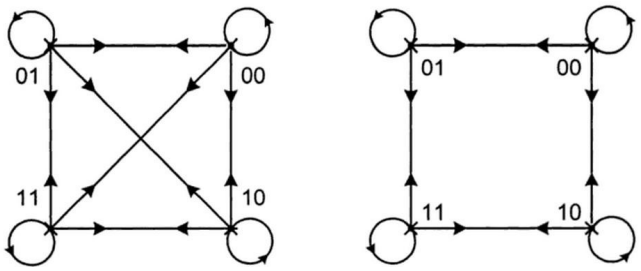


Figura 2 - À esquerda é apresentado o esquema da constelação da modulação QPSK e à direita a da modulação O-QPSK, bem como as possíveis transições nos dois métodos (12).

2.2.3.3. O-QPSK

O mecanismo de modulação O-QPSK (*Offset-Quadrature Phase Shift Keying*) consiste numa variante da técnica QPSK em que é possível codificar 2 bits ao mesmo tempo, com a simples mudança de fase do sinal. Apesar de usar também quatro possíveis fases, codificando dois bits por símbolo, implementa uma restrição nas transições, tal como apresentado à direita na Figura 2. O método de modulação O-QPSK é ainda interessante na sua diferença para o QPSK, na medida em que ao diferirem pela restrição de o primeiro apenas permitir alterações num dos dois bits, é impedido que haja flutuações em amplitude derivadas de variações superiores a 90º (11).

Esta técnica possibilita que tanto na gama dos 915 MHz como na gama dos 2,4 GHz se tenha uma *data rate* de 250 kbps e de 100 kbps na gama dos 868 MHz.

2.3. Arquitecturas de Protocolos para redes sem fios

2.3.1. Topologias de rede

A topologia de uma rede influencia fortemente características que têm sido, ao longo deste texto, apontadas como importantes para uma rede de sensores sem fios, podendo torná-la mais ou menos robusta, com uma maior ou menor autonomia, ou mais ou menos escalável.

São apresentadas as topologias de rede mais básicas, que possibilitam a construção de redes com topologias mais complexas, através da sua associação.

A topologia de estrela, em que todos os elementos da rede têm um único interlocutor, sendo esse o mesmo para todos, é a estrutura de rede mais simples que existe. Diferentes tipos de metodologias podem ser usadas para gerir o acesso ao meio, sendo fácil adoptar mecanismos que impedem a colisão entre mensagens dado que, havendo apenas um interlocutor para todos os dispositivos da rede, estes apenas iniciarão comunicações quando o primeiro estiver desimpedido ou, por outras palavras, o elemento anterior tiver terminado a sua comunicação.

Esta forma de topologia é útil para redes que permitam alta latência ou baixo número de dispositivos integrantes da rede. Isto porque, estando a troca de dados entre dispositivos limitada à disponibilidade de um único, será sempre necessário que este termine uma transacção em curso para iniciar uma nova.

Ao nível das duas camadas mais baixas do modelo ISO/OSI (modelo *Open Systems Interconnection*, arquitectura para transacções entre computadores da *International Organization for Standardization*) – Sessão (camada 2) e Física (camada 1) – é isto que se passa numa rede em estrela, sendo razoavelmente fácil adicionar alguma complexidade à rede acrescentando ao elemento "central" (tal como apresentado na figura abaixo) capacidades de reencaminhamento de mensagens – camada de rede do modelo ISO/OSI –, criando assim a possibilidade de todas os elementos da rede poderem ter vários interlocutores lógicos, se bem que executando as suas comunicações sempre através de um único nó da rede.

Esta solução de rede é também aplicável a redes com uma dispersão espacial relativamente baixa, visto que todos os dispositivos ditos "de campo" ou, no caso das redes de sensores, os sensores sem fios, terem de estar dentro do raio de alcance da unidade central.

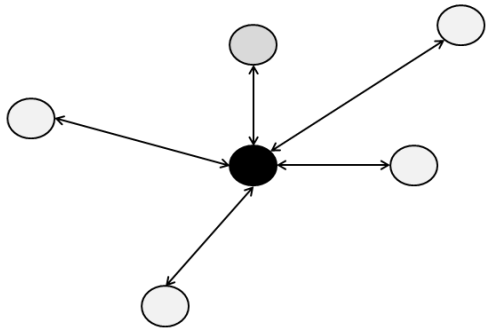


Figura 3 – Imagem representativa de uma rede em estrela, onde as setas correspondem a ligações bidireccionais. Nesta imagem os círculos cinzento claro equivalem a dispositivos de campo (ou, em WSN, sensores) e o círculo a preto ao nó central da rede, que, no caso de existir uma interface com uma rede de outro tipo, também terá essa função.

Os constrangimentos apontados apenas se tornam inconvenientes quando de facto a rede necessita de uma performance superior – por exemplo em termos de latência de dados ou de ocupação espacial. Além dos que foram apontados, existe ainda outro que costuma ser associado às redes em estrela, e que está associado à falha do nó central. É uma afirmação verdadeira a de que, se este nó for desactivado ou entrar em falha, toda a rede falhará também, pois todas as comunicações são suportadas num único ponto. Ainda assim, se estivermos a considerar apenas redes de sensores, e como veremos ao apresentar outras topologias de rede, trata-se de um mal comum entre todas, e que apenas poderá ser ultrapassado através da instalação de um elemento redundante, que entre em actividade aquando da falha do original. Podemos fazer esta afirmação porque numa rede de sensores, salvo raras excepções, em *n*

elementos existem *n-1* elementos produtores de informação e apenas 1 consumidor – o nó central, que é a interface de rede – que, falhando, tornará inútil a tentativa de transmissão de dados de qualquer ponto da rede.

Assim, ao falar de redes sem fios e da robustez da rede associada ao nó central, dever-se-á pensar também em arquivo de dados no transmissor, podendo esses ser eliminados após confirmação da recepção (referente ao termo técnico inglês *acknowledgement*, que significa a resposta de confirmação de recepção de um pacote de dados, consequente à transmissão desse mesmo pacote).

Outro tipo de topologia, em árvore, consiste basicamente na associação de redes em estrela. Se o tipo de rede anterior for considerado de um ponto de vista em que o nó central tem um papel de pai, que possibilita que os "filhos" – os dispositivos de campo – se associem à rede que esta unidade criou, a rede em árvore é equivalente a uma árvore genealógica ou a uma hierarquia (diz-se que a rede está hierarquicamente organizada), que podemos dividir em várias gerações de pais e filhos, de acordo com o número de níveis da rede (o "nível" corresponde ao número máximo de dispositivos de reencaminhamento pelos quais uma mensagem terá de passar entre um produtor e um consumidor (numa WSN, entre o dispositivo de campo e a interface de rede). Com dois níveis, tal como é apresentado na figura abaixo, será possível estender a rede dentro da soma dos alcances dos dois dispositivos a cinzento.

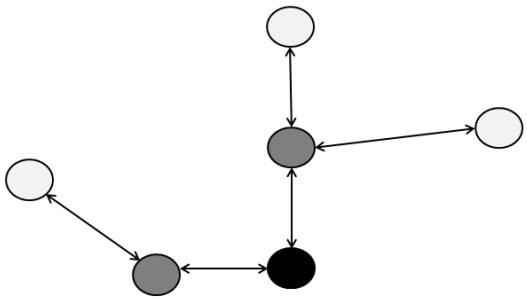


Figura 4 – Imagem representativa de uma rede em árvore. Mais uma vez, os círculos cinzento claro correspondem a dispositivos de campo como sensores ou actuadores, o círculo a preto à interface de rede e, neste caso, e o círculo cinzento escuro a um repetidor ou *Router*, que possibilita adicionar mais um nível à rede.

Em comparação com a topologia anterior, esta acrescenta especialmente a capacidade de mais facilmente expandir a rede, possibilitando ocupar uma maior área, de acordo com o número de níveis que a rede tem.

Para uma rede de dispositivos onde existam diversas ligações lógicas entre esses mesmos dispositivos – tipicamente onde existem simultaneamente aplicações de monitorização e de actuação – esta solução torna-se mais robusta do que a de uma rede em estrela, visto que a falha (por interferência externa, por falta de alimentação, como exemplos) de um dos nós com

funções de *routing* não significa a total falha da rede, podendo ainda manter-se algumas das ligações lógicas entre outros dispositivos. Por outro lado, as ligações em falha poderão ser recuperadas pela comunicação através de um caminho alternativo, visto que vários dispositivos são capacitados de reencaminhamento de mensagens.

Na rede em árvore, as unidades com capacidade de reencaminhamento de mensagens mantêm em memória tabelas com os identificadores das unidades com as quais mantêm comunicação, sendo assim a interface entre os seus "filhos", dispositivos que estão ao seu alcance, e os restantes dispositivos da rede. Através destas tabelas de reencaminhamento é possível que qualquer dispositivo da rede possa endereçar qualquer outro,

A forma mais "completa" de uma topologia de rede consiste na emalhada, que possibilita que sejam criados diferentes caminhos entre um emissor e um destinatário de um pacote de dados. Isto porque, neste tipo de rede, qualquer dispositivo tem a capacidade de reencaminhamento de mensagens, sendo assim possível a existência de vários caminhos alternativos – tantos quanto o número de possíveis interlocutores – tornando a rede mais robusta à falha de um tipo de dispositivo que até agora, nos outros tipos de topologia, havíamos designado de *Router* (alternativamente, podemos designar esse dispositivo de repetidor).

Na rede emalhada, continuam a existir repetidores, mas neste caso qualquer dispositivo é um repetidor, ao mesmo tempo que integra as funções de actuador ou sensor.

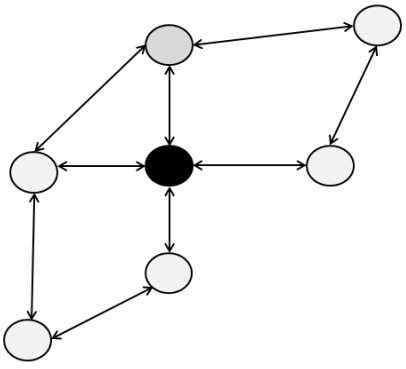


Figura 5 – A imagem pretende representar uma rede emalhada, onde os círculos cinzentos representam novamente dispositivos de campo e o círculo a preto a interface de rede.

2.3.2.Acesso/Privacidade

Esta questão foi já levantada anteriormente, pelo que apenas alguns factores serão aqui adicionados.

De facto, trata-se de uma desvantagem do sem fios em relação a um sistema cablado, o facto de poder ser acessível por um intruso, que se encontre nas imediações da rede local e assim possa

interceptar mensagens, bloquear a rede, ou tomar acções de controlo sobre elementos da rede. É uma preocupação que deve ser respondida, e existem de facto mecanismos que podem ajudar a aumentar fortemente a segurança no acesso a uma rede sem fios.

As principais acções de violação de segurança de uma rede sem fios podem ser enunciadas na seguinte forma:

(i) *Inserção*: este tipo de ataque é feito de forma a introduzir pacotes forjados na rede de comunicações, e assim poder aceder a informação sem autorização. Trata-se de um ataque passivo, já que o atacante apenas tem acesso a informação, sem interferir com as operações da rede;
(ii) O ataque de *máscara* (do inglês *masquerading*) permite ao atacante fazer-se passar por um elemento da rede, o que possibilita, para além das capacidades de um ataque de inserção, apagar pacotes da rede;
(iii) A *violação de autorização* acontece quando um agente externo utiliza serviços da rede sem ter autorização para o fazer, podendo assim entrar em acções de controlo da rede ou dos seus elementos;
(iv) A *perda ou alteração de informação* pode levar a sabotagem dos processos controlados através dos elementos de rede;
(v) O *repúdio* acontece quando uma entidade, que já conseguiu aplicar o ataque de *máscara* fazendo-se passar por outra, passa a tomar de facto o seu lugar, podendo assim deixar de aplicar as suas funções.

Como resposta a estes ataques, é necessário implementar medidas de protecção da rede, pensando essas medidas de forma a serem aplicáveis a redes de sensores sem fios, cujas necessidades e características são diferentes de outras áreas de informática onde a Segurança está mais desenvolvida.

A utilização de algoritmos criptográficos na informação transmitida através da rede deve ser pensada tendo em conta que grande parte dos elementos de rede tem sérias limitações em termos de energia disponível – tipicamente alimentados a bateria –, de capacidade de processamento e de armazenamento de informação.

A melhor forma de abordar este problema é desenhando uma arquitectura de segurança apropriada para o nível de segurança pretendido, que estará associado aos processos nos quais os elementos de rede estão envolvidos, mantendo uma perspectiva realista sobre as suas limitações.

Este assunto será considerado ao longo desta dissertação, tanto aquando da apresentação de diferentes protocolos existentes como na fase de apresentação da Arquitectura do sistema.

2.3.3.Acesso ao Meio

O acesso ao meio é regido através de protocolos que tentam que num determinado momento apenas um dos dispositivos da rede tenha de facto acesso ao meio, impossibilitando assim colisões de mensagens, e libertando as camadas protocolares superiores dessas funções. Estes podem ser divididos entre vários tipos básicos, podendo-se nomear os protocolos baseados em intervalos, definindo espaços no tempo ou em frequência em que apenas um dos dispositivos está habilitado a comunicar; protocolos baseados em sinalização, em que existe um canal alternativo àquele usado para comunicação, apenas para funções de sinalização de transmissão de dados; e protocolos baseados em medição de energia.

Os mecanismos de acesso ao meio são aqui apresentados brevemente, desenvolvendo-se apenas aqueles que são implementados pelos protocolos de comunicação que se expõem de seguida.

2.3.3.1. TDMA

O mecanismo *Time Division Multiple Access* é uma técnica de acesso ao meio que permite a partilha de largura de banda no domínio do tempo. Isso significa que cada banda de frequência é dividida em intervalos temporais, sendo cada um desses intervalos designado de trama TDMA. A cada nó da rede são atribuídas uma ou mais tramas TDMA, sendo que um nó apenas tem permissão para comunicar nos intervalos que lhe foram atribuídos. Apesar de se tratar de uma técnica *half-duplex*, em que apenas um dos interlocutores comunica num determinado instante temporal, e num determinado canal, cada intervalo tem um tempo de duração bastante reduzido.

Deste modo, é necessária uma boa sincronização entre transmissor e receptor, implementando-se um tempo de guarda entre tramas TDMA, no qual não pode haver comunicação entre dispositivos (13).

2.3.3.2. DSSS

O mecanismo *Direct Sequence Spread Spectrum* (DSSS) consiste numa técnica de modulação cujo nível de complexidade é ligeiramente superior ao das técnicas descritas anteriormente, na medida em que existe uma codificação do sinal. O sinal a transmitir é multiplicado por uma sequência de código de ruído pseudo-aleatório designado de código de *chipping*, tendo essa sequência uma frequência superior àquela do sinal original – sendo a dimensão do código de *chipping* também designada de taxa de *chipping* (*chipping rate*).

A comunicação é possível entre emissor e receptor pois o receptor detém a sequência de código de *chipping* definida para aquele emissor, e consegue assim descodificar a mensagem recebida. Caso qualquer outro emissor, com um código de *chipping* diferente, transmita dados naquele canal, a sua mensagem será indecifrável para o receptor, pois o seu código de *chipping* não

permitirá a sua descodificação (11). Esta é a base do *Code Division Multiple Access*, em que cada nó da rede detém o seu código de *chipping*, sendo que todos os códigos são ortogonais entre si, resultando num produto interno nulo, dividindo assim o acesso ao meio através do código de *chipping*.

Tabela 1 - Princípio de funcionamento do método *Direct Sequence Spread Spectrum*.

Código de *chipping*:	00010011100
Dados:	101
	11111111111 00000000000 11111111111
	00010011100 00010011100 00010011100
Sequência transmitida	00010011100 11101100011 00010011100

Este esquema de espalhamento permite uma maior resistência à anteriormente mencionada interferência multi-caminho (*multipath* interference obstrução de canal, bem como uma maior facilidade na partilha de um canal, pois poderão existir várias "conversas" entre diferentes emissores e receptores sem que estes choquem entre si.

2.3.3.3. FHSS

O mecanismo de modulação de *Frequency Hopping Spread Spectrum* (FHSS) segue o mesmo princípio que o de DSSS, na medida em que existe uma codificação do sinal a transmitir que se repercute na sua frequência de transmissão. Como o nome indica, o sinal é transmitido pelos diferentes canais permitidos, sendo a sua sequência de alteração de canal pré-definida e conhecida entre emissor e receptor (11).

Dois diferentes esquemas de FHSS são o *slotted channel hopping* e *slow channel hopping*. O primeiro altera o canal de transmissão a cada *slot*, optimizando a largura de banda e estando assim mais adaptado em casos onde os *Routers* não dispõem de alimentação ilimitada – este método equivale ao FHSS puro. O segundo caso, usado mais frequentemente, faz uma transição mais lenta entre canais, ocupando várias *slots* com o mesmo canal. A Figura 6 apresenta os dois tipos de *Frequency Hopping*.

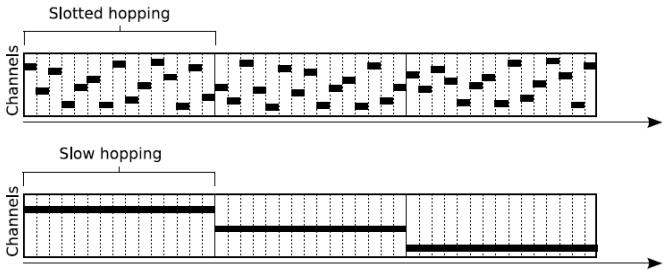


Figura 6 - *Frequency Hopping* por *slotted hopping* e por *slow hopping* (14).

2.3.3.4. CSMA-CA

Este é o mecanismo implementado pela grande parte dos protocolos a discutir, o CSMA-CA (*Carrier Sense Multiple Access with Collision Avoidance*). Trata-se de uma técnica para redes sem fios que – neste caso – apesar de ter esta designação, não tem de facto mecanismos que tentem evitar as colisões entre mensagens, como é feito por exemplo no *Wifi*, onde um dispositivo que pretenda aceder ao meio deverá primeiro ter o seu controlo, através de mensagens RTS (*Request To Send*) e CTS (*Clear To Send*). Ainda assim, existem de facto medidas para um devido acesso ao meio, principalmente através de *Carrier Sense*, que poderá ser chamado em português de "sentir a portadora", uma medida de actividade na rede (15).

O acesso ao meio é assim feito na seguinte forma:

1. Um dispositivo que tenha uma mensagem para transmitir activa o seu rádio no modo receptor, durante um período de tempo pré-determinado;
2. Caso o nível medido de intensidade de sinal (definido normalmente através do RSSI – *Radio Signal Strength Indicator*) esteja abaixo do limite definido como seguro – ou indicativo da falta de actividade rádio na rede –, a transmissão é feita imediatamente;
3. Caso o nível seja superior, o dispositivo "assume" que está a decorrer outra comunicação – ou que o canal está "ocupado" –, e aguarda durante um período de tempo designado como "tempo de recuo" (do inglês *back-off delay*), que é calculado com recurso a um algoritmo que baseado num valor pseudo-aleatório. Após este período de tempo, o dispositivo regressa ao ponto 1, existindo um número limite de novas tentativas.

A geração de um valor pseudo-aleatório para o tempo de recuo em caso de detecção de canal ocupado permite que, mesmo que estejam vários dispositivos a tentar aceder ao canal ao mesmo tempo e, como tal, "recuem" no mesmo instante, a geração de dois valores distintos permita que tentem aceder novamente em momentos diferentes, e consequentemente acedam ao meio sem colisão.

É ainda importante considerar os mecanismos de acesso ao meio que são compostos pela agregação de diferentes métodos – que se poderão designar de básicos –, como por exemplo a combinação de TDMA com CSMA-CA, que será bastante útil em aplicações onde exista um grande número de dispositivos a operar na mesma área. Assim, poder-se-á atribuir a mesma *slot* TDMA a vários dispositivos, sendo que estes disputam o acesso a essa mesma *slot* com base em CSMA-CA.

2.3.4.Normas Concorrentes de Protocolos para Redes de Sensores sem Fios (WSN)

Após esta revisão de matérias de base para comunicações para redes de sensores sem fios, importa compreender e discutir de que forma se partirá para a sua implementação, tendo em conta um dos importantes critérios definidos à partida, a normalização. A normalização é um mecanismo interessante em qualquer área, tomando importância na das redes de sensores sem fios no sentido em que possibilita que todos os interessados num dado produto, desde os seus fabricantes aos seus instaladores ou integradores de sistemas, que conseguem um reconhecimento maior do seu produto e – no caso das pequenas empresas – uma compatibilidade com outros fabricantes, bem como os clientes finais, que poderão utilizar produtos de diferentes marcas, sem terem de ficar obrigados a manter uma marca ou alterar todo o sistema, aquando da necessidade de alterações ou incrementos.

Parecendo um contra-senso, a referência no título desta secção a normas, quando a ideia base da existência de uma norma é que seja única, para que possa ser a mesma a ser usada por todos, reflecte a divergência que tem existido na área (de um ponto de vista genérico, englobando as diferentes aplicações existentes) das redes de sensores sem fios, que pelo facto de ser recente tem tido múltiplas propostas de protocolos de comunicação, que têm encontrado mercado em diferentes tipos de aplicações.

É interessante, antes da apresentação de características técnicas ou mesmo das áreas de aplicação a que cada diferente protocolo se direcciona, tentar perceber o modo de aparecimento destas normas e do funcionamento deste mercado.

Existe, à partida, um elemento regulador que tem influenciado as definições de protocolos: a ITU, que define a forma de uso do espectro electromagnético, tanto em frequência como na potência utilizada, e que é seguida pela legislação da maioria dos países.

Seguidamente, existe outro elemento regulador que, não sendo totalmente abrangente – focou-se apenas numa das gamas de frequência dentro das definidas pela ITU –, definiu as duas camadas protocolares mais baixas segundo o modelo ISO/OSI, normalização que foi seguida por grande parte das normas desenvolvidas a partir dessa: o IEEE, com a norma *IEEE 802.15.4*. É verdade que esta norma se enquadra dentro de um espectro mais alargado de normas/grupos de trabalho, as *IEEE 802*, mas apenas esta é direccionada para redes de área pessoal (PAN – *Personal Area Network*) sem fios e de baixo consumo. Existem outras normas para redes sem fios, como a 802.11, referente ao *Wifi*, e mesmo dentro do grupo *802.15* existe, por exemplo, a norma *Bluetooth* (802.15.1), mas esta também não é destinada a soluções de baixa potência (e portanto baixo consumo).

Para tornar este assunto um pouco mais explícito, é importante referir que dentro do IEEE – *Institute of Electrical and Electronics Engineers* uma associação profissional internacional com finalidades como a normalização, organização de conferências de especialidades tecnológicas ou publicações – existem diferentes grupos de trabalho, dedicados à normalização em áreas como a das redes de comunicações, como é o caso dos grupos dentro do Comité Normalizador *IEEE 802* (16), sendo o *IEEE 802.15.4* o grupo de trabalho (o *Task Group 4 – TG4*) que se foca nas redes PAN sem fios de baixa potência, e que deu origem à norma com a mesma referência.

A partir da criação da *IEEE 802.15.4,* que definiu 27 diferentes canais, na gama de frequência dos 868 MHz (apenas para a Europa, com 1 canal), dos 915 MHz (apenas para os EUA, com 30 canais) e dos 2.4 GHz (mundial, com 16 canais) (17), surgiu uma série de diferentes protocolos de comunicação, como o *6LoWPAN*, o *ZigBee*, o *WirelessHART* ou o *ISA100.11a*, utilizando como base estas duas camadas protocolares.

Assim, apesar de assentes na mesma base, todos os protocolos de comunicação que foram consequentemente desenvolvidos e comercializados são incompatíveis (à parte da compatibilidade entre *WirelessHART* e *ISA100.11a*, que será discutida mais tarde), tentando ganhar margem em diferentes tipos de mercado. O facto de se tratar de uma área tecnológica ainda recente proporcionou que ainda se mantenha uma grande dispersão de protocolos existentes, e que haja bastantes áreas aplicacionais que não têm ainda um protocolo especializado, com características adaptadas ao seu ambiente.

A promoção dos diferentes protocolos tem sido feita através de grupos de trabalho de fundações, alianças ou grupos de interesse, constituídos por vários fabricantes de circuitos integrados, sistemas de instrumentação e controlo, e empresas de *software*, e em grande parte dos casos as mesmas empresas apostam e financiam diferentes protocolos, tentando influenciar e aumentar a probabilidade de aposta num concorrente vencedor.

Para além dos protocolos desenvolvidos sobre a *IEEE 802.15.4*, existem outros desenvolvidos sobre outras gamas de frequência, nomeadamente a dos 433 MHz, e protocolos desenvolvidos para as mesmas frequências utilizadas pela norma do IEEE, mas sem qualquer recurso a esta. Dada a vantagem competitiva dos protocolos desenvolvidos sobre *802.15.4*, suportados pelos principais fabricantes mundiais de circuitos integrados – que passaram a produzir *chips* preparados para comunicar de acordo com a norma, a sua capacidade de desenvolvimento e disseminação por diferentes mercados tem sido muito maior, estando os restantes protocolos – designados proprietários, por serem suportados por apenas um fabricante – relegados a áreas aplicacionais muito específicas, como é o caso do protocolo *ANT*(18), muito comum em aplicações associadas ao desporto (relógios, cintos medidores de pulsação, velocidade e distância percorrida por um corredor, entre outros exemplos). Para além deste caso, existe ainda

um protocolo desenvolvido para a gama dos 433 MHz que se mantém como um potencial candidato ao mercado da instrumentação e de soluções móveis (principalmente sistemas de localização) – o *DASH7* (19) –, que será apresentado na sua própria secção, mais adiante.

Apesar da dispersão existente, nenhum protocolo consegue ainda provar que é o melhor concorrente independentemente da área de aplicação, pois todas as decisões tomadas na sua especificação estão associadas ao ambiente para o qual se destina. Com grande probabilidade, o que se passará no futuro – existindo já algumas indicações nesse sentido – é que diferentes protocolos ganharão o mercado em diferentes aplicações, não existindo um protocolo global destinado às comunicações sem fios de baixa potência.

Assim, o posicionamento de cada protocolo no mercado tem sido no sentido de, por um lado, promover o desenvolvimento de soluções através de associados para um único mercado ou para um número reduzido deles, ou de componentes pré-programados com o protocolo, que outras empresas – não associadas – possam implementar nos seus próprios produtos.

Casos existem em que tecnologias que ganharam uma abrangência de nível mundial foram lançadas por apenas uma empresa, ou um número reduzido delas, mas acontece com mais frequência que a tecnologia ganhe momento através de diferentes tipos de partes interessadas, que se distinguem entre si tanto na cadeia de distribuição dessa mesma tecnologia como na sua dimensão.

Sendo a normalização um fim a alcançar, será antes necessário que existam condições para que esta seja atingível pelos diferentes intervenientes, principalmente os diferentes tipos de fabricante – desenvolvimento de *Software*, fabrico de circuitos integrados, fabrico de módulos *System-on-chip* (SoC), fabricantes de sistemas ou soluções integradas e mesmo instaladores. Muitos destes são empresas de base tecnológica com poucos anos de vida, provenientes de Universidades ou Polos tecnológicos e que não têm a capacidade financeira para entrar numa associação de empresas de muito maior dimensão, pagando taxas de entrada, quotas de permanência e posterior certificação de produtos, para validação de conformidade com a norma de protocolo.

Com todas estas condicionantes em conta, é possível alcançar a seguinte tese: o mercado associado ao desenvolvimento de componentes e ferramentas para redes de sensores sem fios está ainda em desenvolvimento, não estando criadas as condições para a normalização por área de sistemas sem fios. Para que aconteça um estabelecimento das normas por mercado, é imperativo que o próprio mercado (ao nível do consumidor final) tome um dado protocolo como requisito para as suas instalações, condição que apenas poderá acontecer com o decorrer de

alguns anos, sendo consequente da maior disseminação e da afirmação como solução válida das diferentes normas.

Tabela 2 – Comparação entre os diferentes protocolos apresentados neste capítulo, em termos de camadas especificadas na norma, áreas aplicacionais às quais se direccionam, e entidades promotoras.

	DASH7	***ISA100.11a***	***WirelessHART***	***ZigBee***	***6LoWPAN***
Camada PHY	RFID activo (*ISO 18000-7*)	Baseado em *IEEE 802.15.4*	Baseado em *IEEE 802.15.4*	Baseado em *IEEE 802.15.4*	Baseado em *IEEE 802.15.4*
Camada MAC	Especificada	Baseado em *IEEE 802.15.4*	Baseado em *IEEE 802.15.4*	Baseado em *IEEE 802.15.4*	Baseado em *IEEE 802.15.4*
Camada NWK	Especificada	Especificada	Especificada	Especificada	Especificada
Camada TRANS	Especificada	Especificada	Especificada	-	Especificada
Camada APP	Especificada	Especificada	Especificada	Especificada	*TCP/IP*
Área Aplicacional	Sistemas de Localização e Instrumentação Industrial	Automação Industrial	Automação Industrial	Automação de Edifícios, *Smart Grid*, …	Genérico
Desenvolvedor e Promotor	*DASH7 Alliance*	ISA International Society of Automation	HART Foundation	*ZigBee* Alliance	IETF – Internet Engineering Task Force
Frequências de Operação	433,92 MHz	2,4 GHz	2,4 GHz	868 MHz (EU) 915 MHz (EUA/AUS) 2,4 GHz (WO)	868 MHz (EU) 915 MHz (EUA/AUS) 2,4 GHz (WO)

Nas subsecções seguintes serão apresentados os protocolos que têm tido mais sucesso no mercado ou que – não o tendo ainda – apresentam as características mais interessantes, seja na área da instrumentação industrial ou noutras áreas, e será dado foco não só aos pontos mais importantes, relacionados com as suas características técnicas, mas também com o acesso existente a esse mesmo protocolo para uma empresa ou laboratório interessado no seu desenvolvimento e introdução em produtos, visto ser esse mesmo o âmbito do trabalho de desenvolvimento feito ao longo deste Doutoramento.

Serão apresentadas as normas que se encontram mais bem posicionadas no mercado das redes de sensores sem fios, à excepção do já citado protocolo ANT, proprietário e com uma área aplicacional demasiado específica.

Faz-se a ressalva para o problema de, ao reunir informação técnica sobre alguns dos protocolos que ainda se encontram em desenvolvimento, estes estarem ainda mal documentados nas próprias publicações das organizações que os desenvolvem – bem como em publicações científicas de terceiros ou documentos de fabricantes –, tendo-se procurado que este facto não condicionasse a comparação entre protocolos abaixo apresentada.

2.3.4.1. IEEE 802.15.4

Tal como foi atrás indicado, a norma *IEEE 802.15.4* (20) define as duas camadas protocolares mais baixas segundo o modelo ISO/OSI (ver Figura 7), para a criação de redes PAN sem fios de baixa potência. Este protocolo desenvolveu-se a partir do grupo de trabalho do *IEEE 802.15.4*, que se enquadra dentro do grupo 802.15 (21), dedicado a redes PAN sem fios, que por sua vez se enquadra dentro do Comité de Normalização IEEE 802, dedicado a redes de área local (LAN) e de área metropolitana (MAN) (16).

O protocolo *IEEE 802.15.4* foi aprovado em Maio de 2003 e publicado em Outubro do mesmo ano. Com o lançamento do protocolo, o grupo de desenvolvimento foi posto em modo de "hibernação" – sem reuniões regulares ou trabalho – e actualmente existem dois subgrupos em funcionamento, para a continuidade do desenvolvimento da norma: o *802.15.4*a e o *802.15.4*b, sendo que o primeiro se dedica à criação de uma camada PHY alternativa, que proporcione melhores características para localização, baixo consumo e maior alcance (centenas de metros), e o segundo a resolução de falhas ainda existentes na última versão de protocolo. Esta última versão foi lançada em 2007, sendo referida como a *IEEE 802.15.4-2007* (20).

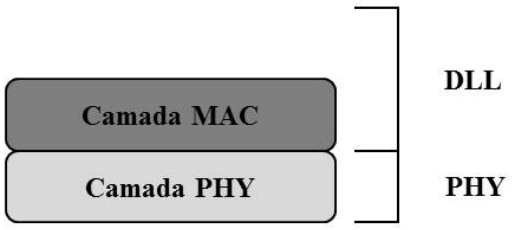


Figura 7 - Camadas definidas na norma *IEEE 802.15.4*, segundo o modelo ISO/OSI. Dentro da camada DLL (Data Link *Layer*) A norma especifica apenas a sub-camada MAC (*Medium* Access Control).

2.3.4.1.1. Elementos de Rede

A norma estabelece um tipo de rede hierarquizada, consagrando dois tipos de dispositivos para as suas redes:

- *Full-Function Devices* (FFD), designados desta forma por serem capacitados de todas as funções disponíveis no protocolo, que incluem gestão e manutenção de rede, e que foram desenhados para estarem permanentemente ligados – portanto alimentado pela tensão de rede.
- *Reduced-Function Devices* (RFD) que, ao contrário do tipo de dispositivos anterior, não têm quaisquer funções de gestão de rede, estando assim definidos para que o seu consumo seja bastante inferior, e consequentemente serem alimentados, por exemplo, com recurso a bateria.

Dentro dos FFD, existe um tipo de dispositivo, único para cada rede e designado de *Coordenador* (*PAN Coordinator*), que executa a sua inicialização, ou seja, que gera os valores determinantes para a sua criação, como o do identificador de rede, e que possibilita que a próxima unidade integre a rede – que seja criada uma ligação lógica entre elas. O outro tipo de dispositivo, designado de *Router*, não tem a capacidade de formação de rede mas, quando integrado numa, permite a associação de outros dispositivos, permitindo o aumento da cobertura espacial da rede, e a criação de topologias de rede mais complexas que a Estrela.

Veja-se que a maior vantagem deste tipo de protocolo de rede é de facto a existência de RFD, que possibilitam a criação de sistemas baseados em sensores e/ou actuadores alimentados a bateria. Com os outros elementos de rede, é então possível criar uma infraestrutura de rede, para transmissão de dados, mas apenas os RFD possibilitam a designada "muito baixa potência".

Assim, estes tipos de dispositivo constituem os blocos construtores de topologias de rede mais complexas, através das funções que lhes são atribuídas, sendo os dispositivos menos capacitados, os RFD, peças que funcionam como unidades terminais.

2.3.4.1.2. Camada Física (PHY)

Tal como foi já indicado, a especificação da camada PHY do protocolo *IEEE 802.15.4* requer que as comunicações sejam efectuadas dentro de 27 canais definidos, nas seguintes frequências: 868-868.8 MHz (1 canal, apenas para a Europa), 902-928 MHz (30 canais, apenas para os EUA), e 2400-2483.5 MHz (16 canais espaçados de 5 MHz entre si, âmbito mundial) (22). A taxa de transmissão nos diferentes canais é tabelada nos 250 kbps.

Existem vários esquemas de modulação definidos pelo protocolo, mas os mais utilizados são derivados do *Direct-Sequence Spread Spectrum* (DSSS), utilizando *Offset-Quadrature Phase Shift Keying* (O-QPSK).

2.3.4.1.3. Camada de Enlace (*Data Link Layer* – DLL)

A norma *IEEE 802.15.4* define apenas a sub-camada MAC, tal como é apresentado na Figura 7.

O acesso ao meio é *efectuado* através do mecanismo CSMA-CA ou um esquema semelhante ao TDMA, que se inicia com a transmissão de uma mensagem designada de *beacon*. Trata-se um tipo de mensagem trocada entre dispositivos onde o Coordenador de rede transmite periodicamente para todos os elementos da rede (*broadcast*) informação sobre a existência de dados pendentes (no próprio Coordenador) para os restantes dispositivos, tendo ainda a função de sincronização entre todos. Esta forma de operação divide cada período de transmissão em 16 intervalos (*slots*), sendo o primeiro dedicado ao *beacon* do Coordenador, e os restantes passíveis de reserva pelos outros dispositivos para as suas próprias transmissões. Dentro destes intervalos, os dispositivos não Coordenadores continuam a aceder à rede pelo método CSMA/CA. No entanto, um modo de operação com estas características é principalmente usado para aplicações de muito baixa latência (podemos defini-la como o atraso de um evento no sistema, na área das WSN normalmente ligado ao armazenamento da informação no dispositivo RFD), visto que a sincronização periódica de dispositivos aumenta o consumo de todo o sistema, afectando principalmente dispositivos com alimentação finita, sendo assim normalmente preterido pelo método mais simples, também designado de *unslotted* (em oposição ao método *slotted* – que poderemos designar de "intervalado") ou *sem beacon* (15) (23).

O formato do pacote *802.15.4* – considerando apenas a camada DLL – está dividido entre o *MAC Header* (MHR - cabeçalho), o *MAC payload* (para comandos e camadas superiores) e o *MAC Footer* (MFR – "rodapé" da camada), tal como é apresentado na Figura 8. O campo MHR inclui os identificadores já mencionados dentro de *Addressing fields*, com 2B para controlo de pacote e 1B para um número de sequência. Todo o campo MAC permite até 127 B, estando 102 B disponíveis para o MAC *payload*.

O *MAC Footer* (MFR, na figura seguinte) contém a *Frame Check Sequence*, que implementa um CRC (*Check Redundancy Code*) de 16 bits para verificação da integridade da mensagem.

Uma funcionalidade importante da camada de Enlace do protocolo *IEEE 802.15.4* é o *acknowledgment* de MAC (MAC ACK), que possibilita reconhecimento de recepção ponto a ponto, na comunicação entre cada dois dispositivos.

<table>
<tr><td>Octets: 2</td><td>1</td><td>0/2</td><td>0/2/8</td><td>0/2</td><td>0/2/8</td><td>variable</td><td>2</td></tr>
<tr><td rowspan="2">Frame control</td><td rowspan="2">Sequence number</td><td>Destination PAN identifier</td><td>Destination address</td><td>Source PAN identifier</td><td>Source address</td><td rowspan="2">Frame payload</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">Addressing fields</td></tr>
<tr><td colspan="6">MHR</td><td>MAC payload</td><td>MFR</td></tr>
</table>

Figura 8 - Formato de pacote *802.15.4* - Camada DLL/MAC (23).

2.3.4.1.4. Topologias consagradas

A norma consagra dois tipos de topologia:

- Estrela, o tipo de rede mais simples, onde todos os dispositivos – RFD ou FFD – trocam dados apenas através do *Coordenador* da rede (caso a aplicação da unidade A queira transmitir uma mensagem para a aplicação da unidade B, deverá enviá-la para C, o Coordenador de rede, que a reencaminhará) – ver Figura 3.
- *Peer-to-peer*, onde todos os dispositivos podem comunicar directamente com os dispositivos dentro do seu raio de alcance. A Figura 9 apresenta uma rede peer-to-peer.

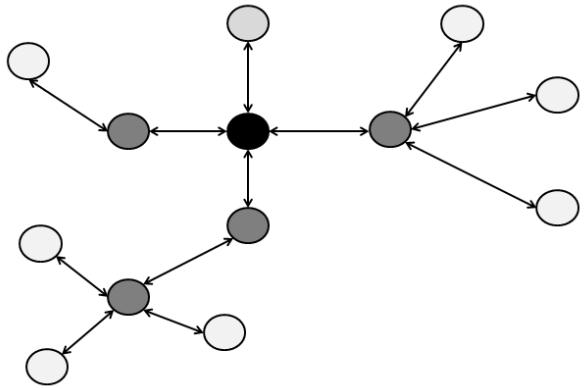


Figura 9 - Representação de uma rede *Peer-to-peer* – na sua versão mais específica de *cluster tree* –, onde o círculo vermelho representa um *Coordenador*, os círculos cinzento-escuro *Routers* e os círculos cinzento-claro RFDs.

A rede *Peer-to-peer* permite uma maior flexibilidade no que toca à topologia da rede, sendo possível que os dispositivos FFD/*Routers* formem ligações entre si, sem necessidade de recurso a um FFD/*Coordenador*, após a formação da rede e desde que se encontrem dentro do alcance de comunicação de um dispositivo FFD já pertencente à rede. Os dispositivos RFD podem agora estabelecer ligações com qualquer outro FFD, com o constrangimento de que apenas podem efectuar a ligação a um único dispositivo.

2.3.4.1.5. Desenvolvimento de Produto

Para além das principais características técnicas definidas por uma norma, é importante ter em conta outros factores, como a existência no mercado de dispositivos adaptados à norma, o seu preço, a sua disponibilidade, a existência de ferramentas de desenvolvimento, e o próprio acesso a implementações de código-fonte do protocolo.

Não sendo estes factores que determinam se as características de um protocolo são superiores ou inferiores em relação a outro, são totalmente determinantes na escolha de um protocolo de

comunicação, principalmente quando essa escolha levará à colocação de um produto no mercado.

Para a norma *IEEE 802.15.4*, pela notoriedade que esta tem e pelo esforço que foi feito pelos principais fabricantes assim que foi lançada em 2003, existem dezenas de dispositivos no mercado, variando entre os seguintes, organizados por ordem crescente de complexidade (e, normalmente, preço):

- Unidades rádio (não programáveis) para associar a um microcontrolador com o protocolo;
- Módulos SoC (*System on Chip*, neste caso um conjunto de microcontrolador e unidade rádio empacotadas numa só) com interface série, configurável através de comandos por outro microcontrolador, programado com o protocolo;
- SoC programáveis conforme a norma e com código-fonte disponível para adaptar a solução (mantendo a conformidade).

Por tudo o que já foi dito, é fácil chegar à conclusão que esta norma é uma base segura na qual se poderá trabalhar, sem grande risco associado, tendo em conta que é usada em todo o mundo e reconhecida em qualquer mercado no qual as WSN já entraram. O que fará a diferença são as camadas protocolares que serão colocadas acima das definidas pela *IEEE 802.15.4*, e que portanto constituirão outras normas por si só ou, para mercados específicos e exigentes como o da Instrumentação Industrial, a vantagem de um concorrente que não segue esta norma mas com características mais adaptadas a esse ambiente, como o caso de protocolos que recorram a frequências de comunicação mais baixas. São essas normas que são apresentadas nas seguintes secções.

2.3.4.2. ZigBee

O protocolo *ZigBee* é o mais conhecido protocolo dentro da área das redes de sensores sem fios, não só por ter sido o primeiro a ser lançado, de entre os protocolos com camadas de alto nível definidas, mas também pelo esforço comercial que foi feito pelos membros da *ZigBee Alliance*.

O protocolo *ZigBee* é mantido e promovido por este grupo de interesse, cujos membros são empresas de topo da área dos Semicondutores, Electrónica Industrial ou Redes de Sensores sem Fios, como são casos a *Emerson Process Management*, a *Texas Instruments*, a *Schneider Electric* ou a *Freescale*, entre outros. Apesar de o protocolo ser publicitado como desenvolvido para mais de 10 aplicações diferentes (24), as aplicações nas quais o protocolo já vingou de facto em relação aos seus concorrentes são a da Domótica e da monitorização de consumos, também conhecida como *Smart Grid*.

O que significa que o protocolo está adaptado a um ou outro tipo de aplicações são as suas características tanto ao nível da camada de aplicação – que tipicamente são mais publicitadas –, onde normalmente existem perfis adaptados às diferentes situações, como é o caso do perfil de Domótica (mais concretamente *Home Automation*) do protocolo *ZigBee* (25), que inclui dispositivos como interruptores, controlo de lâmpadas ou sensores de iluminação (questão descrita em maior pormenor na subsecção Camada de Aplicação (APL), mas também características de mais baixo nível, que o tornam mais adaptado às especificidades do meio ambiente ou dos utilizadores aos quais se destina.

O protocolo *ZigBee* foi desenhado por cima da norma *IEEE 802.15.4*, desde a versão 2003, definindo camadas de Rede (NWK) e Aplicação (APL), tal como é apresentado na Figura 10 (26).

Na camada de rede, e com recurso aos tipos de dispositivo definidos pela norma *IEEE 802.15.4*, o protocolo *ZigBee* define uma rede híbrida com possibilidade de criação de uma rede emalhada (entre FFD/*Routers*), e dentro da camada de aplicação são definidas várias sub-camadas para comunicação entre dispositivos. São estas camadas protocolares que serão descritas nas subsecções seguintes.

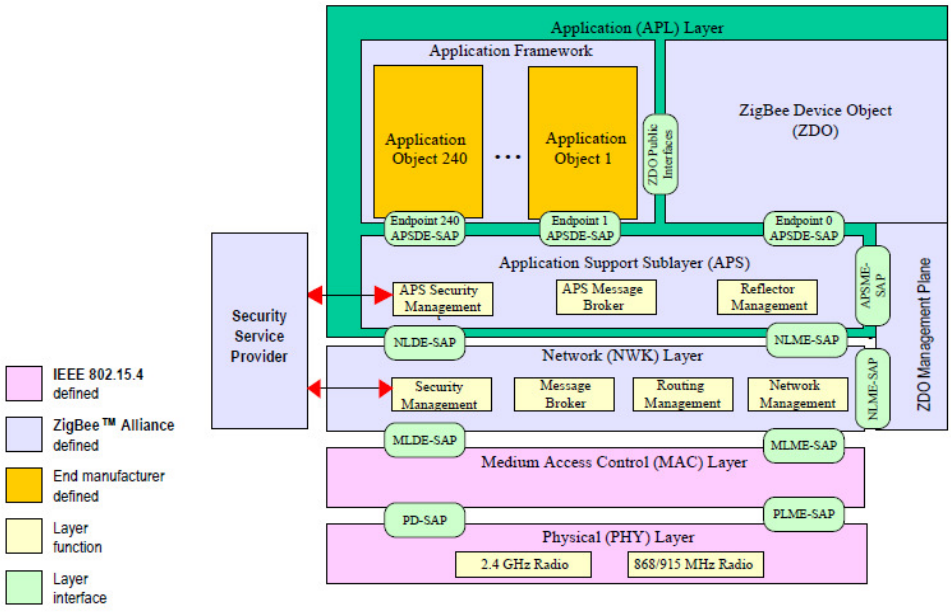


Figura 10 - Arquitectura em camadas segundo o modelo ISO/OSI do protocolo *ZigBee* (26).

2.3.4.2.1. ZigBee e ZigBee PRO

Estes são os nomes comuns dados às versões de protocolo referentes ao lançamento de 2006 (*ZigBee*) e ao último lançamento, de 2007 (*ZigBee PRO*).

Trata-se portanto de uma designação comercial, se bem que as melhorias trazidas pela versão de 2007 são importantes ao nível da alocação de memória, eficiência das comunicações, robustez em relação à resposta a ruído e segurança – razões que levaram ao desenvolvimento desta versão, mais compatível com o ambiente industrial.

A descrição do protocolo feita nas sub-secções seguintes será feita com base na última versão, a *ZigBee PRO*, e portanto omitir-se-á a enumeração das diferenças entre os dois protocolos, visto que a aplicação de interesse é a Indústria, onde as condições ambientais são mais agressivas e portanto um protocolo com características que conferem maior robustez e segurança como o *ZigBee PRO* é mais útil.

2.3.4.2.2. Elementos de Rede

O protocolo *ZigBee* define tipos de dispositivo para além dos definidos na norma *802.15.4*, se bem que mantendo o mesmo conceito:

- Coordenador de Rede (C): é um FFD e trata-se do mesmo tipo de dispositivo com a mesma designação na norma *IEEE 802.15.4*, com as funções de inicialização e formação da rede, associação de dispositivos e segurança de rede;
- *Router* (R): é um FFD e mantém algumas das principais características do Coordenador: capacidade de gestão de rede e associação de dispositivos, mas sem capacidade de formação de rede;
- *End Device* (ED): trata-se do elemento anteriormente (ver *IEEE 802.15.4*) designado como RFD, que agora ganha capacidades ao nível da camada de aplicação, se bem que se mantém sem capacidades de gestão de rede (camada NWK).

2.3.4.2.3. Camada PHY

Mantém a camada física da norma *IEEE 802.15.4*, para todas as frequências definidas.

2.3.4.2.4. Camada DLL

Mantém a camada de acesso ao meio da norma *IEEE 802.15.4*.

2.3.4.2.5. Camada de Rede (NWK)

O protocolo *ZigBee* contempla diferentes tipos de topologias, adicionando funcionalidades sobre a norma *IEEE 802.15.4* que, para além das topologias já consagradas por esta, ainda possibilitam a criação de uma rede emalhada dentro da topologia geral. Apesar deste conceito poder parecer confuso, a representação esquemática que se segue ajuda a perceber que se trata de uma rede emalhada entre *Routers*, mantendo-se as restrições que os dispositivos RFD da norma *802.15.4* a ligar-se apenas a um FFD.

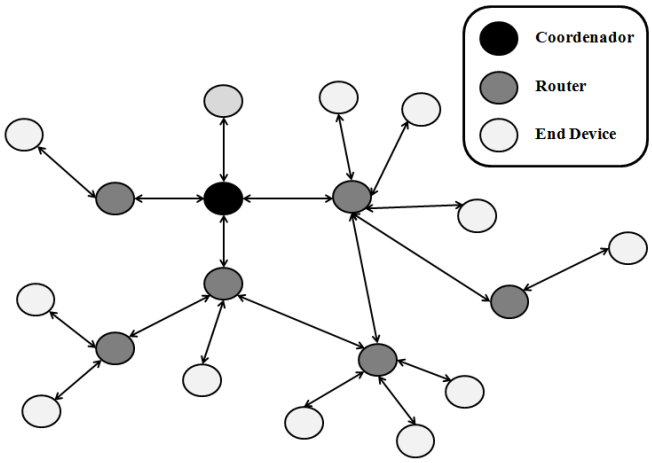


Figura 11 - Representação de uma rede *ZigBee* híbrida, com a formação de uma rede emalhada entre *Routers* e Coordenador, e ligações do tipo Estrela para os ED.

Esta camada suporta serviços como procura e manutenção de rota, reencaminhamento de múltiplos passos (designado em inglês de *multi-hop routing*), segurança e acesso ou saída de uma rede.

Foi referido que a camada de Rede do protocolo *ZigBee* suporta dois tipos de topologia baseados na *Peer-to-peer* da norma *IEEE 802.15.4*, a *cluster tree* (ver Figura 9) e a emalhada (ver Figura 11). Para além das especificidades associadas ao *routing* de mensagens, estas diferem a partir da camada MAC, sendo que a primeira usa o método de acesso com *beacon* e a segunda sem *beacon*, através do simples CSMA-CA, já descrito na secção anterior. Nessa mesma ocasião, as vantagens e desvantagens da escolha de um ou do outro método foram debatidas ao nível da camada MAC, mas uma vez que neste caso a escolha também abrange a camada NWK, a decisão toma uma relevância ainda maior. Esta relevância torna-se visível se se tiver em conta que – principalmente em ambiente industrial – é uma vantagem a possibilidade de formação de redes emalhadas, que capacitam a estrutura da rede de maior robustez em relação ao ubíquo ruído electromagnético.

Considerando então que a topologia de rede escolhida é a emalhada e ignorando de ora em diante a *cluster tree*, o processo de *Routing* no protocolo *ZigBee* é feito através da escolha do caminho (de *Routers*, pois apenas estes têm essa aptidão) mais próximo entre os nós emissor e receptor, sendo a descoberta desse caminho mais curto – ou de menor custo – mantido pelo serviço existente na camada NWK designado de procura de rota (*Route Discovery*). A camada de NWK do protocolo *ZigBee* implementa ainda um mecanismo de *Frequency Agility*, que consiste na detecção de interferência elevada no canal (após a implementação da rede, e com base na contagem de falhas na comunicação) por parte dos dispositivos *Router* e consequente notificação do Coordenador que, com base nas notificações de *Routers* ou na intenção do

utilizador de alterar a rede, envia para os dispositivos da rede o comando de alteração de canal (27).

2.3.4.2.6. Camada de Aplicação (APL)

Na camada de Aplicação são definidos os perfis de aplicação, mais concretamente na sub-camada *Application Framework*, existindo um perfil diferente para cada tipo de aplicação, e também a forma como os dispositivos definidos dentro de cada um desses perfis interagem, através da sub-camada *ZigBee Device Objects* (ZDO). A outra sub-camada existente, a *Application Sub-Layer* (APS), executa serviços para transferência de dados com as camadas inferiores, disponibilizando-os às outras duas sub-camadas (ver Figura 10).

Dentro da *Application Framework* estão definidos os *Application Objects* (APO), existindo um para cada tipo de dispositivo definido nos perfis *ZigBee*, até um limite de 239 por perfil. Cada APO designa-se também de *Endpoint* e consiste numa entidade lógica que controla elementos físicos, como lâmpadas ou estores, ou que mede ou detecta alterações no meio, como sensores de luz ou interruptores. A camada ZDO consiste num APO com características especiais, que têm como principal finalidade a ligação entre APOs, através dos processos de descoberta de rota (RD), para além de serviços ao nível da comunicação, ligação à rede e segurança. A diferença entre a sub-camada APS e a ZDO encontra-se no tipo de interface que é feita com as outras sub-camadas: a sub-camada ZDO serve directamente os APO, estando a camada APS responsável pelos serviços de comunicação e rede para *Routers*, que suportam uma tabela onde é feita a associação entre os identificadores de rede correspondentes aos APO endereçados (serve comunicações entre dispositivos com *bind*, o tipo de ligação lógica de camada de aplicação, entre si).

A *ZigBee Alliance* tem, neste momento, os seguintes perfis disponíveis no seu *website*, cobrindo diferentes áreas de aplicação, e dentro de duas especificações base diferentes (26):

- *ZigBee*
    - *Building* Automation (Eficiência em Espaços comerciais)
    - Smart *Energy* (Poupança Energética Doméstica)
    - *Health Care* (Monitorização de Pacientes e Desporto)
    - *Home Automation* (Domótica)
    - *Telecom Services* (Troca de dados para dispositivos móveis – semelhante a *Bluetooth* para publicidade)
    - *Retail Services* (Monitorização e controlo associados à venda de bens)
- *ZigBee* RF4CE
    - *Remote Control* (Controlos Remotos)

- *Input Device* (Periféricos de Computadores)
- *3D Sync* (transmissão de Vídeo 3D sem fios)

Para o tema de interesse, apenas se tem considerado a norma *ZigBee*, visto que a norma *ZigBee* RF4CE serve especificidades diferentes, como a distância bastante inferior entre nós, bem como o seu número reduzido, que afectaram as suas opções de desenho logo a partir da camada de rede. Tratando-se de uma área completamente diferente, foi omitida.

2.3.4.2.7. Segurança

Quanto à Segurança do protocolo, e considerando esta área nas suas diversas facetas: Confidencialidade, Integridade e Acesso, a sua apresentação pode ser feita na seguinte forma:

- Confidencialidade: o protocolo *ZigBee* usa encriptação AES de 128 bits, estando disponível ao nível da camada de rede, para dispositivos com a mesma chave de rede e ao nível do dispositivo, usando chaves de ligação entre pares de dispositivos. Esta função não é obrigatória, sendo possível activar ou desactivar a encriptação.
- Integridade: o protocolo assume como *default* um mecanismo de verificação de integridade de dados de 64 bits, podendo este ser seleccionável entre 0, 32, 64 ou 128 bits.
- Acesso: o protocolo inclui uma chave de rede de 16 bits, definida pelo Coordenador e comum a todos os dispositivos. Existe ainda, usando a mesma filosofia apresentada no ponto de Confidencialidade, uma chave de ligação entre pares de dispositivos.

Por outro lado, a encriptação de um dado pacote não é da responsabilidade da camada que o gerou, não sendo exclusiva de uma só camada, como é representado na Figura 10.

2.3.4.2.8. Desenvolvimento de Produto

O que foi escrito para a norma *IEEE 802.15.4* pode ser repetido também para o protocolo *ZigBee*. Um esforço grande de publicidade e comercialização deste protocolo tem sido feito pela *ZigBee* Alliance e pelos fabricantes que a integram, existindo módulos pré-programados com perfis do protocolo *ZigBee*, como é o caso do controlador de rede *ZigBee* CC2530 (*ZigBee PRO*) (28), da Texas Instruments, ou o módulo *XBee* (*ZigBee PRO*) da *Digi International* (29), que permitem uma fácil integração em produtos novos, e também de microcontroladores com unidade rádio associada e código-fonte disponibilizado pelo fabricante para a fácil conformidade com o protocolo.

Na verdade, os módulos referidos constituem diferentes estágios de desenvolvimento de produto, tratando- se o módulo XBee de um componente pronto a usar para interface com um microcontrolador de aplicação – sendo constituído pelo *chipset* EM357 do fabricante Ember

(30) –, como um *Router* ou outro associado a um sensor de temperatura, e o módulo CC2530 de um SoC, ao qual é necessário ainda associar componentes passivos para conformação de um *balun* e filtro para comunicações sem fios, cristais para acerto dos temporizadores internos, e regulação de tensão. Sendo estas últimas questões importantes, e também o mínimo ponto de partida para que seja possível o desenvolvimento de produtos com base num protocolo normalizado a existência de *hardware* conforme, a grande diferença está no acesso ao protocolo, e isso é algo que a *ZigBee* Alliance tem possibilitado de uma forma prática – para si e para os possíveis interessados – na medida em que este é disponibilizado através de peças completas de código-fonte, adaptadas ao *hardware* dos seus membros fabricantes.

Por outro lado, estes componentes são de fácil aquisição, estando disponíveis na maior parte dos países, incluindo Portugal, tanto em quantidades de prototipagem como para produção, sendo portanto, deste ponto de vista, uma boa escolha para desenvolvimento de produtos.

2.3.4.3. 6LoWPAN

O protocolo *6LoWPAN* – uma abreviatura de *IPv6 over Low power Wireless Personal Networks* – é um dos mais interessantes protocolos para redes de sensores sem fios, principalmente porque se trata de uma adaptação da rede mais bem sucedida de sempre, a Internet, ao domínio dos pequenos dispositivos, com a finalidade de que qualquer objecto possa estar ligado à Internet. É portanto desenhado para aproveitar todos os protocolos desenvolvidos no âmbito da Internet e, assim, tratar-se da verdadeira implementação da *Internet of Things*, criada pela *IETF – Internet Engineering Task Force* – a comunidade internacional de peritos da área das redes de comunicações, aberta à colaboração de membros individuais e que desenvolve os protocolos usados para a Internet. Tal como acontece nos grupos de normalização do IEEE, está dividida em grupos de trabalho, sendo *6LoWPAN* o nome comum do grupo de trabalho dedicado à implementação do protocolo IPv6 a PAN sem fios de baixa potência.

Este protocolo está altamente virado para soluções móveis, sendo a sua arquitectura pensada de forma a ligar "ilhas" de dispositivos (embebidos), sendo cada uma destas ilhas uma rede *stub* – um extremo da rede, que não executa funções de reencaminhamento de mensagens, apenas recebe ou transmite mensagens para a rede, daí a expressão associada a extremo (da Internet), também designada de LoWPAN. Uma LoWPAN (ver Figura 12) é uma rede de sensores sem fios com um prefixo IPv6 (os primeiros 64 bits dos 128 bits de identificador) em comum, podendo ser definidos três tipos de redes: a *Simple LoWPAN*, onde existe apenas uma interface de rede (ou *Edge Router*) ligada a outra rede IP (ligação que poderá, por exemplo, tomar a forma de *GPRS*), a *Extended LoWPAN*, que dispõe de vários *Edge Routers* ligados entre si

através de um *backbone* (como a *Ethernet*) e a *Ad-hoc LoWPAN*, que não tem qualquer *Edge Router*, e portanto qualquer ligação ao exterior.

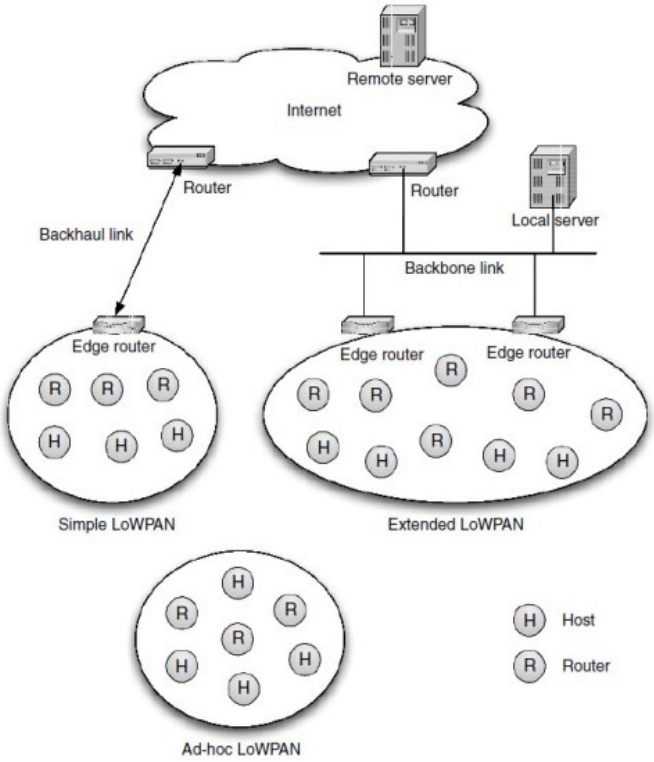


Figura 12 - Arquitectura de rede *6LoWPAN*, onde são apresentados os três diferentes tipos de rede: *Simple LoWPAN*, *Extended LoWPAN* e *Ad-hoc LoWPAN* (31).

O protocolo é estabelecido sobre as duas camadas definidas pela *IEEE 802.15.4*, tendo uma camada chamada "de Adaptação" abaixo da camada de rede (que na Figura 12 foi omitida, encontrando-se dentro da camada NWK), e que tem funções de *routing* e fragmentação e assemblagem de pacotes IPv6.

<table>
<tr><th colspan="3">Protocolo TCP/IP</th><th></th><th colspan="2">Protocolo 6LoWPAN</th></tr>
<tr><td colspan="2">HTTP</td><td>RTP (…)</td><td>APL</td><td colspan="2">Aplicação</td></tr>
<tr><td>TCP</td><td>UDP</td><td>ICMP</td><td>TRANS</td><td>UDP</td><td>ICMP</td></tr>
<tr><td colspan="3">IP</td><td>NWK</td><td colspan="2">IPv6 com LoWPAN</td></tr>
<tr><td colspan="3" rowspan="2">MAC Ethernet</td><td rowspan="2">DLL</td><td colspan="2">Adaptação LoWPAN</td></tr>
<tr><td colspan="2">MAC IEEE 802.15.4</td></tr>
<tr><td colspan="3">PHY Ethernet</td><td>PHY</td><td colspan="2">PHY IEEE 802.15.4</td></tr>
</table>

Figura 13 – Camadas do protocolo *6LoWPAN*, comparado com *TCP/IP*.

2.3.4.3.1. Elementos de rede

Tal como é apresentado na Figura 12, existem diferentes tipos de dispositivo numa LoWPAN, havendo a figura do *Edge Router*, que poderá estar presente em maior ou menor número, de acordo com o tipo de rede, e que consiste na interface de rede, que possibilita a comunicação com o exterior, tendo também funções de inicialização e gestão de rede. A rede é depois composta por *Routers*, que executam funções de gestão de rede e encaminhamento de mensagens e *Hosts*, onde estão alojadas as aplicações de interesse, sejam elas sensores, actuadores, dispositivos de localização, ou aplicações tradicionais *Web*.

2.3.4.3.2. Camada PHY

Consiste na camada PHY do protocolo *IEEE 802.15.4*, usando todas as frequências definidas.

2.3.4.3.3. Camada DLL

Esta camada é baseada na camada MAC do protocolo *802.15.4* – com preferência pelo modo sem *beacon* – mas, tal como foi dito acima, é ainda definida uma camada de interface designada de "adaptação", que permite a fragmentação e assemblagem de pacotes com mais de 127 B, o limite máximo sobre *802.15.4*, e também suporta uma das duas formas de *routing* suportadas pelo protocolo, ao nível da Camada de Enlace e da camada de rede (32).

Esta camada é fundamental para o protocolo *6LoWPAN*, visto que foi necessário preparar um esquema que possibilitasse a transmissão de pacotes IPv6, com uma MTU (*Maximum Transfer Unit*) mínima de 1280 B, sobre o máximo de 102 B permitidos pelo *MAC payload* do protocolo *802.15.4*.

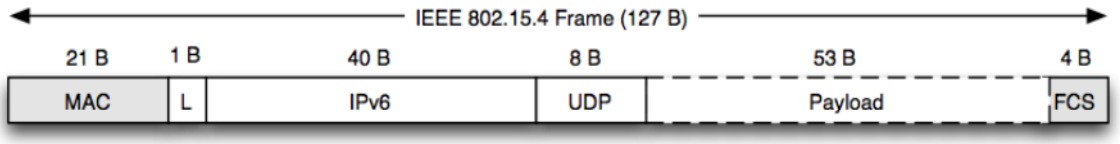


Figura 14 - Endereçamento de 64 bits, cabeçalho UDP/IPv6 completo (31).

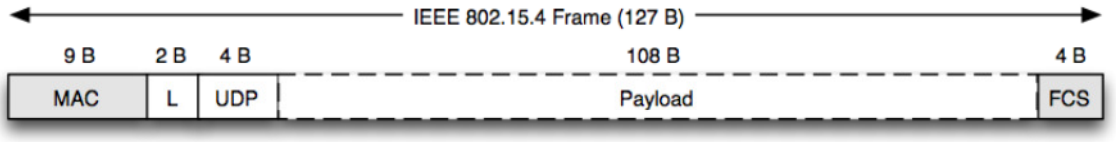


Figura 15 - Endereçamento de 16 bits, cabeçalho UDP/*6LoWPAN* mínimo (31).

A camada de adaptação suporta ainda a fragmentação de pacotes IPv6, através da sua divisão em diferentes pacotes *802.15.4*, incluindo campos dedicados ao tamanho total do *Datagram* (o pacote IPv6 original, indicado como *Datagram Size*) e o identificador único desse pacote, *Datagram Tag*.

Adicionalmente, para endereçamento no interior da PAN, esta camada inclui capacidade de *routing* em rede emalhada – designada de *mesh under* –, com as seguintes características:

(i) Apenas permite reencaminhamento intra-PAN, visto que usa os endereços de 16 ou 64 bits. Isto possibilita que as mensagens sejam reencaminhadas com maior rapidez, mas também não vai ao encontro da especificação do protocolo, que pretende garantir maior eficácia nas LoWPAN ao tornar cada *Router* LoWPAN equivalente a um *Router* comum, onde existe sempre reconstituição de pacotes (que são transmitidos nas LoWPAN em fragmentos);
(ii) O *mesh under* é um mecanismo de *routing* que utiliza ou o endereço de 64bits do protocolo *802.15.4* ou o cabeçalho *6LoWPAN* (cujo endereço provém da mesma fonte). Através do cabeçalho *6LoWPAN* é possível enviar todos os fragmentos pelos diferentes nós muito rapidamente sem ter de reconstituir o pacote.

Decorrendo do primeiro constrangimento, tem existido uma preferência já notada no trabalho dos desenvolvedores de soluções baseadas no protocolo, como é o caso do Sistema Operativo Contiki (33), que se verificou mais recentemente na norma do protocolo (34), dando preferência ao *routing* da camada NWK (*route over*).

2.3.4.3.4. Camada NWK

A camada de rede do protocolo *6LoWPAN* é uma adaptação do protocolo IPv6 a dispositivos com baixa memória e redes de baixo consumo, sendo aplicadas, tal como na camada anterior, medidas de compressão de cabeçalhos, de maneira a compatibilizar tecnologias. Apesar de o endereço IPv6 ser constituído por 128 bits, o quádruplo do endereço IPv4, é utilizado o facto de o prefixo do endereço (os primeiros 64 bits) ser comum a todos os nós de uma LoWPAN para que este seja omitido em comunicações intra-PAN. Assim, uma das funções do Edge *Router* é também a gestão do prefixo de LoWPAN.

$$172.16.254.1 \rightarrow Endereço\ IPv4$$
$$2001{:}0DB8{:}AC10{:}FE01{:}0000{:}0000{:}0000{:}0000 \rightarrow Endereço\ IPv6$$

Figura 16 - Endereços IPv4 e IPv6.

O protocolo define um método para comunicação em rede emalhada, se bem que esta ainda se encontra fora do último documento validado pelo grupo de trabalho (35). O método será baseado numa adaptação do algoritmo *Neighbor Discovery* (ND) do protocolo IPv6, com características próprias para baixo consumo.

No já mencionado (tópico anterior) sistema *Route Over* é utilizado o *routing* IP, onde cada nó *Router* actua como um *Router* IP comum, o que obriga a que seja feita a reconstituição do

pacote em cada nó. Por um lado a reconstituição de pacotes causa uma maior necessidade de processamento, mas por outro garante uma maior eficácia em redes dinâmicas. Cada mensagem inclui o endereço de origem e de destino, pelo que as decisões de endereçamento são feitas através da consulta de uma tabela de *routing*, seleccionando-se o próximo dispositivo a receber a mensagem.

Um protocolo de *routing* IP é adaptável às alterações da rede, enquanto o *mesh under* não tem essa capacidade. O protocolo é designado de RPL – *Routing over Lossy and Low-Power Networks* – e distingue os dispositivos entre DODAG *Routers* (DODAG significa *Destination Oriented Directed acyclic graph*), que não são mais que o nó central da rede, os *parents* que são nós com capacidade de *routing* (FFD) e os *children* que são RFD (ou *leaf nodes*), sem capacidade de *routing*. Normalmente, num protocolo de *routing*, sempre que existem alterações na rede, o protocolo automaticamente estabelece novas rotas, consoante essas alterações. No ponto de vista do RPL, esta prática causaria um grande desgaste dos nós, visto que as designadas *Low power and Lossy networks* são por norma dinâmicas e iriam obrigar a constantes actualizações. Deste modo, o RPL ignora as alterações na constituição da rede, e só estabelece uma rota quando tem uma mensagem para enviar, dizendo-se que funciona *on-demand*.

Actualmente, a última versão encontra-se em validação (34), e se aceite irá substituir a actual, implementando finalmente os mecanismos que permitirão ND, endereçamento intra-PAN e detecção de endereços duplicados. O desenvolvimento futuro do protocolo terá de passar ainda por algumas funções importantes, como suporte de *cache* para dispositivos adormecidos (34).

2.3.4.3.5. Camada de Transporte (TRANS)

Ao nível da camada de transporte, o protocolo contém as sub-camadas *User Datagram Protocol* (UDP) e *Internet Control Messaging* Protocol (ICMP), suportando assim serviços de:

- UDP
    - Transmissão de mensagens – ou datagramas – compatível com o *Internet Protocol Suite*, disponível para as aplicações a introduzir em camadas superiores.
- ICMP
    - Controlo de troca de mensagens, com mensagens de erro do tipo de serviço indisponível ou destinatário indisponível.

Esta é outra das principais forças do protocolo *6LoWPAN*, para além de estar a ser desenvolvido pelo IETF, o facto de ser baseado no protocolo mais bem-sucedido de sempre, e daí se tornar a sua extensão "natural" para a *Internet of Things*.

2.3.4.3.6. Camada APL

A implementação dos dois protocolos de camada de transporte abre a porta para que as aplicações existentes tanto nos nós *6LoWPAN* como nos serviços remotos com os quais estas interagem façam as suas comunicações segundo a Socket API, uma aproximação bastante usada para troca de dados.

Tal como foi mencionado anteriormente, um dos principais objectivos deste protocolo é a utilização de protocolos já existentes, e esse princípio é também aplicado ao nível da camada de aplicação, sejam esses protocolos provenientes do *Internet Protocol Suite* ou de outros protocolos de WSN, como é o caso do *ISA100.11a* para Automação Industrial ou o *ZigBee* para Domótica ou Smart Grid.

2.3.4.3.7. Segurança

Quanto a medidas implementadas para garantir os três requisitos associados à segurança informática, o protocolo suporta as seguintes medidas, por camada:

- MAC – implementação das medidas consagradas no protocolo *IEEE 802.15.4*;
- NWK – implementa mecanismos já existentes no protocolo IP, mais propriamente:
    - Cabeçalho de autenticação (AH), para integridade e autenticação, definido na RFC4302;
    - *Encapsulating Security Payload* (ESP), para encriptação de dados, através do método AES/CCM.

2.3.4.3.8. Desenvolvimento de produto

O protocolo *6LoWPAN* tem apresentado uma boa participação por parte de fabricantes de *chipsets* e desenvolvedores de código-máquina, existindo actualmente (2011) várias soluções possíveis para integrar capacidades de comunicações sem fios baseadas no protocolo em sensores inteligentes. São exemplos disso o JenNet-IP, da NXP/Jennic (36) ou o recente CC-*6LoWPAN*, com chipset da Texas Instruments – o CC430F5137, nos 868/915 MHz – e *software* da *Sensinode*, o sistema operativo *Nanostack 2.0,* que já suporta todas as funcionalidades definidas na actual versão do protocolo, possibilitando uma Simple LoWPAN com rede emalhada. Existem também plataformas de desenvolvimento interessantes, nomeadamente o telosB ou o micaZ, que são suportados pelo sistema operativo ContikiOS-2.5, que inclui o RPL.

Estes módulos programáveis com código fonte disponível constituem formas de rapidamente introduzir o protocolo sobre sensores inteligentes, e criar soluções compatíveis com o *6LoWPAN*, com preços de mercado competitivos, e disponíveis em quantidades para

prototipagem e produção. Não é portanto um constrangimento a disponibilidade de componentes compatíveis com este protocolo.

2.3.4.4. ISA100.11a

O protocolo *ISA100.11a* é desenvolvido no seio da *International Society of Automation* (ISA), no seu Comité ISA100, dedicado a Sistemas Sem fios para Automação sendo que, dos diversos grupos de trabalho existentes, o *ISA100.11a* é dedicado a dispositivos de baixo consumo.

O projecto ISA100, no qual esta norma está inserida, foi iniciado pela ISA no sentido de criar uma gama extensa de redes de controlo para Automação, desde o sistema de controlo ao dispositivo de campo, incluindo, naturalmente, a rede de campo (*Fieldbus*), e a versão mais recente da norma está aprovada desde Setembro de 2009. A ideia principal por trás do projecto, associada às redes de sensores e actuadores, é a de definir camadas protocolares de baixo nível bem adaptadas ao ambiente industrial, ao mesmo tempo que são criados perfis de dispositivos para aplicações típicas, ao nível da camada de aplicação, suportadas sobre a camada de transporte.

Esta primeira versão do protocolo (*ISA100.11a*-2009) é altamente virada para aplicações de automação industrial, sendo a prova disso o facto de ser desenhada principalmente para aplicações que apenas toleram actualizações de dados até 100 ms, claramente apontando a aplicações de controlo (37).

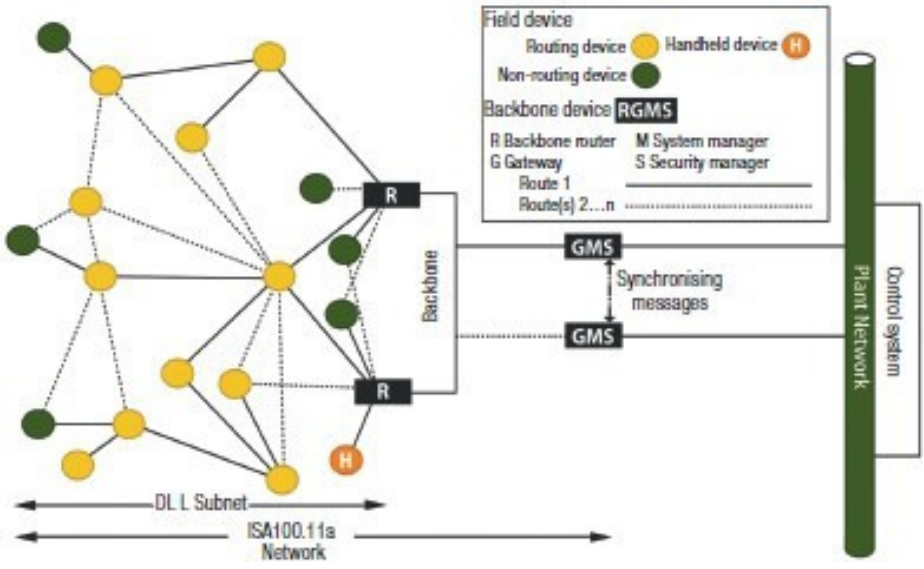


Figura 17 - Representação de uma rede *ISA100.11a*, explicitando os diferentes tipos de dispositivos (38).

O protocolo define níveis de criticidade das mensagens que são enviadas pelos diferentes dispositivos, de acordo com os dados que geram ou com as acções que executam. Na Figura 18

são apresentados os cinco níveis definidos, bem como o grau de criticidade que lhes está associado. As classes com índices mais baixos estão associadas a acções de controlo, as principais visadas por esta norma, mas que também inclui graus de criticidade mais reduzida, associados a aplicações onde as tecnologias sem fios são mais comuns, seja em aplicações de alerta ou de CbM (*Monitoring*).

Safety	0	Emergency action	Always critical	Safety interlock Emergency shutdown Automatic fire control
Control	1	Closed loop Regulatory control	Often critical	Control of primary actuators High frequency cascades
	2	Closed loop Supervisory control	Usually non-critical	Low frequency cascade loops Multivariable controls Optimizers
	3	Open loop control	Human in the loop	Manual flare Remote opening of security gate Manual pump/valve adjustment
Monitoring	4	Alerting	Short-term consequences	Event-based maintenance Battery low indicator Asset tracking
	5	Logging Downloading/ uploading	No immediate consequences	History collection Preventative maintenance rounds Sequence of events (SOE) reporting

Figura 18 - Classes de criticidade de mensagens *ISA100.11a* (39).

Uma breve nota ao protocolo que serve de base ao *ISA100.11a* e ao protocolo que será apresentado logo de seguida, o *WirelessHART*. Este consiste no protocolo TSMP – *Time Synchronized Mesh Protocol* – desenvolvido pela Dust Networks. O TSMP pode ser considerado um subprotocolo multicamada, integrando as funcionalidades de camada de Enlace que são colocadas sobre a camada MAC do protocolo *IEEE 802.15.4* (como se explicará, nomeadamente o protocolo *Time Slotted Channel Hopping*), de camada de Rede e de camada de Transporte.

TSMP Stack	Standard Wireless Stack	OSI Stack
Application	Application	Application
Presentation	Presentation	Presentation
Session	Session	Session
TSMP	**Network**	**Transport**
		Network
	Media Access	**Data Link**
Physical	Physical	Physical

Figura 19 - Equivalência entre o protocolo TSMP e o modelo ISO/OSI (40).

No TSMP, o acesso ao meio é *efectuado* através de TDMA, sendo as *slots* temporais atribuídas aos dispositivos para acesso ao meio. Aquando da alocação de *slots* temporais aos diferentes dispositivos, é também indicada uma prioridade de dados a transmitir (mencionada atrás), acção executada pelo Gestor de rede. Para além deste mecanismo, o protocolo TSMP implementa um esquema de *frequency hopping* (FHSS). A implementação de TDMA bem como FHSS possibilita uma multiplicação de oportunidades de acesso à rede para cada dispositivo, uma vez que não só um determinado dispositivo terá uma *slot* na qual poderá aceder sem interferência de

outros, como ainda utilizará uma sequência de canais distinta dos restantes. Esta multiplicação de oportunidades de acesso é representada na figura seguinte (40).

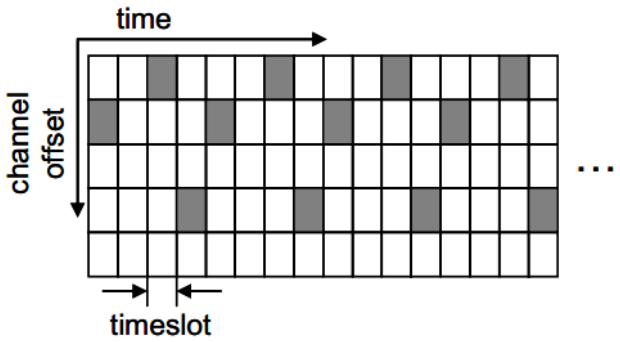


Figura 20 - representação dos esquemas de TDMA e FHSS do protocolo TSMP (40).

Existe ainda mais um método introduzido para criar imunidade a ruído ou a canais sobreutilizados, a detecção dessa mesma condição num canal e a sua consequente eliminação da lista de canais válidos (designado de *Frequency Agility*) (40).

2.3.4.4.1. Elementos de rede

Tal como é apresentado na Figura 17, o protocolo consagra diferentes tipos de elementos de rede:

- *Gateway*, que permite a interface entre a rede sem fios e o *backbone* da infrastrutura de rede, normalmente baseado num protocolo *Fieldbus*. Este elemento inclui também as seguintes funções, que poderão estar todas concentradas no mesmo dispositivo ou distribuídas por vários:
  - Gestão de Rede
  - Gestão de Segurança
- *Backbone Router*, um dispositivo com uma interface sem fios, de rede *ISA100.11a*, e uma interface de rede de campo, sobre a qual pode encapsular dados de outras redes de campo. Pode também permitir também a extensão da rede, ao criar uma maior área de cobertura.
- Dispositivo de Campo com *Routing*, que poderá ou não comportar sensores ou actuadores, mas que, em todas as situações, fará *routing* de dados a percorrer a rede (indicado como *Routing Device*, na Figura 17);
- Dispositivo de Campo sem *Routing*, que suportará sensores ou actuadores, e normalmente será alimentado a baterias, sem funções de *routing* (*Non-routing Device*, na Figura 17);
- Dispositivo portátil, com funções de instalação, configuração ou manutenção dos restantes dispositivos de campo (*Handheld Device*).

2.3.4.4.2. Camada PHY

Este protocolo é também baseado na norma *IEEE 802.15.4*, com a restrição de apenas suportar frequências na gama dos 2.4 GHz.

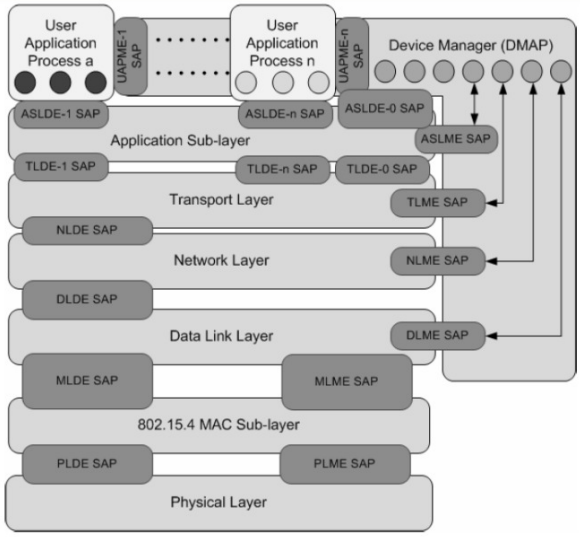


Figura 21 - Modelo em camadas do protocolo *ISA100.11a* (41).

2.3.4.4.3. Camada DLL

A Camada de Enlace divide-se entre duas sub-camadas – tal como é apresentado na Figura 21, sendo a inferior a camada MAC do protocolo *802.15.4*, e a superior, definida como "DLL superior" (*Upper DLL*) que é responsável pela gestão do esquema de TDMA (*Time Division Multiple Access*), com as seguintes características:

- Implementa o método de acesso à rede TDMA: onde os nós se encontram sincronizados e comunicam em *slots* ou intervalos temporais específicos a cada um, permitindo redução da interferência e características de baixo consumo;
- Permite *Frequency Hopping*: a transmissão de dados em canais diferentes em caso de detecção de ruído electromagnético elevado no canal de operação;
- *Mesh Routing*: implementa, logo na camada DLL, um mecanismo de encaminhamento de mensagens em rede emalhada.

Para além destas funcionalidades, o protocolo ainda usa um método de *Channel Blacklisting* detectando canais ruidosos para posterior exclusão da lista de canais utilizados.

O dispositivo nomeado anteriormente como *Gateway* define qual dos métodos é utilizado, e também faz a atribuição de caminhos e ligações entre os diferentes dispositivos de campo, sendo que cada ligação pode ser associada a uma ou mais *slots* temporais.

A Camada de Enlace deste protocolo suporta *routing* em duas formas diferentes (42):

- Grafo: em que todos os caminhos são determinados pelo Gestor de Rede, e descarregados para cada dispositivo de campo. Quando uma mensagem é enviada, é colocado um cabeçalho com o identificador do grafo, que corresponde a um destinatário específico;
- Fonte: que funciona como o *routing* de grafo onde, ao invés de existir um cabeçalho com o identificador do grafo, todos os identificadores dos dispositivos intermediários são colocados.

2.3.4.4.4. Camada NWK

A camada de rede encarrega-se da manutenção da qualidade de serviço (QoS), bem como de esquemas de mais alto nível de *routing*. Tal como havia sido mencionado atrás, esta camada foi desenhada com base na camada IP do protocolo *6LoWPAN*, sendo os seus cabeçalhos compatíveis. Desta forma, a camada de rede deste protocolo permite, tal como a do protocolo *6LoWPAN*, a fragmentação e reassemblagem de mensagens de maior dimensão.

O *routing* efectuado por esta camada difere do implementado na camada anterior na medida em que permite que dispositivos com constrangimentos de alimentação tenham funções de reencaminhamento de mensagens, e portanto que existam dispositivos de campo com *routing* alimentados a bateria.

Uma outra funcionalidade interessante que distingue este protocolo dos restantes e que opera no sentido da poupança nos dispositivos com constrangimentos energéticos é a de *backbone routing*, onde os vários *backbone Routers* instalados na infrastrutura cablada do protocolo comunicam entre si possibilitando ligação entre sub-redes como se da mesma se tratasse, do ponto de vista do dispositivo. Veja-se que esta funcionalidade não é definida no protocolo *ISA100.11a*, mas sim noutra norma do grupo ISA100 permitirão *routing* entre secções diferentes da rede, que responderão a diferentes *backbone Routers*) (37). Esta função é apresentada na Figura 17.

2.3.4.4.5. Camada TRANS

A camada de transporte do *ISA100.11a* encarrega-se de comunicações baseadas em *acknowledgement* entre emissor e destinatário final (i.e., *end-to-end acknowledgement*), bem como comunicações sem esta função, dependendo do nível requerido de fiabilidade do serviço. Por outro lado, consagra também funções relacionadas com segurança – encriptação de dados – também na mesma forma em que a comunicação é interpretada, sendo cada mensagem desencriptada apenas no seu destino (*end-to-end*) (37).

2.3.4.4.6. Camada APL

A camada de aplicação inclui um protocolo de *tunneling* (apenas nas *Gateway*s), que permite que outros protocolos – visando principalmente protocolos Fieldbus, como Profibus, Modbus, HART ou Fieldbus Foundation – sejam transportados sobre *ISA100.11a*. Este é um conceito interessante introduzido por esta norma, que assim lhe permite maior compatibilidade com os protocolos de redes de campo já instalados no terreno (37).

2.3.4.4.7. Segurança

Tal como outros protocolos, o *ISA100.11a* implementa medidas no sentido de impedir a violação de mensagens, através de encriptação, manter a integridade e autenticidade dos dados transmitidos ao longo da rede e impedir ataques externos contra o bom funcionamento da rede.

A segurança é implementada em duas camadas e com dois paradigmas, ponto a ponto na cada de Enlace e entre emissor e destinatário final na camada de Transporte (37). Na camada de Enlace, cada *Router* desencripta a mensagem que recebe, autentica o seu emissor e encripta-a novamente. Na camada de Transporte, o dispositivo emissor autentica e encripta a mensagem a transmitir, sendo que apenas o destinatário final a desencriptará, verificando a autenticidade do emissor.

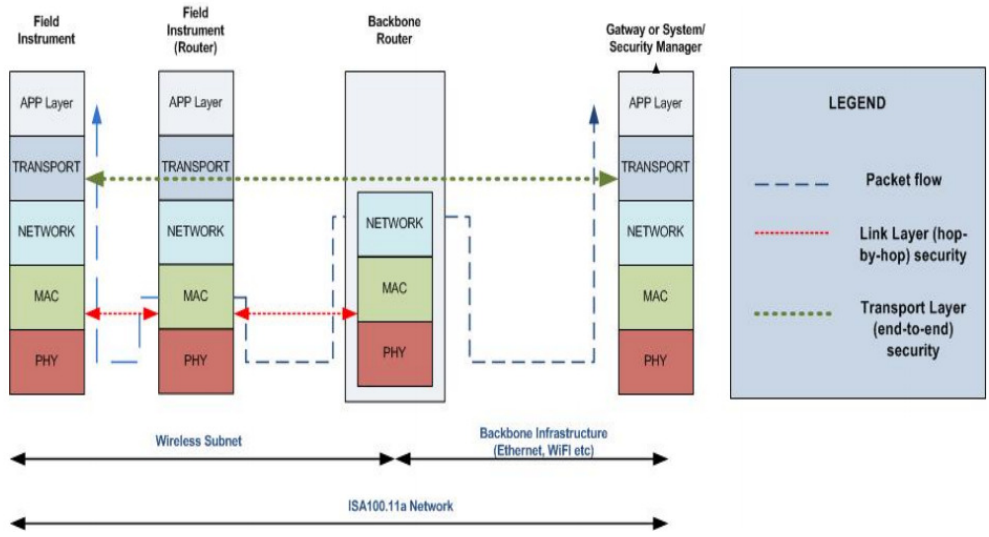


Figura 22 - Esquemas de verificação de Segurança do protocolo *ISA100.11a*. (37)

No que toca à encriptação propriamente dita, o protocolo implementa a encriptação AES de 128 bits na norma *IEEE 802.15.4*, sendo todas as chaves geradas e mantidas pelo Gestor de Segurança. Adicionalmente, pode ainda ser implementada uma verificação da data e hora de criação da mensagem, com consequente verificação por parte do destinatário final, ao nível da camada de Transporte. Uma vez que o protocolo *ISA100.11a* é baseado em tempo de resposta a um dado evento, se o destinatário final detectar que a mensagem foi criada há mais de n

segundos do que o seu limite máximo (sendo este valor configurável), poderá descartá-la, oferecendo assim protecção contra ataques de repetição de mensagem (*replay atack*) (37).

2.3.4.4.8. Desenvolvimento de Produto

Tendo em conta que este protocolo ainda está em desenvolvimento, bem como a existência de um outro protocolo desenhado para Automação, o aparecimento de módulos ou código fonte desenhados para o protocolo *ISA100.11a* tem demorado a acontecer, existindo apenas um único fabricante, a Nivis, uma empresa americana.

Apesar da existência de vários fabricantes que publicitam sistemas de monitorização ou automação com comunicações sobre este protocolo, todos são membros das empresas que suportaram o seu desenvolvimento, e portanto não é possível dizer que existe uma difusão no mercado de soluções para desenvolvimento sobre *ISA100.11a* – Honeywell, Yokogawa ou Nivis (43).

Mesmo optando pelos dispositivos da Nivis, que obteve em 2010 a certificação dos seus produtos pelo *ISA100 Wireless Compliance Institute*, estes têm um preço ainda muito acima do praticado por fabricantes de módulos de outros protocolos no mercado, cerca de cinco vezes mais, bem como a necessidade de importação dos EUA.

Adicionalmente, não existe qualquer *firmware* passível de ser introduzido em outros módulos de comunicações, ou outras peças configuráveis e compatíveis com o protocolo *ISA100.11a*.

Tudo isto indica no sentido de que, apesar de se tratar de um protocolo extremamente interessante, pela base que tem ao ser desenvolvido no seio da ISA e pelas funcionalidades extra que traz para o meio industrial e que o diferenciam dos restantes protocolos, o *ISA100.11a* necessita ainda de tempo para amadurecimento – relacionado com a sua entrada no mercado. A alternativa, que passaria pela implementação do protocolo com base na norma e a sua consequente certificação junto do ISA100 WCI acarretaria um custo incomportável para uma PME. Veja-se que um kit de desenvolvimento para uma universidade, apenas para testes e com poucos dispositivos para uma instalação, tem um custo cerca de vinte vezes superior a um kit de qualquer outro fabricante que suporta o protocolo *ZigBee* (dados de 2011, em comunicação directa com o fornecedor Nivis).

2.3.4.5. *WirelessHART*

O protocolo *WirelessHART* consiste na extensão para o domínio do sem fios do protocolo HART, da HART Foundation, e um acrónimo de *Highway Addressable Remote Transducer*

Protocol, uma norma de um protocolo para comunicações de campo (44). Este protocolo foi lançado em 2007, tendo sido o primeiro protocolo para redes sem fios de baixa potência a ter sido desenvolvido para ambiente industrial, mais concretamente para a Indústria de Processos, com vista a monitorização e também controlo de processos. Atingiu o grau de norma industrial internacional do IEC (*International Electrotechnical* Commission) em 2010, tendo-lhe sido atribuída a norma IEC62591-1 (*Industrial communication networks - Wireless communication network and communication profiles - WirelessHART™*) (45).

Este protocolo tem várias semelhanças com o protocolo *ISA100.11a*, desenvolvido posteriormente, de tal forma que existe já um grupo de trabalho dentro do ISA100 para criar a compatibilidade entre os dois protocolos.

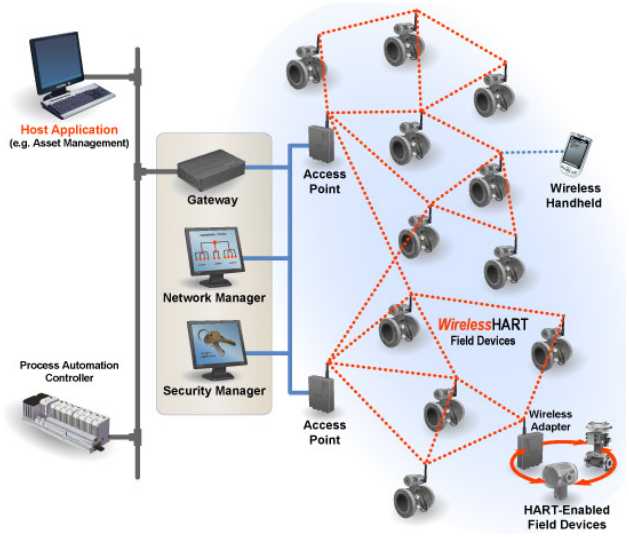


Figura 23 - Esquema da arquitectura de uma rede *WirelessHART*, com a representação dos diferentes tipos de elementos de rede (46).

Tem também uma aproximação semelhante no que toca à atribuição de prioridade a diferentes tipos de mensagem, neste caso dividida entre dados provenientes do Gestor de rede, que têm a prioridade mais alta, e os restantes dados, com prioridade superior a mensagens com dados de sensores e finalmente de informação de eventos.

O protocolo, tal como os descritos anteriormente, é baseado na norma *IEEE 802.15.4*, com algumas funcionalidades adicionais ao nível da camada DLL.

2.3.4.5.1. Elementos de rede

As redes *WirelessHART* permitem duas topologias diferentes, em estrela ou emalhada, sendo que a segunda é preferível na maior parte das aplicações, tendo em conta a robustez que adiciona ao criar diferentes caminhos e o aumento do alcance que possibilita, sendo apresentada na Figura 23.

A norma de protocolo define seis diferentes tipos de elementos de rede:

- A *Gateway*, uma interface entre a infrastrutura da rede de campo (rede HART) e a rede *WirelessHART*, permitindo a ligação dos dispositivos de campo às aplicações de utilizador;
- O Gestor de Rede (*Network Manager*), que configura a *Gateway* através de comandos de rede HART, permitindo *buffering* de grandes quantidades de dados de sensores, notificação de eventos ou resposta a comandos. Para além da configuração da *Gateway*, o Gestor de rede configura também os dispositivos de campo. Uma rede *WirelessHART* permite a existência de vários Gestores de rede, mas apenas por questões de redundância, visto que apenas um poderá estar em funções. Outras funções importantes do Gestor de rede consistem na manutenção das tabelas de *routing*, e do agendamento das comunicações (visto que o protocolo assenta num acesso à rede com base em TDMA);
- O Gestor de Segurança (*Security Manager*), que gere as diferentes chaves que protegem as comunicações e assim evita a intrusão;
- O dispositivo de campo (*Field Device*), desenhado para ser alimentado a baterias e ter, ao mesmo tempo, a capacidade de *routing*, e que está ligado aos sensores ou actuadores;
- O dispositivo portátil, para configuração e manutenção dos dispositivos instalados;
- O adaptador (*WirelessHART Adapter*), que consiste numa interface HART – *WirelessHART*, desenhado para substituir ligações HART ou 4-20 mA, sendo alimentado a partir do *loop*.

2.3.4.5.2. Camada PHY

Sendo esta camada equivalente à camada física do protocolo *IEEE 802.15.4*, o protocolo apenas está disponível na gama de frequência dos 2.4 GHz, com DSSS.

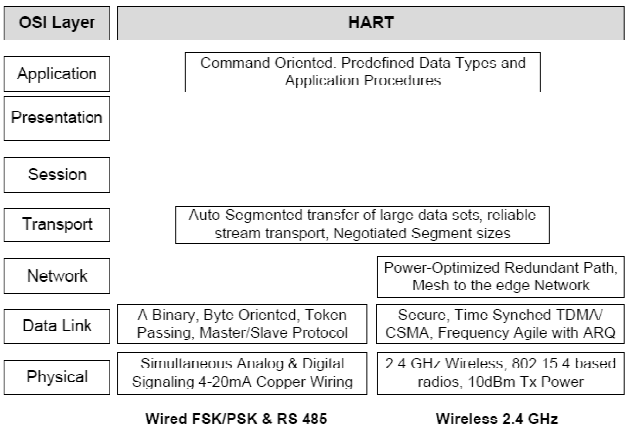


Figura 24 - Arquitectura em camadas do protocolo *WirelessHART* (42).

2.3.4.5.3. Camada DLL

Tal como havia sido indicado na secção Elementos de rede, o acesso à rede é sincronizado (protocolo TSMP), e portanto regulado através de TDMA, tendo cada *slot* temporal 10ms (47). Ao impor uma sincronização a implementação do mecanismo TDMA no protocolo *WirelessHART* permite que todos os dispositivos – mesmo aqueles alimentados a bateria –, sejam capazes de reencaminhar mensagens, proporcionando uma rede totalmente emalhada.

2.3.4.5.4. Camada NWK

Esta camada implementa os mecanismos de reencaminhamento de mensagens através de dois diferentes protocolos, já descritos para a norma *ISA100.11a*, *routing* de Grafo e *routing* de fonte (42). A diferença em relação a esta norma é que todos os dispositivos têm a capacidade de reencaminhamento de mensagens, consumindo ainda assim baixa potência. Este método é implementado através da já referida sincronização e atribuição de *slots* temporais aos diferentes nós da rede, aquando da instalação, e com configuração geral da rede através do Gestor de rede, que também regula os caminhos a seguir em qualquer tipo de protocolo de *routing* usado. Cada nó da rede tem a capacidade de ter o papel de nó "pai" e nó "filho", mantendo uma tabela de todos os seus vizinhos: os nós "pai", que podem encaminhar as suas mensagens, e os nós "filho", que encaminham mensagens através do nó que se está a considerar. A possibilidade de um nó da rede ser simplesmente filho, por quaisquer razões que sejam (necessidade de muito baixa latência, bateria com carga reduzida, etc.), é configurável (48).

2.3.4.5.5. Camada TRANS

Tal como os protocolos anteriores, o *WirelessHART* possibilita também comunicação com e sem suporte de ligação. Aplicações que necessitem de uma troca de dados fiável serão configuradas de forma a seguir o primeiro caso, existindo uma inicialização da ligação pela abertura de uma porta no destinatário, através de um comando HART, que configura a taxa de transmissão, por via do Gestor de rede. A fiabilidade da chegada dos dados é feita através de *acknowledgement*, e todos os pacotes são transmitidos na sua devida ordem. No final da comunicação a porta será novamente fechada, terminando a ligação. Naturalmente, existe também aqui um compromisso entre fiabilidade e quantidade de dados transmitidos, visto que estes mecanismos adicionam cabeçalhos às mensagens transmitidas. Para as aplicações que não necessitam de uma fiabilidade tão alta, e que aceitam a possibilidade do extravio de dados, garantindo assim a redução de cabeçalhos e a passagem mais rápida da mensagem na rede, é possível também configurar as suas comunicações sem *acknowledgement* (14).

2.3.4.5.6. Camada APL

Ao nível da camada de aplicação, existe uma conformidade com o protocolo HART, visto que o protocolo *WirelessHART* se trata de uma adaptação da norma que já existia para uma infrastrutura cablada, sobre *IEEE 802.15.4* (ver Figura 24).

2.3.4.5.7. Segurança

O protocolo implementa medidas de segurança que estão definidas como *default* e que não podem ser alteradas, estando constantemente ligadas. A segurança do ponto de vista da confidencialidade é implementada com base em encriptação AES de 128 bits, como é feito nos restantes protocolos mencionados, se bem que numa base *end-to-end*, ao nível da camada de rede/transporte, com encriptação de todos os dados da camada de rede à excepção do seu cabeçalho (49).

Relativamente à integridade, o protocolo beneficia, tal como também foi visto para os protocolos já descritos, do *Message Integrity Code* (de 32, 64 ou 128 bits) da norma *IEEE 802.15.4*, que poderá ser complementado com o modo CCM. Relativamente à autenticação, e igualmente à imagem dos anteriores protocolos, o *WirelessHART* implementa chaves de rede para aceitação de dados transmitidos entre dispositivos, bem como chaves de ligação à rede. Adicionalmente, este protocolo encripta as mensagens de ligação à rede, através de uma chave de *join*/associação.

2.3.4.5.8. Desenvolvimento de produto

Tendo sido o primeiro protocolo a ser desenvolvido – já em 2007 – direccionado para redes sem fios de baixa potência para ambiente industrial, o protocolo *WirelessHART* alcançou um desenvolvimento notável, ainda não comparável em termos de presença no mercado ao protocolo *ZigBee*, mas ainda assim presente, com vários fabricantes com módulos no mercado para inclusão em sensores inteligentes, e que possibilitam assim uma criação de sistemas de monitorização / automação baseados em *WirelessHART* muito mais rápida. As notícias mais recentes (junho de 2012) apontam no sentido de já terem sido instalados 100.000 dispositivos, em mais de 8.000 redes *WirelessHART* (50).

São exemplos os módulos da Dust Networks (mais propriamente da Linear Technology, que adquiriu a Dust Networks em Dezembro de 2011 (51)), reconhecida empresa da área, que aliás participou no desenvolvimento deste protocolo, e módulos de outros fabricantes, como a Nivis ou a RFM (módulos também baseados em controladores Dust Networks) (52)(53)(54).

Os módulos da Dust Networks/Linear Technology são parte constituinte dos sistemas *WirelessHART* da Emerson e Honeywell, empresas reconhecidas da área da Automação

Industrial, o que garante uma produção de dispositivos considerável, se bem que o seu custo de mercado – apesar de ser expectavelmente superior ao de soluções para ambiente doméstico ou empresarial – ainda está cerca de cinco vezes acima do preço de um módulo *ZigBee PRO* (dados fornecedor). No entanto, é neste momento a única norma desenhada para ambiente industrial que oferece condições de uma adaptação relativamente rápida e a custo aceitável para novos produtos.

2.3.4.6. DASH7

O protocolo *DASH7* é desenvolvido e promovido por um conjunto de empresas que estão associadas através da *DASH7* Alliance, empresas como a Texas Instruments, a Savi Technology ou a Semtech. O seu nome provém da norma ISO/IEC 18000-7, que define a tecnologia de RFID activo para 433 MHz (55). É nesta gama de frequência que o protocolo *DASH7* se baseia, sendo assim o único dos protocolos descritos que não é construído sobre a norma *IEEE 802.15.4*.

Em 2009, o Departamento de Defesa (DoD) dos EUA assinou um contrato de 429 mil dólares para o desenvolvimento do protocolo *DASH7*. Em março do mesmo ano, foi criada a *DASH7* Alliance (56).

Apesar de o protocolo ser considerado aberto pela *DASH7 Alliance*, apenas no segundo trimestre de 2012 se tornou disponível ao público em geral informação relativa à especificação. Desta forma, até esta altura apenas associados tiveram acesso ao *draft* da norma. O Modo 2 é este *draft*, que se trata de um *upgrade* à norma ISO/IEC 18000-7, e que se encontra neste momento em processo de aprovação ISO/IEC (57).

A ideia do desenvolvimento de um protocolo de comunicações para redes de sensores nos 433 MHz pretende portanto apostar em longo alcance – a organização publicita um alcance regulável entre 10m e 10 km (58) – e uma topologia de rede o mais simples possível, implementando assim apenas redes em estrela. Apesar desta imagem de protocolo mais "simples", quando comparado com os seus congéneres dos 2,4 GHz, foi já anunciado um *upgrade* futuro para possibilitar uma topologia emalhada.

O protocolo prevê 7 camadas: Física, Enlace, Rede, Transporte, Sessão e Aplicação, sendo que esta última ainda se encontra em desenvolvimento (59). As restantes são descritas de seguida.

2.3.4.6.1. Elementos de rede

No modo 1 deste protocolo, os elementos que constituíam a rede *DASH7* eram à semelhança da norma ISO/IEC 18000-7, apenas com dispositivos Interrogador (o comum *reader*) e dispositivos *tag*, para os elementos sensores, numa adaptação das *tags* activas. No modo 2, existem já 4 tipos de dispositivo: *blinker*, *endpoint*, *Subcontroller* e *Gateway*, sendo que se distinguem entre si, tal como nos restantes protocolos, através das capacidades que detêm, dentro do conjunto de possibilidades que o protocolo permite.

Device Class	Transmits	Receives	Complete Featureset	Wake-on Scan Cycle	Always-on Receiver
Blinker	•				
Endpoint	•	•		•	
Subcontroller	•	•	•	•	
Gateway	•	•	•		•

Figura 25 - Funcionalidades por tipo de dispositivo - protocolo *DASH7* (60).

O dispositivo *Blinker* consiste no elemento mais simples dentro do protocolo *DASH7*, tratando-se de um tipo de dispositivo que apenas detêm funções de transmissão de dados. O elemento *Endpoint* trata-se de um tipo Dispositivo Terminal, com características de transmissão e recepção de dados, mas apenas em modo *wake-on event*, ou seja, apenas recebe dados aquando de um pedido da sua unidade pai, que armazena dados que lhe são encaminhados – ao estilo do tipo de comunicação interrogador-*tag,*do denominado Modo 1. O dispositivo *Subcontroller* e *Gateway* têm praticamente as mesmas características, apenas com uma distinção fulcral para a sua operação: o dispositivo *Gateway* trata-se de um típico *router* ou coordenador de rede, com a sua unidade rádio sempre ligada, sendo que o dispositivo Subcontroller funciona no modo *wake-on*, do mesmo modo que um *Endpoint* (61).

2.3.4.6.2. Camada PHY

O protocolo consagra na sua versão actual 8 canais entre os 433,05 MHz e os 434,79 MHz, sendo a modulação usada a GFSK. A frequência de base fixa-se nos 433,92 MHz, e a taxa de transmissão máxima (designada de *turbo data* rate) é de 200 kbps, sendo a normal (*normal data rate*) de 27,7 kbps (62). A largura de banda dos canais é definida através do índice de largura de banda, que poderá ser um de quatro, de acordo com a Figura 26.

Bandwidth Index	Channel Bandwidth	Modulation	Symbol Rate
0x00	0.432 MHz	FSK-1.8	55.555 kHz
0x01	0.216 MHz	FSK-1.8	55.555 kHz
0x02	0.432 MHz	FSK-0.5	200 kHz
0x03	0.648 MHz	FSK-0.5	200 kHz

Figura 26 - Índices de largura de banda do protocolo *DASH7* (61).

O protocolo possibilita que sejam implementados simultaneamente diferentes canais, até 8 canais concorrentes à *normal data rate* e 4 canais à *turbo data rate* (61) (59).

2.3.4.6.3. Camada de Enlace

O acesso à rede é executado através do mecanismo CSMA, já descrito, incluindo ainda um mecanismo de "guarda" dos canais cujo acesso ocorre de acordo com CSMA, uma vez que o protocolo também consagra canais com acesso livre, sem CSMA. Este mecanismo consiste na implementação de um "tempo de guarda" que existe entre transmissões de mensagens, e que é sempre inferior ao tempo de transmissão de uma mensagem. Deste modo, se o tempo de uma transmissão é superior ao tempo de guarda e o período de silêncio (aquele durante o qual os restantes dispositivos aguardam) é inferior ao tempo de guarda, então o canal está em modo de "guarda" pelo menos durante um "tempo de guarda", não ocorrendo aí acesso sem o mecanismo CSMA. Apesar de apenas se referir o mecanismo CSMA, na verdade o protocolo implementa o CSMA-CA, sendo que a funcionalidade de *Collision Avoidance* foi "transportada" para a camada de Transporte. É no subtópico que lhe está dedicado que se explica este mecanismo (61).

A camada contém dois tipos de mensagens: de *background* e de *foreground*, sendo que as últimas se tratam do tipo comum de mensagens de dados (incluem endereçamento, etc) e as primeiras mensagens de extrema simplicidade, que servem para sincronização de grupos de dispositivos.

Existe um esquema designado de *channel scan cycling*, em que os diferentes dispositivos percorrem todos os canais designados para a rede, verificando se estão transmissões a decorrer – seja de *background frames* ou de *foreground frames*, percorrendo cada um durante um determinado período de tempo, e passando de seguida para o próximo canal. Um dispositivo apenas interrompe o seu *channel scan cycling* quando está desligado ou quando uma comunicação está a decorrer. Adicionalmente, existe um esquema designado de *beacon transmit series,* semelhante ao *channel cycling*, em que uma mensagem de *beacon* é transmitida pelo

dispositivo para o espectro em caso de fim de *channel cycling* (auto-reset), ou em caso de evento periódico programado (61).

O endereçamento de camada de Enlace é efectuado através de identificadores de 64 bits, que são exclusivos a cada dispositivo *DASH7*.

Manuf ID	Extension	Serial Number
16 bits	8 bits	40 bits

Figura 27 – Composição de um identificador *DASH7* - identificador de fabricante (Manuf ID), extensão (extension) e número de série (serial number) (61).

Na Figura 27 é apresentado o esquema de geração de um identificador. Neste, o campo extensão ainda não tem uma utilização definida do presente Modo 2, podendo ser ignorado.

Nesta camada é ainda implementado um mecanismo de segurança, através da encriptação com base no algoritmo AES-128.

A comunicação com dispositivos adormecidos é efectuada através de um paradigma distinto daquele dos protocolos baseados em *802.15.4*, designado de *wake-on radio*. O *wake-on radio* consiste na ligação periódica do dispositivo rádio e verificação da transmissão de mensagens destinadas àquele dispositivo (*endpoint*), sendo que o emissor transmite periodicamente um aviso de envio de mensagem para o *endpoint*. Assim, não existe transmissão de uma mensagem de *beacon* por parte do *endpoint*, mas antes uma activação periódica do modo de recepção (61).

2.3.4.6.4. Camada de Rede

O protocolo designado de M2NP (*Mode 2 Network Protocol*) define o endereçamento no protocolo *DASH7* Modo 2, possibilitando uma rede *multi-hop*, mantendo o mesmo esquema de pedido-resposta. O esquema de *multi-hop* apenas permite uma distância de 2 entre emissor e receptor, e é mantido através de tabelas de reencaminhamento. Em todas as transmissões existem 4 diferentes tipos de dispositivo: origem (aquele que gera a mensagem), solicitante (aquele que origina o pedido de transmissão), correspondente (aquele que responde ao pedido do solicitante) e destinatário (dispositivo ao qual a mensagem se destina) (61) .

2.3.4.6.5. Camada de Transporte

O protocolo designado de M2QP (*Mode 2 Query Protocol*) regula a comunicação entre dispositivos, ao implementar dois tipos de métodos de diálogo entre membros da rede: arbitrado e não arbitrado. O primeiro trata-se de um diálogo permanente entre dispositivos solicitadores e dispositivos correspondentes, sendo que o primeiro se trata de um único dispositivo, que envia uma série de pedidos e o segundo poderá tratar-se de um grupo de dispositivos que reconhece o

identificador do solicitador. O modo não arbitrado trata-se de uma comunicação dita "normal", onde existe um único solicitador e n correspondentes, mas cujos identificadores são indicados na mensagem (61).

Para além dos designados "modelos de diálogo", esta camada define ainda três modelos de *Collision Avoidance*, uma vez que o processo CSMA-CA que implementa está espalhado pelas diferentes camadas. O protocolo define dois esquemas de Controlo: de Congestão e de Fluxo, e que controlam o processo de CSMA da camada de Enlace (61).

2.3.4.6.6. Camada de Sessão

É nesta camada que é implementado o mecanismo de *wake-on radio*, em que dispositivos adormecidos são retirados desse estado através da detecção de um evento. Vários eventos podem proporcionar o *wake-on*, como (60):

- Pesquisa de canal, da camada de Enlace;
- *Beacon transmit series*, da camada de Enlace;
- Pesquisa passiva de eventos RF externos (camada de Aplicação);
- Eventos de sensores (camada de Aplicação);
- Qualquer evento de camada de Aplicação ao qual seja dado esse direito.

O controlo da pesquisa de canal permite que se efectue a transição entre estados adormecido e ligado para dispositivos alimentados a, sendo que esta ocorre caso uma série de pesquisas de canal ocorra sem qualquer *foreground frame* recebida.

Os eventos RF externos referidos são relativos a, por exemplo, mensagens recebidas durante os períodos de pesquisa de canal provenientes de dispositivos de uma *stack* RF diferente. No fundo, trata-se da recepção de qualquer forma que não através de *channel cycling*.

Os eventos de sensores referem-se ao início de um diálogo *DASH7* a partir da detecção de um evento de sensor, sendo que este deverá ter um identificador de acordo com a norma ISO 21451-7 (61).

2.3.4.6.7. *DASH7* e NFC

O protocolo *DASH7* está baseado na gama de frequência do espectro electromagnético dos 433 MHz (433,92 MHz), principalmente pelas razões já enumeradas, como o maior alcance das suas comunicações e maior robustez em relação a questões como distorção multi-caminho em ambiente industrial. No entanto, existe mais uma vantagem ainda não nomeada desta gama de frequências, a possibilidade de usar a mesma antena para comunicações NFC (*Near Field Communication*), nos 14 MHz (13,56 MHZ), visto que a frequência de base do protocolo

DASH7 é seu múltiplo. Assim, e apesar de o protocolo NFC sair do âmbito das redes de sensores sem fios e competir com tecnologias como o RFID passivo, para muito curtas distâncias – e aplicações como identificação pessoal –, trata-se de uma vantagem que o protocolo *DASH7* poderá ter em relação aos seus competidores, ao conseguir colocar no mercado duas tecnologias de comunicações por um custo mais baixo.

2.3.4.6.8. Desenvolvimento de produto

No actual momento de desenvolvimento, é apenas possível uma solução com base no protocolo *DASH7* através da associação como membro à *DASH7* Alliance, visto que não existe qualquer fabricante de módulos com base neste protocolo, bem como informação mais específica sobre o Modo 2 disponível para não membros.

A única solução poderia ser a adaptação de uma implementação oficial *open source* do protocolo, *opentag*, e daí adaptar a um microcontrolador preferencial. Ainda assim a falta de informação inviabiliza este desenvolvimento, e apesar das valências protocolares apresentadas e da interessante noção de que um protocolo baseado numa gama de frequência inferior aos 2.4 GHz poderia vingar em ambientes mais ruidosos, não é ainda possível planear a implementação deste protocolo.

2.3.5.Características físicas de dispositivos

2.3.5.1.1. Para frequências dentro da norma *IEEE 802.15.4*

As características dos dispositivos baseados nesta norma poderão variar, principalmente de acordo com a frequência de comunicação para a qual foram concebidos.

Tabela 3 - Características e valores típicos de rádios de baixa potência, para WSN, à taxa de transmissão da 250 kbps.

	Potência[1]	**Sensibilidade**	**Rejeição de Canal Adjacente**	**Rejeição de Canal Alternado**	**Tamanho (mm^3)**
2,4 GHz	-10 a 20 dBm	-99 dBm	35 dB	56 dB	13 x 25 x 2,5
868 MHz	-10 a 20 dBm	-108 dBm	30 dB	40 dB	13 x 25 x 2,5
433 MHz	-30 a 13 dBm	-95 dBm	25 dB	14 dB	9,8 x 9,8 x 2,5[2]

[1] Apesar de estar indicado como valor máximo 20 dBm, não significa que este seja o possível, pois deve cumprir os limites definidos pelo estado no qual é usado.

[2] O dispositivo indicado para os 433 MHz consiste num SoC, que não inclui o circuito de *balun*, tendo portanto dimensões consideravelmente inferiores aos restantes apresentados.

	Consumo Tx/Rx[3]	**Consumo Modo *Off***	**Tensão de Alimentação**
2,4 GHz	27 mA	1 uA	2,8 a 3,6V
868 MHz	28 mA	1 uA	2,8 a 3,6V
433 MHz	29,2 mA/17,1 mA	1 uA	1,8 a 3,6V

Na tabela seguinte são apresentadas as características físicas típicas de dispositivos rádio desenhados para comunicações segundo a *IEEE 802.15.4*, nas duas gamas de frequência possíveis no espaço da União Europeia, 868 MHz e 2,4 GHz.

Figura 28 - Exemplo de dispositivos OEM (Original Equipment Manufacturer) desenhados para comunicação sobre *IEEE 802.15.4*, nos 2,4 GHz (63).

Considerando a performance deste tipo de dispositivos, nos 2,4 GHz, um dos pontos mais importantes que lhe estão associados é o alcance. Tal como foi apontado na secção Tecnologias de Radiofrequência, existem diversos factores que influenciam a performance de uma ligação entre dois dispositivos sem fios – relativos ao meio no qual os dispositivos estão instalados –, aos quais ainda acrescem outros apontados na Tabela 3 – relativos ao aparelho de rádio. Em concreto, é necessário considerar factores intrínsecos a cada rádio, e que poderão ser reguláveis, como a potência de transmissão (comprometendo consumo), a sensibilidade (comprometendo a *datarate*), ou a antena usada, que poderá ser direccional ou isotrópica e ter ganho ou não (antenas com ganho serão maiores), com factores do meio, que não são controláveis, e que incluem factores ambientais como ruído electromagnético gerado por outros equipamentos ou a quantidade e características dos obstáculos entre os dispositivos. Por esta razão, é difícil ou mesmo impossível planear sistemas sem fios apenas com base nos dados fornecidos pelos fabricantes desses mesmos dispositivos, visto que os valores indicados para alcances são sempre relativos a condições ideais, como a existência de linha de vista, a inexistência de ruído, e a

[3] O consumo é dependente da potência de transmissão, e portanto os valores apresentados são referentes à potência de 10 dBm. Para simplicidade, considerou-se que o consumo do modo de recepção (Rx) é igual ao do modo de transmissão (Tx).

utilização de potência máxima e sensibilidade mínima (nem sempre possíveis, principalmente a transmissão em potência máxima em dispositivos a bateria).

Assim, e de acordo com testes feitos com dispositivos comprados ou desenvolvidos ao longo deste trabalho, e que serão apresentados no capítulo de resultados, é possível dizer que, tipicamente, em condições normais de montagem e configuração[4], cerca de 150 m quando emissor e receptor estão em linha de vista, cerca de 80 m sem linha de vista mas em espaço aberto, e 20 m através de paredes, para uma potência típica de 10 dBm. Para a gama dos 868 MHz, o alcance aumenta, para cerca de 200 m em linha de vista, 100 m com obstáculos e em espaço aberto, e 30 m com obstáculos através de paredes.

2.4. Alimentação de dispositivos de baixa potência

Este tema constitui uma secção por si só, visto que é um dos pontos fulcrais que permitem a criação de redes totalmente sem fios, do ponto de vista das comunicações e da alimentação. Veja-se que apesar de grande parte dos dispositivos rádio actuais (2011/2012) permitirem consumos na casa dos 80mW nos modos de transmissão ou recepção, um conjunto de baterias de tipo AA terá, no máximo, uma capacidade à volta de 2,5 A.h a 3,6 V (tensão que permite alimentar electrónica de baixa potência), o que corresponderia a uma autonomia de 4 dias. Por outro lado, o papel dos protocolos de comunicação para redes sem fios de baixa potência consiste efectivamente na redução do tempo em que o dispositivo rádio se encontra ligado, consumindo corrente principalmente devido ao seu modo de recepção. Assim, qualquer protocolo moderno possibilita já consumos abaixo dos 300 µW (através de mecanismos baseados em *duty cycle*, colocando o dispositivo rádio desligado durante grande parte do tempo), o que se traduz numa autonomia de mais de 3 anos, para a mesma bateria.

Apesar desta perspectiva parecer suficientemente satisfatória, visto que a maior parte das aplicações aceitarão um período para manutenção de 3 anos, é necessário ter também em conta que, para além dos consumos derivados das comunicações, existem ainda os consumos provenientes do tipo de aplicação, que igualmente condicionam as necessidades energéticas do dispositivo. Para além deste factor, há ainda outros tipos de tecnologia em que, se as necessidades energéticas forem suficientemente baixas, permitirão tornar o sensor autónomo também da perspectiva da alimentação, através de captura energética.

[4] Os dispositivos são instalados de uma forma típica de instalação, não sendo a esta feita para maximizar uma ligação e assim obter o máximo alcance para apenas uma ligação (por exemplo usando antenas direccionais, e colocando ambos os dispositivos de forma a igualar polaridades). Por outro lado, os dispositivos não têm antenas de alto ganho (típico em sensores) e a potência de transmissão não é a máxima (comummente um sensor transmite a 1 dBm, de forma a minimizar a corrente gasta em transmissão).

2.4.1.Adaptação e Conversão de Tensão

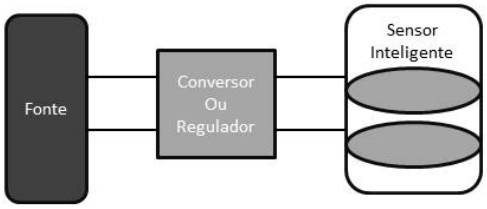


Figura 29 - Esquema representativo do sistema típico de alimentação de um sensor inteligente.

Na Figura 29 é apresentado o sistema habitual de alimentação de um sensor inteligente, onde o elemento central depende em qualquer caso da fonte de alimentação usada, visto que terá de fazer a adaptação da tensão de alimentação fornecida pela fonte para um nível que poderá variar entre 3,6 e 2,8V, a janela de tensão de alimentação permitida pela maior parte da electrónica utilizada (microcontroladores, sensores e dispositivos rádio). A opção entre um conversor DC/DC ou um regulador de tensão (tipicamente um *Low dropout regulator* – LDO) deverá ser feita de acordo com as características de entrada e saída pretendidas, tendo em conta que dois dos parâmetros mais importantes a ter em conta são a sua eficiência e a corrente consumida.

Em comparação com o LDO, o conversor DC/DC é especialmente útil em aplicações onde existe variação da tensão de alimentação ao longo do tempo, como no caso de alimentação por supercondensadores, cuja tensão baixa à medida que a sua carga vai sendo consumida. Um DC/DC do tipo *buck*/*boost* permite conversão para uma tensão fixa pretendida, inferior à tensão de entrada (modo *buck*) e, à medida que esta vai baixando de tal forma que se desce abaixo de um dado limite, continua a converter para a tensão fixa pretendida, ainda que a tensão de entrada seja inferior a esta (modo *boost*). É útil para que o máximo da carga existente num dispositivo de armazenamento de energia deste tipo seja aproveitado. Este tipo de componente também permite outras funções, como isolamento galvânico (pode ser constituído por um transformador), mas são constituintes mais caros e mais complexos, o que leva a que tenham, para componentes equivalentes, correntes quiescentes mais altas do que os reguladores LDO, que continuam a permitir uma boa eficiência e correntes quiescentes mais baixas (chegando facilmente à ordem de 1 microampere), extremamente úteis para a redução do consumo dos dispositivos em modo adormecido. A corrente quiescente consiste na corrente mínima de consumo do dispositivo, quando não existe carga ou, em aproximação, quando esta é muito abaixo da carga para a qual foi desenhado, na casa das décimas de microampere para conversores DC/DC[5]).

[5] Fonte: conversor DC/DC de baixa corrente quiescente TI TPS54062 - http://www.ti.com/product/tps54062

A eficiência do dispositivo como um todo está ligada à própria eficiência do seu elemento de regulação de tensão, o que constitui – para além da corrente quiescente – a um dos principais problemas na sua utilização, as perdas energéticas que estão associadas (à conversão de tensão). No entanto, e tendo em conta a necessidade deste tipo de componentes, existem elementos de regulação destinados a aplicações de baixo consumo e custo com eficiências na casa dos 90 %.

2.4.2.Consumo de um sensor sem fios

É necessário, para tratar o tema do consumo de um sensor sem fios – um dispositivo de muito baixa potência, na casa das dezenas de uW.h –, considerar os seguintes conceitos:

- Consumo de cada um dos seus constituintes, seja em modo activo seja em modo adormecido[6];
- Equilíbrio e programação entre modos activos e modos adormecidos de cada constituinte – o que é tipicamente designado de *duty cycle*[7]

De acordo com as necessidades de cada um dos componentes em termos de consumo, e tendo em mente a longevidade pretendida, é necessário programar o dispositivo, bem como configurar periféricos como a unidade rádio ou sensores para que o *duty cycle* seja tal que o consumo médio do dispositivo possibilite a longevidade sem manutenção tipicamente pretendida para um sensor inteligente industrial, de 2 anos. Veja-se o cálculo seguinte, do consumo máximo que uma bateria com uma capacidade de 2A.h permite:

$$consumo\ médio\ por\ hora = \frac{capacidade\ da\ bateria}{horas\ de\ serviço} = \frac{2000\ mA.h}{2\,.365\,.24\ horas}.90\% \cong 100\ \mu A$$

Considerando que o consumo típico de um microcontrolador em modo activo é de cerca de 2 mA.h, somando-se cerca de 20 mA.h para uma unidade rádio em modo receptor e cerca de 800 µA.h por sensor (valores a 3,3 V), é necessária uma redução em cerca de duas ordens de grandeza, apenas alcançada através da implementação de um *duty cycle* apertado.

Esta performance é conseguida através de esquemas de programação de execução periódica de tarefas, nomeadamente de medição e comunicação com a rede, em aplicações de monitorização contínua.

[6] O chamado "modo adormecido" consiste num tipo de configuração de dispositivos microcontroladores, em que estes são programados para, tipicamente, desactivarem todos os seus constituintes principais, à excepção das suas entradas (digitais ou analógicas), para a detecção de eventos, ou de temporizadores internos programáveis, para a periódica chamada de rotinas. Este modo permite consumos muito mais baixos do que os de modo activo, constituindo tipicamente cerca de 1% deste.

[7] *Duty cycle* é um termo técnico que pretende representar os modos de funcionamento periódico de um dispositivo, que neste tipo de aplicação passa grande parte do tempo em modo adormecido (todos os seus componentes neste modo) e um período de tempo mínimo a executar funções de comunicação e aquisição de dados.

2.4.3. Alimentação por fontes finitas

Por fontes finitas consideram-se unicamente baterias, sejam do tipo primário ou secundário. Poder-se-iam considerar também os supercondensadores (condensadores electroquímicos de dupla camada), uma tecnologia em franco desenvolvimento, mas que (por si só) ainda não permite alimentar um dispositivo continuamente durante um longo período de tempo, não só por não suportar uma carga comparável à de uma bateria, mas pelo facto de a sua tensão baixar também continuamente, até níveis que impossibilitam o funcionamento do dispositivo (64)(65).

Assim, em grande parte das aplicações são usadas baterias, seleccionadas de acordo com:

- As dimensões máximas permitidas pela aplicação do dispositivo;
- As necessidades energéticas (em termos de capacidade) do dispositivo, para um tempo médio sem manutenção;
- A corrente máxima (mesmo que instantânea, durante alguns milissegundos) consumida pelo dispositivo, e que deverá ser inferior à corrente máxima que a bateria consegue debitar.

Actualmente as tecnologias de bateria primária que permitem uma densidade energética mais elevada são as do Lítio, associadas ao Cloreto de Tionilo (como cátodo), como o Cloreto de Lítio-Tionilo ($LiSOCl_2$), com uma capacidade por kg de 290 W.h/kg ou o Cloreto de Lítio-Tionilo com Cloreto de Bromo ($LiSOCl_2$,LiBr), com uma capacidade por kg de 350 W.h/kg, sendo o primeiro mais comum no mercado. Assim, uma bateria desta tecnologia (já considerada no exemplo da introdução desta secção), do tipo AA terá uma capacidade de 2,5 A.h a 3,6 V (66).

As baterias possibilitam também uma tensão muito mais estável do que um condensador, com performances de curva de descarga que se aproximam a uma curva em degrau, debitando sempre a mesma tensão para uma mesma carga, ao longo de toda a vida útil (ver Figura 30).

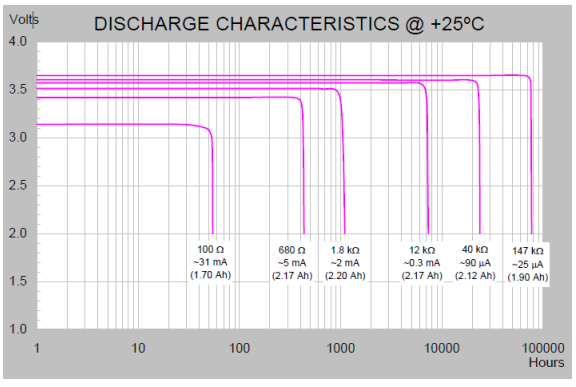


Figura 30 - Curva da tensão fornecida (associada à sua descarga) de uma bateria tipo AA da tecnologia $LiSOCl_2$, para diferentes cargas, ao longo do tempo (67).

A outra característica principal a ter em conta ao seleccionar uma bateria está associada à corrente máxima que esta poderá debitar. Se é verdade que uma bateria consegue debitar mais corrente do que o valor indicado como máximo pelo fabricante, também é verdade que este tipo de ocorrência é danoso para a bateria, reduzindo consideravelmente a sua capacidade. Assim, e para a tecnologia considerada ($LiSOCl_2$), é possível adquirir baterias com características até uma corrente de pico permitida de 200 mA e uma corrente contínua permitida de 100 mA (67). Mesmo em casos onde a carga requisitada pelo dispositivo não ultrapassa a carga de pico permitida, é expectável que, para cargas mais elevadas a tensão aos terminais da bateria desça também, tal como é ilustrado na Figura 30, de tensão de acordo com a carga que o dispositivo está a impor.

Assim, para soluções onde o tamanho é importante – e é habitual que seja, visto que grande parte dos dispositivos sensores, tal como foi discutido na Introdução, tem dimensões reduzidas e que são comparáveis à da bateria – deve existir um bom planeamento, em termos da dimensão máxima e da capacidade necessária para que tenha a autonomia pretendida, o que também vai afectar a corrente máxima que a bateria poderá debitar para o sistema. Mesmo considerando baterias com alto rendimento e que poderão debitar o valor mais alto possível de corrente, ao baixar do exemplo dado atrás para uma bateria tipo ½ AA, a corrente de pulso permitida passa para metade dos valores apresentados. Apesar de que este valor não constrinja ainda a solução, já que se esperam, tipicamente, consumos máximos na casa dos 50 mA, soluções de menor dimensão serão fortemente constrangidas por estes factores, necessitando de um bom compromisso entre as três condições.

2.4.4.Alimentação por fontes "infinitas" – Captura Energética

Apesar de a alimentação através de baterias já possibilitar uma performance interessante para a maior parte das aplicações baseadas em redes de sensores sem fios, é também bastante atraente a ideia de não ser necessário qualquer tipo de manutenção, ao tornar o dispositivo autónomo também do ponto de vista da alimentação, ao prescindir de baterias. É possível fazê-lo ao implementar sistemas baseados em captura energética, utilizando dispositivos que convertem energia ambiente em energia eléctrica, e com uma performance tal que possibilita a alimentação quase perpétua (visto que a electrónica utilizada tem um tempo de vida finito) do dispositivo. O desenvolvimento de tais componentes é, por si só, base suficiente para uma dissertação de doutoramento, mas existem no mercado dispositivos já desenvolvidos, que executam não só a captação de uma forma de energia ambiente como a armazenam e controlam, de acordo com as necessidades energéticas da carga, que possibilitam a rápida e controlada introdução de técnicas de captura energética em dispositivos de baixo consumo.

A literatura relacionada com métodos de captura energética apresenta uma série de variáveis para as quais já foram encetados esforços para desenvolver dispositivos de captura energética, conciliando dimensões reduzidas com uma boa performance em termos de conversão energética. Os ambientes para os quais este trabalho se destina, naves fabris ou instalações exteriores, são pródigas nestas formas de energia, tendo exemplos como:

- Gradiente térmico: energia libertada por exemplo em fornos industriais ou equipamentos onde ocorra fricção;
- Campos Electromagnéticos: na monitorização de estações de produção ou de transformação de energia eléctrica, estando altas tensões envolvidas, que criam campos magnéticos consideráveis nas suas proximidades, e que poderão criar correntes eléctricas em bobinas através de indução magnética;
- Luz: para soluções em naves industriais, a luz ambiente persiste continuamente, possibilitando a geração contínua de energia, e para soluções em exterior a geração de energia durante o dia, devidamente associada a uma forma do seu armazenamento, possibilita também a contínua alimentação de um dispositivo;
- Vibrações: geradas por máquinas, na casa dos 50-60 Hz ou, para sistemas de localização, pelo movimento do corpo humano, com frequências próximas de 1 Hz.

Os diferentes tipos de dispositivos para captura energética que se encontram no mercado permitem o desenvolvimento de soluções sem fios alimentadas por este método, de acordo com o ambiente ao qual essas mesmas soluções se destinam. Esta escolha implica não só a presença da forma energética em larga escala mas também características ligadas à forma que o dispositivo deverá ter enquanto produto.

3. Arquitectura Geral do Sistema

3.1. Introdução

Tal como se demonstrou no capítulo anterior, o desenvolvimento e a instalação de redes de comunicações sem fios em determinados ambientes industriais – para fins de Instrumentação e de Automação – constitui, por si só, um factor de inovação. No entanto, seguindo também a linha de apresentação do estado da técnica nesta área, foi demonstrado que as soluções existentes se encontram ainda em estado de desenvolvimento e que, como tal, existe ainda espaço para a criação de um novo sistema, empregando como base protocolos já existentes e combinando-os com as adaptações necessárias ao fim pretendido – a aplicação pretendida. Para além disso, a Inovação consiste não só na criação de sistemas novos mas também na sua difusão e consequente aceitação por parte do mercado.

Neste sentido, é apresentada no presente capítulo uma arquitectura de sistema de instrumentação baseada primeiramente em comunicações sem fios, mas também incluindo dispositivos de campo apenas habilitados a comunicações cabladas. A mesma arquitectura de rede de comunicações foi implementada sobre dois diferentes tipos de protocolo, diferentes desde a sua camada física, tal como se verá mais à frente nesta dissertação, e que se aplicam principalmente a diferentes tipos de ambiente e de necessidade de informação.

Partir-se-á da rede geral de comunicações, onde estão incluídos dispositivos e protocolos que não foram desenvolvidos no âmbito desta dissertação, mas que permitem a interface do sistema apresentado com outros sistemas, possibilitando assim funcionalidades como a ligação à *Internet*, o armazenamento de dados em servidor remoto ou a visualização de dados e configuração de parâmetros por parte de um utilizador.

Posteriormente, apresenta-se a rede "híbrida" na qual todo o sistema de comunicações se baseia.

Neste capítulo são assim apresentadas as escolhas tomadas no desenvolvimento desta arquitectura de rede, que possibilitam a criação de redes de sensores sem fios, que incluem as já atrás mencionadas ilhas onde existem comunicações cabladas, e que são integradas sobre a rede sem fios, dando assim azo a uma rede de comunicações altamente versátil e distribuída, que cumpre ainda necessidades de segurança de informação e de fiabilidade de rede.

3.2. Cenários de Aplicação

Os cenários de aplicação para os quais as soluções foram desenhadas foram já genericamente descritos, no capítulo introdutório, mas merecem um maior pormenor, de forma a apresentar em detalhe as condições fronteiras que levaram às escolhas em termos de arquitectura de rede.

Assim, os sistemas foram desenhados tendo em conta tanto ambientes fabris como ambientes de indústrias de processo, com um principal foco nas segundas, mais concretamente cimenteiras, subestações eléctricas e refinarias (Indústrias Cimenteira, de Energia e *Oil & Gas*). As soluções foram sempre pensadas do ponto de vista da monitorização, para proporcionar um seguimento contínuo do estado de equipamentos, bem como aviso em situações de alerta. Estas funcionalidades proporcionam não só um aumento da eficiência das instalações industriais, ao permitirem uma sincronização entre a manutenção de um dado equipamento e a proximidade da sua situação de falha, mas também da segurança das instalações, pois permitem evitar situações de acidente.

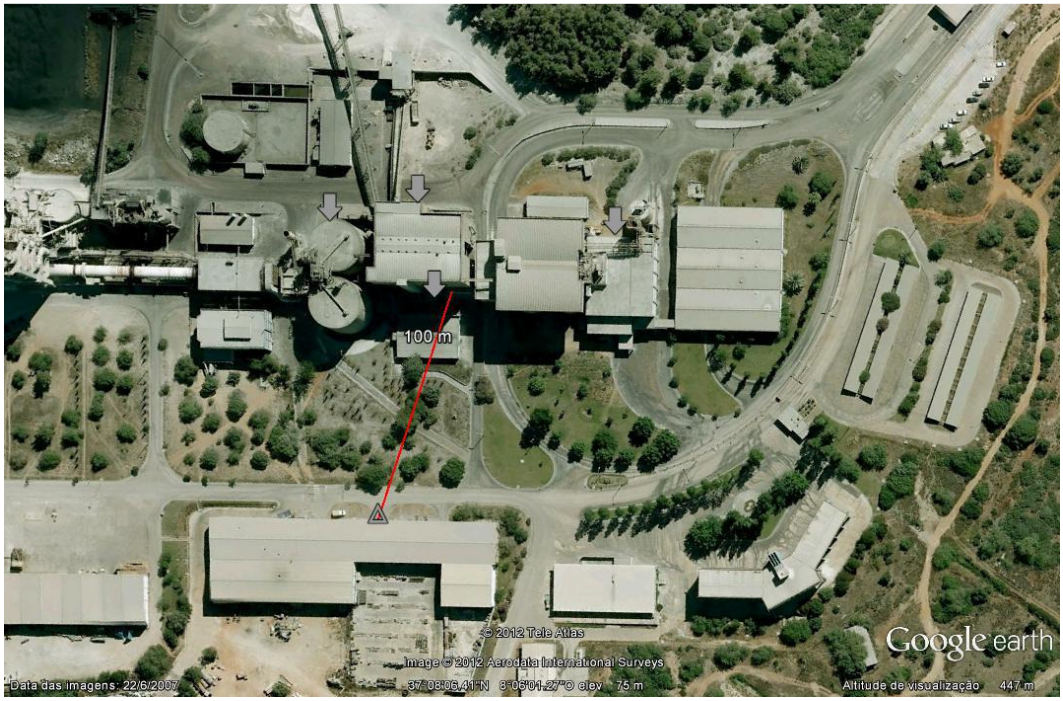


Figura 31 - Fotografia de satélite das instalações da Cimpor em Loulé. São indicados alguns pontos de monitorização (setas), bem como o ponto de instalação do ponto de acesso da rede (triângulo). Fonte: Google, 2007.

Na Figura 31 é apresentada uma fotografia de satélite das instalações de uma cimenteira para a qual foi feito um estudo de instalação de sensores de vibrações, sendo que se verificou uma necessidade de todos os sensores comunicarem sem fios, dada a falta de pontos de acesso à rede eléctrica, que permitiria a alimentação de uma rede de campo cablada. Foram também factores tidos em conta as elevadas distâncias entre pontos de monitorização e também a grande

quantidade de barreiras existentes ao longo da instalação industrial, entre maquinaria e paredes metálicas.

Veja-se assim que, para uma rede sem fios com 3 a 5 sensores sem fios por cada ponto indicado na figura, existe ainda uma grande quantidade de barreiras metálicas que é necessário ultrapassar e portanto a necessidade de recorrer a repetidores, colocados estrategicamente no terreno, e que fazem a ligação entre os pontos de medição mais remotos e o ponto de acesso. No entanto, não chegou a resultar qualquer instalação baseada nesta ou noutra proposta.

Figura 32 - Fotografia de satélite da subestação eléctrica da EDP no Alto de S. João em Coimbra. As setas representam alguns dos pontos de monitorização e o triângulo o ponto de acesso da rede. Fonte: Google, 2007.

Na Figura 32 é apresentada uma fotografia da subestação eléctrica da EDP onde foi feita uma instalação piloto de sensores sem fios (e que será apresentada em detalhe no capítulo 6), e onde são apresentados alguns dos pontos de monitorização. Apesar de tal não ser explícito na imagem, e de a distância entre os pontos de medição mais remotos e o ponto de acesso da rede ser reduzida em comparação com a instalação anterior, existe uma grande quantidade de metal junto aos pontos de medição, o que leva a reflexões de sinal. Numa subestação pretende-se monitorizar continuamente diferentes equipamentos, como disjuntores, transformadores e seccionadores, sendo as características das variáveis monitorizadas de diferentes tipos. No caso dos seccionadores e disjuntores, visto que são órgãos que apenas alteram o seu estado ocasionalmente, aplica-se facilmente um sensor sem fios, que detecta estes eventos e alerta à central. No caso dos transformadores, estes necessitam de uma monitorização contínua, de uma ordem superior a 1 Hz.

3.3. Rede Geral de Comunicações

A rede de sensores sem fios está integrada numa maior arquitectura de rede, que permite o acesso remoto à rede local de campo, através da *Internet*, tanto para a recepção de dados e sua consequente visualização numa interface gráfica de utilizador (GUI), normalmente um s*oftware* do tipo SCADA, como para o envio de mensagens de configuração para a rede, que permitem, por exemplo, a configuração de novo dispositivo sensor ou a alteração de parâmetros de funcionamento de um dispositivo instalado.

Esta rede global inclui, pelo menos, um dispositivo que comunica no mesmo protocolo de rede cablada de campo e que permite o acesso à *Web* (representado com o nome Interface *Web*, na Figura 33). Existem também com frequência outros sensores e unidades de interface que estão ligados diretamente a esta rede de campo, tal como se apresentará mais à frente.

O dispositivo referenciado na Figura 33 como Unidade Central consiste simplesmente num dispositivo que pertence ao *backbone* da rede de campo, e no qual toda a informação gerada e destinada à rede de campo se congrega. É o identificador deste dispositivo que é configurado na memória dos dispositivos de campo geradores de informação, sendo esses dados encaminhados para a interface *web*, já num protocolo que esta reconhece, como RS-232 ou *Ethernet*.

A interface *web* tem a responsabilidade de envio de dados de monitorização para um servidor *web* dedicado, podendo consistir em diferentes tipos de dispositivos, que obedecem a diferentes protocolos, de acordo com as características da instalação.

Como exemplo, o caso típico de uma instalação remota, sem acesso local à *web*, necessita que a interface *web* seja um dispositivo com capacidade de comunicação segundo um protocolo de rede móvel (ex. GPRS).

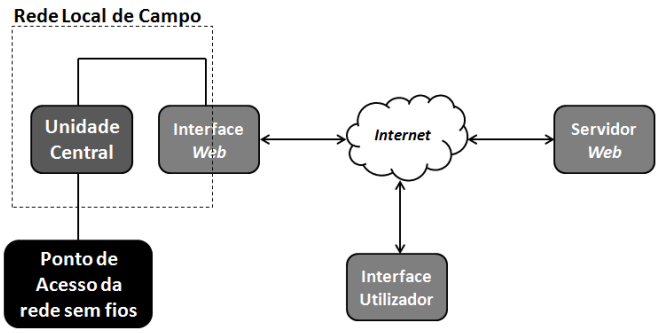


Figura 33 - Arquitectura Física da Rede de comunicações, e representações de fluxos de dados.

A arquitectura permite a ligação a diferentes redes de campo, que transmitem os dados provenientes dos dispositivos sensores para o referido Servidor *Web*, ao qual a interface de utilizador acede, também via *Internet*. Assim, com a *Internet* a ter um papel preponderante na

arquitectura geral da rede, é possível aceder a qualquer rede de campo e a dados guardados no Servidor a partir de qualquer interface de utilizador devidamente autenticada, via *web*, possibilitando um elevado nível de controlo sobre os dispositivos remotos instalados e sobre os dados de monitorização, em qualquer local.

Os dados de monitorização são guardados no servidor dedicado, havendo um acesso directo – no ponto de vista da transmissão de dados no sentido desta interface para a rede local – através da *web* à rede local de campo, e que diferentes interfaces de utilizador possam realizar todas estas funções.

O Ponto de Acesso da rede sem fios de baixa potência, analogamente aos protocolos de comunicações apresentados no anterior capítulo, consiste no Coordenador de rede. Em qualquer uma das redes apresentadas, baseadas em diferentes protocolos de comunicação, é nesta unidade que se concentra a gestão das funções de segurança, acesso à rede e interface com o *backbone* da rede de campo.

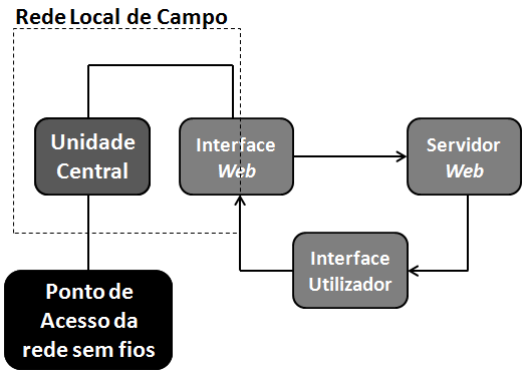


Figura 34 - Arquitectura da rede de comunicações – modo "*offline*".

Para além das funções de gestão e segurança de rede, a unidade central tem um papel preponderante no endereçamento de mensagens, visto que funciona como *gateway* entre a rede cablada de campo e a rede local sem fios, onde o endereçamento é feito com identificadores próprios. Este ponto será abordado novamente mais à frente, bem como a forma como possibilita uma simples e automática substituição de dispositivos e correcção de falhas.

Sendo esta a realização preferencial do sistema de comunicações, é igualmente possível um funcionamento "*offline*", onde a interface humana ou de utilizador está directamente ligada à interface web, bem como ao servidor, tal como apresentado na Figura 34.

Interessa neste ponto discutir a existência de um *backbone* cablado, no fundo o porquê de a rede não ser totalmente sem fios logo a partir da unidade central. A razão principal é a de que frequentemente existe um grande aglomerado de dispositivos nesta região, tipicamente com acesso a alimentação a rede eléctrica, para além de que o próprio ponto de acesso da rede sem

fios ter de ser alimentado permanentemente. Desse modo, e uma vez que é necessário alimentar todos esses dispositivos através de cabo, é lógico que também comuniquem através do mesmo cabo, levando a uma rede de campo. Outra razão que está como que "camuflada" nesta é a de que a utilização de uma rede cablada, mais reconhecida no meio industrial, permite a melhor penetração das redes sem fios que sobre aquela são suportadas nesse mesmo meio.

3.4. Rede de Campo

As comunicações através de redes de campo baseiam-se no protocolo *CANbus*, que por sua vez está baseado na norma CAN (do inglês *Controller Area Network*), que provém da área automóvel e que se apresenta como uma rede embebida, dada a alta densidade de dispositivos sensores e actuadores presentes num automóvel.

3.4.1.1. Rede e Endereçamento

O endereçamento sobre o protocolo *CANbus* é efectuado sobre identificadores de 64 bits, que permitem configurar os controladores de comunicações de cada dispositivo *CANbus* a receber ou filtrar uma determinada mensagem. Sob este esquema, todos os dispositivos recebem todas as mensagens colocadas no barramento *CANbus*, à excepção daquelas que forem filtradas por não corresponderem ao identificador atribuído. Neste contexto, é possível assim criar "máscaras" para um grupo de dispositivos, ou apenas para determinado dispositivo.

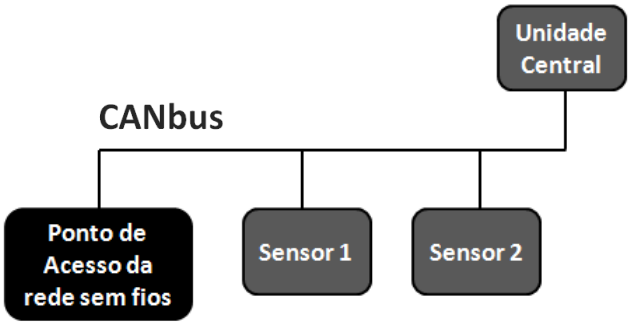


Figura 35 - Representação de um *backbone* de rede geral.

No tópico anterior é referido por várias vezes o *backbone* da rede de campo, pretendendo-se aqui referir a ligação central da rede de campo, que faz a ligação entre os diferentes dispositivos geradores de informação, ou que proporcionam a ligação a estes, e a já mencionada unidade central da rede.

A Figura 35 apresenta um *backbone* sobre o qual estão instalados dois sensores e uma *gateway* de acesso a uma rede sem fios, numa instalação típica, onde poderão ser colocados mais sensores, actuadores ou *Gateways* de acesso a sub-redes de outros protocolos. O protocolo

usado no *backbone* da rede é uma versão proprietária do protocolo *CANbus,* cujas características interessam para definir algumas condições fronteira dos protocolos sem fios.

Uma delas consiste no formato da trama do protocolo *CANbus*, que contém um espaço reduzido e fixo para dados.

ID emissor (1B)	**ID destino (1B)**	**ID *gateway* (1B)**	**Função / comando (1B)**	**Dados (argumento) (2B)**	**Dados (nº ordem) (2B)**	**Dados (extra) (2B)**

Figura 36 - Trama da mensagem *CANbus*.

A trama é constituída por 10 Bytes, sendo:

- 3 Bytes dedicados a identificadores:
    - Identificador geral do emissor da mensagem, que não tem de corresponder ao identificador do emissor da mensagem na rede *CANbus*;
    - Identificador geral do destinatário da mensagem, que uma vez mais poderá não corresponder ao do destinatário na rede *CANbus*;
    - Identificador geral do destinatário da mensagem dentro da rede *CANbus*, ou identificador da *gateway*, que tem sempre de pertencer à rede *CANbus* e será o destinatário mais próximo da mensagem: como exemplo, uma mensagem proveniente de uma unidade central e dirigida a um dispositivo sem fios ligado através do ponto de acesso da Figura 35 tem necessariamente de ter este dispositivo como ID da *gateway*;
- 1 Byte à função que será desempenhada, e que consiste no comando a executar pela unidade destinatária: veja-se que em caso de mensagens de dados provenientes de sensores e dirigidas à unidade central para posterior reenvio para o servidor, a função servirá como identificador do tipo de dados que foram transmitidos; por outro lado, aquando da transmissão de um comando para uma unidade de campo, como um sensor, a função corresponde ao comando que a unidade deverá implementar;
- 6 Bytes para dados:
    - Argumento, tipicamente usado para inserção de dados de sensores;
    - Número de ordem, que no caso de a mensagem ser de dados de sensores inclui um valor incremental;
    - Extra, também usado tipicamente para inserção de dados de sensores.

3.4.1.2. Camadas Física e DLL

A camada física do protocolo *CANbus* é baseada na norma ISO 11898-2, que define as camadas Física e de Enlace, também designada de CAN *high speed*, por possibilitar taxas de transmissão de dados até 1 Mbps, utilizada em todas as redes desenvolvidas.

O barramento CAN é constituído por dois fios diferenciais, designados de CAN *high* (CANH) e CAN *low* (CANL), sendo a sua condição diferencial importante para reduzir a interferência electromagnética externa sobre o barramento. A transmissão é efectuada com base em dois diferentes estados de tensão: o recessivo, em que ambos os sinais se encontram em alta impedância – com a diferença de potencial entre sinais CANH e CANL é inferior a 0,5V –, e o dominante, em que a diferença de potencial entre os sinais CANH e CANL é superior a 0,9V (68).

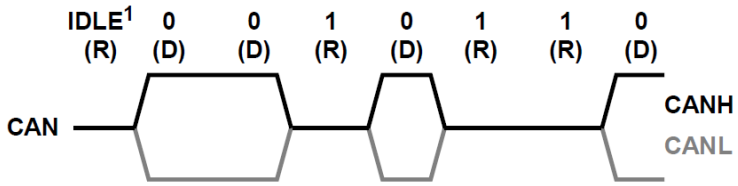


Figura 37 - Níveis de tensão dos sinais CANH e CANL, com representação dos bits lógicos correspondentes (68).

Na figura acima são representados os níveis de tensão dos fios CANH e CANL, e a sua correspondência aos bits lógicos 1 e 0. Como é aqui demonstrado, o bit lógico 1 é obtido a partir do estado recessivo, e o bit lógico 0 a partir do estado dominante.

O acesso à rede é efectuado com base no anteriormente descrito mecanismo CSMA-CA, em que cada dispositivo, antes de aceder ao meio, verifica o nível de tensão da rede. Caso um tempo limite configurado e considerado como seguro for ultrapassado sem verificação de actividade no barramento, o dispositivo inicia a sua transmissão. No entanto, é ainda possível que vários dispositivos tentem aceder no mesmo instante, podendo originar colisões. Por essa razão, após a transmissão de cada bit o dispositivo transmissor verifica novamente o nível de tensão na rede, verificando se é o mesmo que impôs. Caso seja diferente, é indicativo de que existe outro dispositivo a aceder à rede, e o dispositivo que transmitir a mensagem de maior prioridade ganhará o acesso à rede sem que a sua mensagem seja destruída por colisão. Ganha assim importância a definição de estado recessivo e dominante, uma vez que os bits iniciais de uma mensagem são referentes ao seu identificador, tendo as mensagens prioritárias um identificador mais elevado, ou seja, com maior número de bits dominantes (68).

A trama da mensagem *CANbus* é composta por 11 bits de campo de identificador, que poderão aumentar para 29 bits caso seja selecionada a opção *Extended Identifier*.

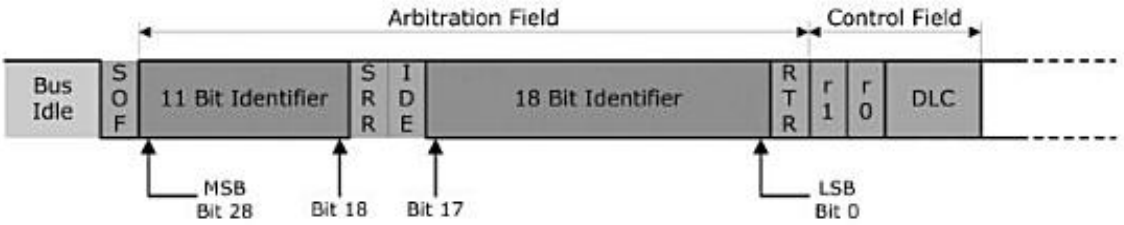


Figura 38 - - trama *CANbus* com Extended Identifier (69).

A utilização de *standard identifier* ou *extended identifier* é identificada através do bit IDE, sendo que um valor recessivo indica *extended* e um valor dominante indica *standard*.

Nas aplicações do presente trabalho foi utilizado o *extended identifier*, para que possa ser incluída na mensagem a seguinte informação:

Tabela 4 - Dados incluídos no campo *18 bit identifier*.

Função	Não utilizados	Emissor	Destinatário
1 B	2b	1B	1B

Tabela 5 - Dados incluídos no campo de dados.

Destinatário final da mensagem	Dispositivo	Argumento	Nº ordem	Extra
1B	2B	2B	2B	2B

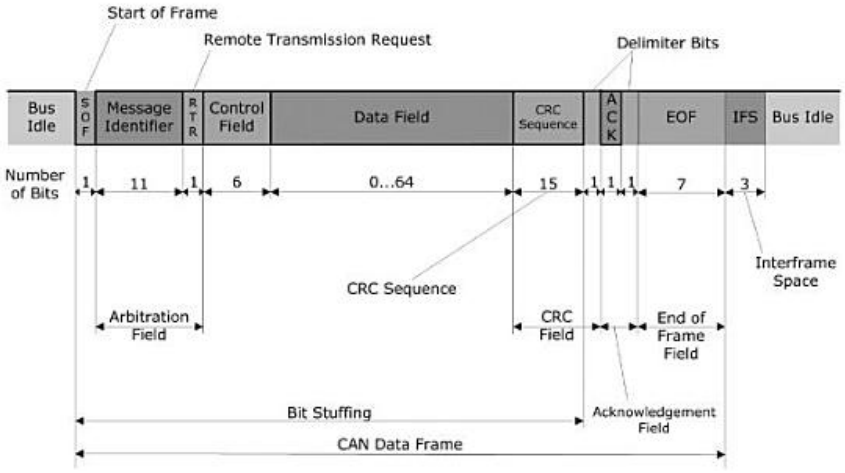


Figura 39 - trama completa *CANbus* com Standard Identifier (69).

O campo de *extended identifier* é utilizado para determinar se um dispositivo deverá aceitar determinada mensagem, seja por ser proveniente de um outro dispositivo do qual deverá receber mensagens ou se esta lhe é endereçada. É por essa razão que são configuradas máscaras na memória do dispositivo controlador *CANbus*, que mais não são do que filtros correspondentes aos dispositivos emissores dos quais poderão ser recebidas mensagens e ao próprio dispositivo, ao seu identificador. O modo estabelecido como comum consiste em aceitar mensagens de qualquer dispositivo, apenas filtrando aquelas que são dirigidas ao próprio.

3.5. Arquitectura da rede de sensores sem fios

A arquitectura da rede de sensores sem fios contempla a existência de sensores com diferentes propósitos, principalmente do ponto de vista da taxa de aquisição e transmissão de dados. Como foi visto no capítulo anterior, um dispositivo com uma taxa de transmissão de dados com um valor não muito elevado (como por exemplo 10 Hz) tem um consumo bastante superior a um dispositivo que se encontra num estado adormecido durante grande parte do seu período de funcionamento (ver Alimentação de dispositivos de baixa potência), e como tal esta taxa de transmissão poderá ser de tal forma elevada que já não é possível que o sensor seja alimentado com recurso a baterias.

Deste modo, e tendo em conta que muitas vezes existe a necessidade de altas taxas de aquisição e transmissão de dados, a arquitectura contempla esta dualidade, considerando que esses sensores terão de ser alimentados com recurso à tensão de rede – portanto cablada –, mas ainda prescindindo de um cabo para comunicações, e ainda assim mantendo parte da poupança referida no capítulo introdutório. Visto que a rede sem fios consagra a integração de sub-redes cabladas, esta designa-se de híbrida.

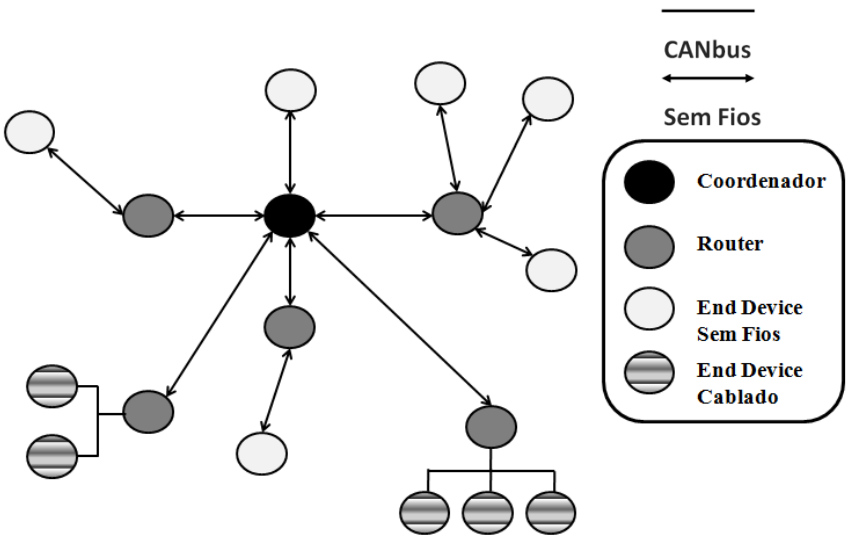


Figura 40 - Representação da arquitectura de rede.

Na Figura 40, a unidade identificada como Coordenador corresponde à unidade identificada como Unidade Central, na Figura 33 e na Figura 34.

A "hibridez" da rede permite que sejam instaladas em quaisquer *Routers* sub-redes cabladas de protocolos de rede de campo, sendo ainda possível instalar outras sub-redes sobre aquelas instaladas, usando a mesma metodologia de reencaminhamento de mensagens (apresentada no capítulo seguinte).

No entanto, as redes sem fios foram desenhadas tendo em vista apenas duas *gateways* sobre um mesmo troço *CANbus*, isto é, apenas dois níveis de distância da unidade central da rede no que toca a diferentes protocolos, tendo todas as instalações de campo sido feitas com esse preceito. O exemplo apresentado na Figura 40 é representativo da topologia típica de rede, não sendo assim – à partida – permitidas novas (sub-)sub-redes que partissem dos *End Devices* cablados, ainda que a arquitectura de rede, pelo seu protocolo de reencaminhamento de mensagens, o permita.

3.6. Os dispositivos

As diferentes unidades ou dispositivos que constituem a rede de sensores sem fios têm uma base física comum, diferindo naturalmente apenas na tecnologia utilizada – 433 MHz ou 2.4 GHz. Dentro de uma dada tecnologia, o módulo físico é o mesmo, sendo programado em fábrica com um *software* genérico, e configurado de acordo com o dispositivo no qual é inserido. Desta forma, existe um único módulo e um único código-fonte, que permitem diferentes configurações, de acordo com o tipo de dispositivo no qual o módulo é inserido. Os módulos desenvolvidos, do ponto de vista físico, serão apresentados em detalhe no capítulo Plataformas de Hardware desenvolvidas.

Do ponto de vista lógico, existem três diferentes dispositivos, o *Coordenador*, o *Router* e o *End Device*, sendo que um dispositivo é configurado como Coordenador previamente à sua instalação, através de uma mensagem de configuração que lhe é transmitida, pelo que o seu modo de fábrica (*default*) é *Router*.

3.6.1.1. Coordenador (CD)

O Coordenador cumpre as funções de estabelecimento de rede, que consiste nos passos de definição dos parâmetros físicos e lógicos de rede, e verificação da existência de outras unidades já ligadas na rede. O Coordenador tem ainda funções de gestão do acesso à rede e manutenção das tabelas de reencaminhamento de mensagens visto que faz, em qualquer tipo de instalação, a interface entre a rede de sensores sem fios e a rede cablada de campo. Apenas é permitida a existência de um Coordenador por rede, sendo que se um dispositivo Coordenador

verificar durante o seu processo de inicialização de rede que já existe um outro Coordenador no canal em que este "pretende" implementar a sua rede, descartá-lo-á e pesquisará outro canal para o fazer. Este dispositivo requer uma fonte de alimentação inesgotável (ou de grande capacidade, comparando com o seu típico consumo), visto que necessita de estar continuamente ligado.

3.6.1.2. *Router* (RT)

Esta unidade não tem a capacidade de inicialização de rede, tal como o Coordenador, podendo apenas fazer parte da rede a partir do momento em que esta já foi criada por aquela unidade. A partir desse ponto, permite a adesão à rede por parte de outras unidades e o reencaminhamento de mensagens de e para esses dispositivos e outros dentro do seu alcance, possibilitando assim o aumento da abrangência total da rede (considerando uma topologia emalhada). Uma característica importante dos *Routers* – também presente no Coordenador – é a de armazenamento de mensagens para dispositivos filhos que estejam em modo adormecido num dado momento. Tal como o Coordenador, também este dispositivo necessita de estar continuamente em modo ligado.

3.6.1.3. Dispositivo Terminal (DT)

Estes dispositivos (Terminais, ou *End Devices*, na nomenclatura inglesa) consistem nas interfaces físicas da rede, consistindo nos sensores com ou sem fios, propriamente ditos. As suas funções – do ponto de vista da rede – são bastante reduzidas, tendo apenas a capacidade de acesso à rede através de um (único) dispositivo *Router* ou Coordenador. Ver-se-á que em caso de falha do *Router* de acesso de um determinado DT, este iniciará o processo de pesquisa de um novo *Router* que lhe permita o acesso à rede.

3.7. Sensor inteligente

É com base neste dispositivo que se almeja qualquer desenvolvimento na área das redes sem fios de baixa potência, a capacidade de criar redes de comunicação com elementos com uma regulação de potência tal que possam suportar sensores, actuadores ou aplicações de localização, dando alguns exemplos, e ainda ser alimentados através de uma fonte com muito baixa corrente disponível (casa das dezenas de mA).

O que o dispositivo possibilita prende-se com os objectivos elencados no Capítulo 1, uma autonomia e uma dimensão tão reduzida, associadas à inexistência de quaisquer fios de ligação, que possibilitam a sua instalação em locais remotos, perigosos, dotados de movimento (ainda que constrangido) ou mesmo móveis.

Assim, é interessante apresentar quais os elementos que poderão constituir um sensor inteligente – focar-nos-emos apenas em sensores, que estiveram presentes em todos os sistemas desenvolvidos nesta dissertação, ao contrário de actuadores ou *tags* de localização – e os diferentes tipos de conformação que poderá tomar.

À luz da presente arquitectura, um sensor inteligente, tal como a seguinte figura apresenta, é constituído por:

- um microcontrolador (ou controlador) de aplicação, responsável pelo controlo de sensores, armazenamento e cálculo sobre os dados que deles são gerados, bem como pela passagem dos dados tratados para o controlador de comunicações;
- um microcontrolador (ou controlador) de comunicações, responsável pela ligação a uma rede sem fios – recepção de dados destinados ao controlador de aplicação e transmissão de mensagens provenientes do referido controlador para o seu destinatário na rede sem fios;
- sensores, sendo que são independentes do controlador de comunicações, mas que deverão ter um consumo baixo, suporte de modo adormecido e interface SPI;
- circuito regulador de alimentação, com baixas perdas na conversão de tensão a partir de uma bateria;
- uma bateria.

Através deste conjunto de componentes é possível criar dispositivos remotamente configuráveis que monitorizam processos ou equipamentos, com muito baixos consumos e, consequentemente, uma longevidade de operação na casa dos anos (dependendo da aplicação e da frequência de monitorização).

3.8. Escolhas protocolares

Toda a apresentação do capítulo 2 relativa a normas concorrentes para uma uniformização dos protocolos de comunicação para o meio industrial advém de um dos objectivos apresentados no capítulo 1, o da criação de uma solução compatível com soluções de outros fabricantes. Desta forma, esta auscultação e conhecimento dos protocolos para comunicações sem fios de baixa potência que permitem a almejada compatibilidade foram necessários, donde resultou a escolha do protocolo *ZigBee PRO*.

A principal razão associada a esta escolha prende-se com a facilidade de desenvolvimento de soluções industriais. Esta "facilidade" está associada ao acesso a ferramentas e a módulos de desenvolvimento, que vários fabricantes disponibilizam (70)(71), bem como ao acesso a módulos para integração em produto final.

A referida facilidade de desenvolvimento tem um resultado extremamente importante na concepção e desenvolvimento de um produto, o seu preço de fabrico e o tempo para obtenção dos seus componentes, que – grosso modo – no final resultam no seu custo. Assim, e tal como é possível compreender pelos dados apresentados nos diferentes subtópicos Desenvolvimento de Produto da secção Normas Concorrentes de Protocolos para Redes de Sensores sem Fios (WSN), apesar de fabricantes associados a todas as normas disponibilizarem *kits* de desenvolvimento, proporcionando assim facilidades na obtenção de um primeiro protótipo, à excepção dos protocolos *ZigBee*, *6LoWPAN* e *WirelessHART*, as normas apresentadas têm ainda tímidas presenças em distribuidores no que toca a componentes preparadas com o seu protocolo, para constituição de produtos.

Como tal, o *Time-To-Market* destes protocolos torna-se maior quando comparado com o seleccionado, uma vez que é necessário um maior tempo de desenvolvimento, no que toca à adaptação do *software* disponível ao hardware pretendido.

Poder-se-ia discutir que o protocolo *6LoWPAN*, tal como é referido no subtópico de Desenvolvimento de produto que lhe é dedicado, também tem tido grande aceitação por diferentes grupos de interesse da área das comunicações sem fios de baixa potência – e portanto módulos com este protocolo disponíveis no mercado –, sendo até uma norma que não depende de grupos empresariais mas sim da IETF, e que como tal apresenta valências interessantes em relação ao protocolo escolhido.

É também verdade que numa comparação entre os protocolos *ZigBee* e *WirelessHART*, é inegável que o último apresenta melhores condições de operação em ambiente industrial, demonstrando melhores qualidades de baixo nível, nomeadamente para ultrapassar distorção multi-caminho de sinal; melhores mecanismos de segurança, para impedir o acesso de terceiros aos dados; ou uma maior robustez relativamente a falhas (para além de maior capacidade de associação de novos elementos à rede) por todos os dispositivos – mesmo os terminais – serem capazes de reencaminhar dados (através do protocolo TSMP).

No entanto, a comparação deve ainda ter em conta os seguintes critérios: (i) o mercado em 2008 no que toca a soluções disponíveis e (ii) o preço que essas mesmas soluções apresentam.

Por um lado, a situação de desenvolvimento do protocolo *ZigBee* era superior à do protocolo *6LoWPAN*, não existindo nessa altura módulos preparados, ou mesmo o conjunto de especificações que hoje existem (72). Pelo primeiro critério, o protocolo *ZigBee* vingaria em relação ao protocolo *WirelessHART*, uma vez que àquela data não existiam os referidos módulos (capítulo 2, protocolo *WirelessHART*). Pelo segundo critério, e ainda que a diferença de preço apenas seja significativa relativamente para o protocolo *WirelessHART* (módulos *WirelessHART*

cerca de três vezes mais caros), esta diferença ainda se encontra dentro de um limite aceitável para uma solução destinada ao ambiente industrial, reflectidas no preço do produto final. Com a variedade de módulos para os diferentes protocolos existente nos dias de hoje (2012), o protocolo *WirelessHART* apresenta-se como o mais interessante e consequentemente a melhor solução para o mercado industrial. Associada a essa variedade existente, o teste que este protocolo tem vindo a sofrer (referido no capítulo 2, secção *WirelessHART*) também garante uma maior segurança na sua escolha.

Relativamente ao protocolo *ISA100.11a*, apesar de se tratar também de um protocolo desenhado para o ambiente industrial, a dificuldade que tem ocorrido nos últimos anos na sua completa passagem para o mercado, com soluções que o integrem e permitam uma inclusão em produtos finais, não permite sequer que se pondere a sua introdução num produto.

Apesar das actuais valências do protocolo *WirelessHART*, as opções tomadas devem ser avaliadas à luz da data na qual foram tomadas, e por daí ter-se optado pelo protocolo *ZigBee*. Assim, esta opção foi tomada tendo em conta aplicações com alta densidade de sensores e com baixa latência de dados, colmatadas pela alta taxa de transferência de dados – tendo em conta o panorama das redes de baixa potência –, de 250 kbps neste protocolo, e pela possibilidade de ligação de um alto número de sensores alimentados a bateria a um único *Router*, o qual está ligado aos seus pares – dispositivos FFD, na terminologia da norma *802.15.4* – sob uma rede emalhada, que traz uma maior robustez relativamente a falhas.

Ver-se-á mais à frente, no capítulo 4, de que forma as valências do protocolo *ZigBee* foram utilizadas na solução desenvolvida.

No entanto, uma das maiores fraquezas dos protocolos que comunicam na gama dos 2.4 GHz prende-se exactamente com o reduzido alcance que esta frequência proporciona, quando comparada com gamas de frequências comummente designadas de sub-GHz, na casa das centenas de MHz (tal como prova a Equação 2, de *de Friis*).

Daí, foi identificada a necessidade de ter uma solução que proporcionasse ligações entre dispositivos de maior alcance, e mais robustas em relação a ruído electromagnético, obstáculos ou mesmo atravessar paredes.

Na Europa, estas gamas de frequências resumem-se às já referidas ISM, dos 433 MHz (433.05-434.790 MHz) e dos 868 MHz (865-868MHz).

Por se tratar de uma gama de frequências mais baixas e como tal com um alcance superior, a gama dos 433 MHz foi escolhida para uma segunda solução, destinada a aplicações com menor densidade de sensores ou, mesmo que esta seja alta ou comparável a aplicações que à partida se

aplicaria uma rede baseada em *ZigBee*, onde existe elevado ruído electromagnético gerado pela maquinaria que os dispositivos instalados monitorizarão, ou mesmo grandes massas metálicas, que se tornam extremamente danosas para comunicações de baixo comprimento de onda, devido a interferências derivadas de reflexões.

Tendo em conta que, tal como foi apresentado na secção Arquitecturas de protocolos para redes sem fios, apenas existe um protocolo conhecido e apresentado ao mercado para esta gama de frequências, o *DASH7*, este seria à partida o eleito para a referida solução. No entanto, apesar do interesse que suscita e das possibilidades que pode proporcionar (ver subtópico DASH7), trata-se ainda de um protocolo em desenvolvimento, e que até à data de início de desenvolvimento desta solução protocolar ainda não tinha uma especificação base totalmente definida e portanto menos referências de código-fonte que permitissem a sua introdução numa solução industrial (73).

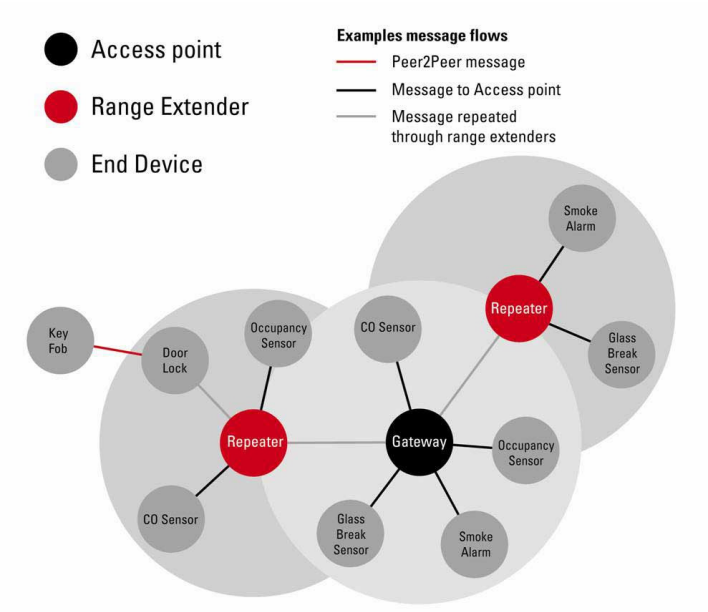


Figura 41 - Estrutura da topologia de rede *SimpliciTI*.

Assim, foi desenvolvido um protocolo *ad-hoc*, com base nas camadas física e de acesso à rede definidas pelo protocolo *SimpliciTI*, desenvolvido pela Texas Instruments (74). Sobre estas camadas foi implementada uma outra de *routing*, para permitir um maior alcance da rede e robustez.

3.9. Funcionalidades comuns aos dois protocolos desenvolvidos

3.9.1. Identificadores de rede geral

Como foi visto, a arquitectura sobre a qual ambos os protocolos desenvolvidos assentam consagra uma rede híbrida, tendo esta expressão o significado de que existem sub-redes redes

cabladas integradas na própria rede sem fios, apresentada na Figura 40. Para que tal seja possível, foi introduzido um esquema de endereçamento que é baseado nos identificadores da rede geral, sendo esta a que engloba o backbone (rede cablada), a rede sem fios e as sub-redes cabladas, conjunto que é apresentado na Figura 42.

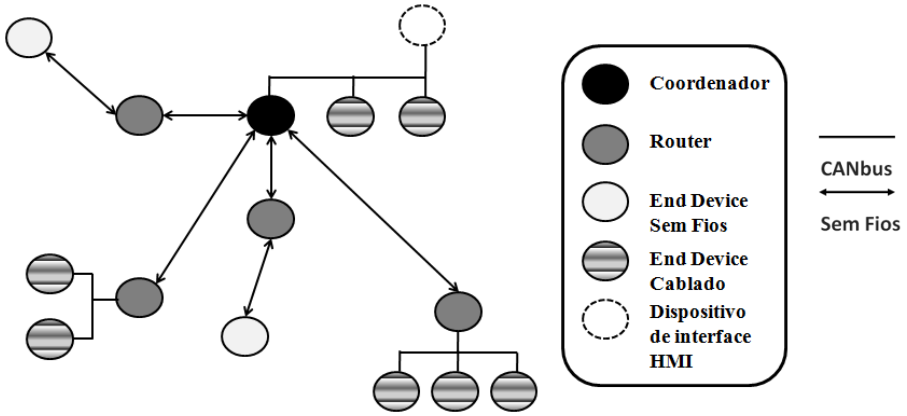


Figura 42 – Representação de uma instalação de rede de campo que inclui uma rede sem fios constituída por dispositivos terminais com e sem fios, *Routers* e coordenador.

Esta rede, onde existem pelo menos dois tipos diferentes de protocolo, tem identificadores únicos comuns a qualquer protocolo, de 8 bits, sendo esses identificadores atribuídos pelo instalador de rede, através de uma interface HMI, e transportados na camada de aplicação do protocolo.

3.9.2.Atribuição de endereços gerais

O processo para a atribuição deste identificador é simples: todas as unidades têm guardado em memória não volátil um número de série de 64 bits, que as identifica unicamente em todas as criadas pelo fabricante. Assim, quando uma unidade é ligada apenas é alcançável através deste número de série, uma vez que existirão outras na rede também sem identificador geral atribuído. Deste modo, após a instalação no terreno dos dispositivos e dos meios de ligação (cablagens e/ou unidades de ligação intermédia), o instalador introduz no *software* HMI que proporciona a sua interface com a rede o número de série da unidade em questão e o identificador geral pretendido, o que espoleta o envio de uma mensagem *broadcast*, com um argumento igual ao número de série da unidade em questão, colocando-a em modo de configuração, e consecutivamente uma mensagem com argumento igual ao identificador. São feitas outras configurações, mas de momento apenas nos interessa a relativa à atribuição de endereço.

A partir desse momento, a unidade é endereçável através do identificador geral, sendo que na rede *CANbus* o endereço CAN é igual ao identificador geral, e na rede sem fios, qualquer que seja o protocolo, existe uma tabela que relaciona todos os identificadores gerais de unidades que

são ligadas ao nó central da rede geral pela rede sem fios com os respectivos identificadores de rede sem fios.

3.9.3.Encaminhamento de mensagens em redes sem fios híbridas

O encaminhamento de mensagens é, em primeira análise, feito com base nos identificadores gerais de 8 bits, sendo na rede *CANbus* necessário que o dispositivo emissor indique o endereço geral do dispositivo destinatário e o endereço geral da *gateway* que poderá estar entre eles, na mesma forma que a apresentada para o endereçamento em rede *CANbus* (ver o subtópico Rede de Campo do presente capítulo – considerando os endereços de 8 bits, e não de 16).

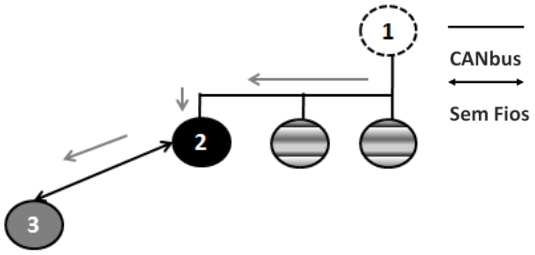


Figura 43 - Uma mensagem transmitida pelo dispositivo 1 para o dispositivo 3 deve indicar o dispositivo 2 como *gateway*, uma vez que 1 e 3 coexistem numa mesma rede geral mas em sub-redes de diferentes protocolos.

Tal como é apresentado na Figura 43, um dispositivo Coordenador (a preto) faz de *gateway* entre dispositivos pertencentes à rede de campo e à rede sem fios, sendo necessário para a rede *CANbus* que, em caso de o destinatário imediato não ser o final, seja introduzido o seu endereço – ou seja, a rede *CANbus* não tem qualquer protocolo de *routing*.

O mesmo tipo de esquema existe para o endereçamento sobre as redes sem fios, onde – caso a unidade emissora e destinatária estejam em sub-redes de protocolos diferentes – é necessário associar-lhe o endereço da unidade *gateway*, como é visto na Figura 44.

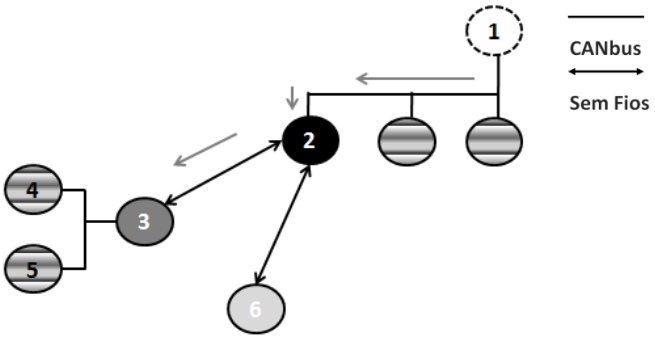


Figura 44 - Endereçamento sobre a rede *ZigBee*.

As *gateways* para a rede entre o *backbone* e as redes sem fios, como se referiu atrás, mantêm tabelas com os identificadores de todas as unidades pertencentes à rede de sensores sem fios, considerando que sub-redes cabladas que sejam integradas pela rede sem fios fazem parte da rede. A estratégia baseia-se em passar para as camadas inferiores a responsabilidade do reencaminhamento de mensagens. Na figura acima, os dispositivos 1 e 2 pertencem à rede *CANbus*, 2, 3 e 6 pertencem à rede sem fios e 3, 4 e 5 pertencem a uma sub-rede *CANbus*, integrada sobre a rede sem fios, 3 é um dispositivo *Router* e 6 um Dispositivo Terminal. Assim, uma mensagem endereçada para o dispositivo 4 a partir do dispositivo 1 é endereçada de 2 para 3, que pertencem à rede sem fios, uma vez que na tabela que associa identificadores gerais de rede com identificadores de rede sem fios (de camada de rede) e que é mantida no Coordenador (na Figura 44, a preto) o identificador geral de rede da unidade 4 está associado ao identificador de rede sem fios da unidade 3.

Tal associação é feita por uma verificação feita no Coordenador, a cada mensagem recebida da rede sem fios, do emissor na rede sem fios e do emissor original, que permite não só criar a entrada na tabela como uma actualização constante do identificador de rede sem fios.

Identificador geral de rede	Identificador de rede sem fios
0x03	0x1234
0x04	0x1234
0x05	0x1234
0x06	0x0123

Figura 45 - Exemplo de uma tabela de reencaminhamento de *gateway* central, referente à rede apresentada na Figura 44. Veja-se que o identificador de rede sem fios da unidade 3 se repete para as unidades 4 e 5, como se estivessem instaladas no mesmo dispositivo. Todos os valores estão em hexadecimal.

Este processo é importante porque, em qualquer dos protocolos desenvolvidos, o processo de atribuição de um identificador de rede sem fios a um dispositivo é variável, de acordo com a ordem de inicialização do dispositivo em relação a outros dispositivos na rede. Como tal, é possível que após uma reinicialização venha a ser atribuído um identificador diferente do inicial, o que provocaria uma desactualização da tabela de associações no Coordenador.

Uma vez que, a cada inicialização, um dispositivo envia para a unidade central da rede uma mensagem com informação de inicialização, esse processo permite que imediatamente após seja actualizada a tabela do Coordenador.

Deste modo, cada mensagem transmitida transporta na sua camada de aplicação os identificadores gerais de rede das unidades emissora e destinatária, sendo que aquando da "entrada" na rede sem fios a camada de aplicação lhe associará o identificador de rede sem fios, correspondente ao identificador de camada de rede. Este conceito é ilustrado na Figura 46.

Na figura acima, as mensagens são reencaminhadas para os dispositivos integradores que pertencem à rede sem fios, 4 e 7. Para a camada de aplicação da rede sem fios, entre o dispositivo 3 e os dispositivos 4 e 7 poderão estar n dispositivos (de acordo com a capacidade da rede em questão), sendo o reencaminhamento das mensagens através destes da responsabilidade da camada de rede.

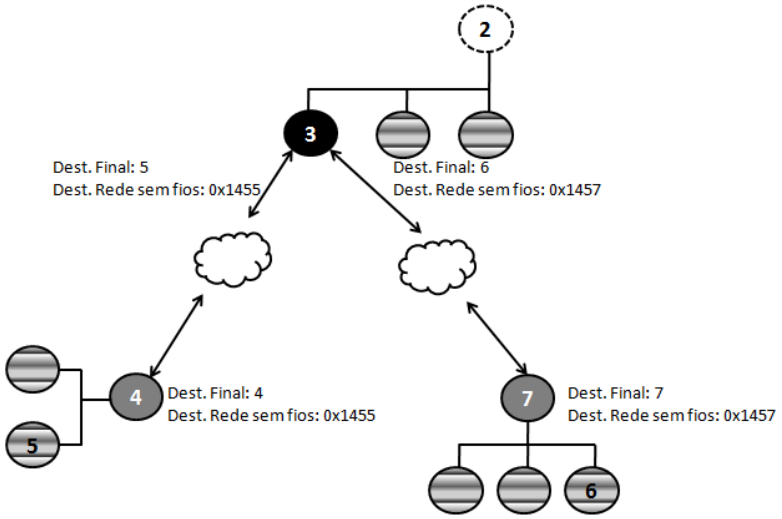


Figura 46 - Representação da transmissão de duas mensagens que têm como destinatários os dispositivos 6 e 5.

3.9.4.Esquema de *Acknowledgement*

Uma das funcionalidades importantes de um protocolo de comunicações – e que ganha ainda mais relevância quando se trata de um protocolo sem fios – é a utilização de mensagens de confirmação da recepção correcta de dados, conhecida como *Acknowledgement,* ou reconhecimento da recepção. Como exemplo, no protocolo *ZigBee* existem duas formas distintas, o *acknowledgement end-to-end* e o *acknowledgement next hop*. Na primeira situação, quando a mensagem chega ao seu destinatário final é enviado um *acknowledgement* para o dispositivo emissor inicial. Na segunda, é enviada uma destas mensagens a cada transmissão entre nós, mesmo que sejam apenas intermediários. A segunda opção é mais simples e menos consumidora de energia e de largura de banda, mas implica um compromisso no que toca à fiabilidade da rede, uma vez que o dispositivo emissor não poderá confirmar que a mensagem atingiu o seu destino, o que poderá levar a perdas de dados. Mas existe outra opção, a criação de uma funcionalidade intermédia, para além das funções do protocolo em questão, e que leve à geração de uma mensagem dirigida ao nó emissor, por parte de um nó intermediário, caso este não receba o *acknowledgement next hop* do seu destinatário intermédio.

No caso do *ZigBee*, pretendeu-se com a opção escolhida gerir este compromisso de fiabilidade com energia consumida, e como tal foi adoptado o esquema de *acknowledgement next hop*. Ver-

se-á na secção correspondente ao protocolo 433MHz que, salvo as óbvias características de mais baixo nível, se trata de um esquema igual.

Tendo em conta esta escolha e para uma maior fiabilidade dos protocolos, foi criada uma funcionalidade adicional, que "responsabiliza" cada nó pela mensagem que está a transmitir, tal como se fosse o seu emissor inicial. Esta estratégia assenta em três características: a da repetição da tentativa de comunicação, a manutenção em memória de mensagens sem *acknowledgement* (com a consequência da remoção de mensagens cujo *acknowledgment* foi recebido) e, adicionalmente, a detecção em hierarquias protocolares superiores da não recepção de dados.

Apesar de, na maior parte dos casos, em caso de falha do dispositivo configurado como próximo passo/salto (*next hop*) ser possível encontrar outro caminho, também existirão outros em que não existirá alternativa, por não haver outro FFD dentro do alcance do dispositivo que pretende transmitir a mensagem. Como tal, não há qualquer outra possibilidade de comunicação para o referido dispositivo, e é então imperativo que exista uma monitorização periódica de recepção de dados em elementos com maior proximidade à *gateway/*Coordenador de rede, com a qual o utilizador interage, sendo que neste caso essa função cabe ao *software* SCADA.

Uma vez que este *software* está fora do âmbito das redes sem fios deste trabalho, referir-se-á apenas que existe uma rotina que periodicamente verifica o refrescamento de dados recebidos de cada um dos elementos geradores de informação da rede (associada à sua taxa de geração de dados). Caso não sejam recebidos dados por mais tempo do que um valor pré-definido, gerar-se-á uma mensagem de alerta para o utilizador, para intervenção sobre o equipamento.

Visto que nem todos os sensores inteligentes têm como finalidade a captura periódica de dados mas também a detecção de eventos – sendo que o evento de interesse poderá ter uma periodicidade bem definida ou completamente aleatória – todos os dispositivos com funções de detecção de evento transmitem também uma mensagem periódica para o refrescamento da referida *flag* de verificação no *software* SCADA, para que seja reconhecível o seu bom funcionamento.

Uma nota sobre a fiabilidade da rede e a criação de funções para a sua melhoria fora do âmbito da rede sem fios: é necessário este tipo de estratégia porque em caso de falha permanente de um dispositivo poderá ser forçoso que haja intervenção de um técnico para substituição do equipamento. É um argumento forte que uma rede verdadeiramente fiável deverá incorporar estratégias que assegurem a manutenção de todas as ligações mesmo em caso de falha de um nó intermediário (*Router*). No entanto, existirão muitos cenários em que sensores isolados ou grupos de sensores estarão apenas dentro do alcance de um *Router*, sendo que a falha deste se traduzirá na desconexão daqueles da restante rede. Uma solução é a redundância de dispositivos

críticos – existindo sempre um ou mais dispositivos de reserva, que entram em funcionamento ao detectar a falha do principal –, definidos como aqueles que não dispõem de uma alternativa em termos de ligação à rede para um ou mais dispositivos. Em ambiente industrial, esta é uma opção relevante, e que deve ser tida em consideração. No entanto, escolheu-se não a considerar como a regra, uma vez que uma das principais condições-fronteira definidas no capítulo 2 foi a do preço das soluções.

Por outro lado, existem também as falhas de comunicação na tentativa de endereçamento dos dispositivos de campo, por exemplo ao transmitir mensagens de configuração. Nestes casos, se ocorrer a falha de recepção de *acknowledgement* mesmo após o número configurado de novas tentativas, é enviada uma mensagem partindo do dispositivo que está a tentar comunicar para a unidade central da rede, dando conta da falha daquele dispositivo / troço da rede.

Essas são as razões pelas quais se optou por ter uma rotina de monitorização do estado de ligação dos dispositivos de campo – sensores e *Routers* – para detectar possíveis falhas ou avarias. Esta questão implica, na óptica escolhida, uma desresponsabilização a cada transmissão com sucesso por parte do seu emissor, passando essa responsabilidade para o nó receptor, no caso de este não ser o destinatário da mensagem em questão. Por outro lado, e para que não ocorra perda de dados, cada nó a transmitir uma dada mensagem mantem-na em memória, podendo ser recuperada.

3.9.5.Formato da trama de aplicação

Na secção Rede de Campo do presente capítulo foi apresentada a trama do protocolo *CANbus*. A trama do protocolo *CANbus* foi adaptada e incorporada nos protocolos desenvolvidos, de forma a haver compatibilidade e simplicidade na transformação de mensagens entre protocolos.

Veja-se que apenas existem 6 bytes disponíveis (ver Figura 36) para dados em cada mensagem. Se é verdade que serão suficientes em grande parte dos casos, em que um sensor inteligente incorpora um ou dois sensores, como por exemplo de humidade e de temperatura, e que esses sensores gerarão dados de 2 B que serão transmitidos periodicamente para a unidade central, também existem casos onde será necessário transmitir uma maior quantidade de dados, como por exemplo no envio de uma série de dados para cálculos que requerem maior capacidade computacional, a executar em PC (p. ex. o cálculo de uma transformada de *Fourier*, necessária em algumas das aplicações desenvolvidas, que um dispositivo de maior memória e velocidade de processamento como um PC executará de forma mais rápida e fiável). Noutros casos, um sensor inteligente incorporará quatro ou mesmo cinco sensores, necessitando de distribuir esses dados por mais do que uma mensagem (p. ex., um dos sensores desenvolvidos incorpora um

acelerómetro triaxial e um sensor de temperatura, que correspondem efectivamente a quatro sensores – aceleração segundo cada um dos eixos e temperatura).

A primeira abordagem pensada para adaptar a trama das mensagens das redes sem fios ao nível da camada de aplicação foi de simplesmente manter o formato do protocolo *CANbus*, tendo todas as mensagens 6B de dados, 1B de função/comando e 2B de identificadores, prescindindo-se, tal como já foi mencionado, do identificador de *gateway*, ao encargo da camada de rede.

Por outro lado, esta imposição de um tamanho fixo na trama não é concordante com os critérios definidos inicialmente para os protocolos de rede sem fios, uma vez que não cumpriria com preceitos de baixo consumo, tanto para grandes como para pequenas quantidades de dados. Nos dois diferentes casos:

- um sensor inteligente com apenas um sensor, do qual recolhe dados de 2B com uma periodicidade definida. Poder-se ia considerar que o sensor guardaria os dados até ter uma quantidade que preenchesse a mensagem de 6B, mas é ainda mais interessante que a mensagem possa ter um tamanho variável, de acordo com a aplicação e com as necessidades de maior ou menor latência de dados da aplicação. Assim, poder-se-á configurar o tamanho máximo da mensagem para aquele tipo de dados, que corresponde a uma dada latência, medida em tempo com o número de períodos em que dados são guardados em memória;
- para um sensor inteligente com um ou mais sensores dos quais seja necessário reunir uma grande quantidade de dados – como é o caso do sistema desenvolvido para monitorização de maquinaria de transmissão de movimento com base em aceleração, em que pelo menos 1024 valores de aceleração de um dos eixos têm de ser adquiridos (que correspondem a 2048 Bytes) – seria necessário transmitir 512 mensagens (uma vez que cada mensagem apenas dispõe de 4B para dados de sensores, sendo os restantes dois para numeração/número de ordem). Assim, a alternativa será usar a capacidade máxima de uma mensagem disponibilizada por cada um dos protocolos desenvolvidos.

A questão por detrás da poupança obtida, ao ter um tamanho variável de mensagem de dados prende-se com:

- o gasto associado às diferentes fases do processo de transmissão de uma mensagem através da rede sem fios, que se repetem a cada mensagem transmitida (ver secções Protocolo *ZigBee PRO* e Protocolo 433 MHz, e respectivos tópicos Camada de Enlace / Acesso ao Meio);
- à quantidade de informação fixa numa trama correspondente às diferentes camadas protocolares, que acompanha cada mensagem transmitida.

Como tal, a adaptação da dimensão de mensagem aos dados que contém corresponderá, no contexto das redes sem fios de baixa potência, a uma poupança energética.

O formato implementado para a trama está apresentado na Figura 47.

Tamanho da mensagem (1B)	**ID Destinatário (1 B)**	**ID Emissor (1B)**	**Função / Comando (1B)**	**Dados (variável)**

Figura 47 - Representação da trama de aplicação dos protocolos desenvolvidos. Tanto o ID destinatário como o ID emissor correspondem aos identificadores de rede geral.

Repare-se que existe um campo para indicar o tamanho da mensagem. Essa opção deve-se ao facto de ambos os protocolos, como se verá, incorporarem campos de tamanho de mensagem na trama, ambos com 1B.

3.9.6.Comunicação com dispositivos "adormecidos"

Uma das questões vitais para as redes de sensores sem fios é a da gestão de energia dos dispositivos sensores, que são tipicamente alimentados a bateria, o que obriga a um racionamento da carga que contêm, que possibilite que os dispositivos se mantenham em funcionamento, apenas com uma bateria e sem recurso a manutenção, durante períodos de tempo bastante extensos, da ordem dos anos.

Como foi apresentado atrás, a tecnologia de baterias existente permite esta longevidade, mas ainda assim é necessária uma correcta definição das funções mais consumidoras de energia do dispositivo, como as comunicações com outros elementos da rede ou a recolha de dados dos sensores e consequentes cálculos associados.

Focando-nos no primeiro factor, associado às comunicações, é importante considerar os diferentes cenários de funcionamento dos dispositivos sensores, que obrigam a que executem comunicações com a rede:

- sensor inteligente para detecção de evento: mantém o(s) sensor(es) que contém em estado de *standby*, que lhe permita detectar uma alteração dos parâmetros que monitoriza, sendo que nesse momento transmitirá os dados referentes ao evento;
- sensor inteligente para monitorização contínua: periodicamente, sendo esse período um valor bem definido e configurado aquando da inicialização, o dispositivo adquire dados do(s) sensor(es) que contém, e transmite os dados adquiridos;
- sensor inteligente para monitorização contínua com período dinâmico: de acordo com os valores adquiridos – normalmente o dispositivo sensor calcula a sua média, aumentando o período de aquisição caso exista uma discrepância superior a uma

percentagem pré-definida em relação à média, e diminuindo o período caso a discrepância seja inferior – o dispositivo sensor adequa o período de transmissão de dados, diferindo este do caso anterior por o período não ser bem conhecido;

A abordagem seguida é a já desenvolvida no capítulo anterior, a de manter todos os elementos do controlador de comunicações – nome dado ao microcontrolador que contém o protocolo de comunicações de rede sem fios – em *standby* durante todo o seu funcionamento, saindo deste apenas por interrupção de um periférico ou entidade externa, podendo esta ser proveniente de:

- comunicação por parte do microcontrolador de aplicação, normalmente associada a dados previamente adquiridos, por qualquer uma das formas acima elencadas;
- relógio interno, pré-configurado para, periodicamente, fazer uma interrupção ao controlador de comunicações para este executar uma ligação à rede.

O primeiro caso é simples de compreender e executar, o controlador de aplicação adquire dados, reúne-os e processa-os de acordo com cálculos que resumem os dados numa média ou num valor eficaz, e transmite-os para o controlador de comunicações. Este irá sair do modo *standby*, iniciar o processo de transmissão de dados, de acordo com o esquema de acesso à rede, e transmitir os dados que recebe do microcontrolador de aplicação para a sua unidade pai na rede, que por sua vez os reencaminhará até ao destinatário.

O segundo caso acarreta uma maior complexidade, uma vez que não se destina à transmissão de dados do dispositivo para a sua unidade pai, que se encontra sempre em modo ligado, e portanto acessível. Esta opção serve exactamente para a transmissão de mensagens em sentido contrário à primeira, para que o Dispositivo Terminal possa receber dados provenientes de outros dispositivos na rede, apesar de se encontrar em grande parte do tempo em modo desligado/*standby*. Como tal, após uma interrupção do relógio interno, configurada para indicar que passou um período de acesso à rede, o controlador de comunicações:

- coloca em modo ligado o microcontrolador e o transceptor;
- inicia o processo designado de *polling*, enviando uma mensagem para a sua unidade pai, sendo essa mensagem um pedido para lhe serem enviadas mensagens pendentes que lhe tivessem sido encaminhadas desde o último *polling*;
- a unidade pai envia a resposta, que poderá ser nula, não existindo quaisquer mensagens, ou enviando as diferentes mensagens que lhe são encaminhadas, sendo que após recepção de uma mensagem por parte da unidade filho, esta é apagada da memória da unidade pai;

- as mensagens pendentes são guardadas em memória no controlador de comunicações e enviadas progressivamente (sob condição de resposta) para o microcontrolador de aplicação.

Enquanto um Dispositivo Terminal está em modo adormecido, não podendo assim receber dados provenientes de outros dispositivos da rede, a sua unidade pai armazena as mensagens que lhe são encaminhadas.

Este processo foi utilizado no protocolo *ZigBee*, que incorpora esse esquema, sendo descrito em maior detalhe na secção abaixo. No caso do protocolo 433 MHz, foi usado um esquema semelhante, para simplicidade do desenvolvimento do produto e também poupança de energia. Apesar de se tratar de um processo eficaz do ponto de vista da fiabilidade, uma vez que os dados são armazenados sempre em dispositivos que estão continuamente ligados (*Routers* e Coordenador), requer um consumo adicional por parte do Dispositivo Terminal, que terá de se ligar constantemente e executar o processo de *polling*, mesmo que não existam dados pendentes para si.

3.9.7. Interface Controlador de Aplicação – Controlador de Comunicações

O controlador de comunicações consiste num módulo independente, dotado pelo menos de um microcontrolador e uma unidade rádio (um transceptor rádio), sendo que o microcontrolador está programado para controlar o dispositivo rádio e para comunicar através de uma interface série com outro microcontrolador. Na arquitectura dos protocolos desenvolvidos, o controlador de comunicações é uma unidade separada de qualquer outra, sendo portanto necessário, em qualquer aplicação, que exista um controlador de aplicação (tal como apresentado no esquema da Figura 48), que executa as funções necessárias para cumprir uma dada aplicação (reencaminhamento de dados ou detecção de eventos) – seja o reencaminhamento de mensagens entre uma rede sem fios e uma rede cablada, a aquisição de dados de sensores ou a gestão da interface entre um *backbone* de uma rede industrial (cablado) e uma rede sem fios.

Como tal, o controlador de comunicações tem de conter um conjunto de instruções pré-programadas, para que possa ser facilmente configurado pelo controlador de aplicação, de acordo com as funções que deve cumprir. Estas instruções devem agrupar-se em funções que, sendo invocadas pelo controlador de aplicação, permitem a execução de tarefas complexas, como a ligação ou criação de uma rede, transmissão de dados, *reset*, pedido de dados de rede, etc.

Figura 48- Esquema de ligação entre dois dispositivos através de uma estrutura modular de controladores de comunicações e controladores de aplicação.

É com apoio neste conceito que foi escolhido o controlador de comunicações para o protocolo *ZigBee PRO*, uma unidade já desenvolvida e que contém o protocolo, e também que foi desenvolvido o protocolo proprietário com base no protocolo *SimpliciTI* para os 433 MHz. Sobre esta base, as funções executadas pelo controlador de comunicações a pedido do controlador de aplicação são:

- configuração de parâmetros, sendo a configuração uma função principal e o parâmetro a configurar uma função secundária dessa função principal, com pelo menos os seguintes parâmetros:
  - tipo de dispositivo na rede (p. ex. Coordenador);
  - potência de transmissão;
  - lista de canais para operação;
  - identificadores de rede;
  - configurações de reencaminhamento de mensagens (*Router*s);
  - configurações de acesso à rede (*End Devices*);
- pedido de ligação à rede ou criação de rede, no caso do Coordenador;
- transmissão de dados em mensagens de tamanho variável.

Por outro lado, o controlador de comunicações é responsável por, autonomamente, e do ponto de vista da comunicação com o controlador de aplicação:

- notificar e entregar mensagens destinadas ao controlador de aplicação;
- verificar a entrega de uma dada mensagem (segundo o esquema já descrito de *acknowledgement*), notificando o controlador de aplicação da entrega da mensagem, ou da falha desta;
- ligação periódica à rede para verificação de mensagens pendentes, no caso de ser um *End Device*.

A detecção de falhas na comunicação e consequente inicialização do processo de ligação à rede é, deste modo, da responsabilidade do controlador de comunicações, que detecta a falha através das mensagens de erro no *acknowledgement* recebido por parte do controlador de comunicações.

4. Tecnologias de realização

Tal como se apresentou no capítulo anterior, a arquitectura local da rede compreende uma rede cablada e uma rede sem fios sendo que, apesar de ter sido igualmente desenvolvida uma unidade de interface entre as duas, por ora apenas nos focaremos na rede sem fios, ponto central desta dissertação.

O protocolo de comunicação escolhido para constituir a estrutura central da rede foi o protocolo *CANbus – Controller Area Network* – que se trata de um protocolo de referência e com uma performance interessante para o ambiente industrial.

De acordo com as características ambientais e com as aplicações elencadas nos dois capítulos anteriores, dois sistemas foram desenvolvidos, em diferentes espaços temporais e com vista a diferentes aplicações. Apesar desta diferença, ambos partilham as características apresentadas no capítulo anterior.

Primeiramente, foi desenvolvida uma rede de sensores sem fios sobre 2.4 GHz, com base no protocolo *ZigBee PRO*, escolhido por se tratar do protocolo mais desenvolvido no mercado em termos de ferramentas de desenvolvimento disponíveis e de seguida pretendeu-se deter uma solução que possibilitasse um alcance de ligação maior pelo que, pelas razões apontadas no capítulo anterior, se desenvolveu um protocolo proprietário – sobre uma plataforma pré-existente, o protocolo *SimpliciTI* da *Texas Instruments* – sobre os 433 MHz.

4.1. Protocolo *ZigBee PRO*

Como foi explicado no capítulo anterior, o protocolo *ZigBee PRO* (2ª versão do protocolo *ZigBee*) foi o escolhido para integrar esta solução de instrumentação industrial. Este protocolo segue as definições de dispositivos acima apresentadas, Coordenador, *Router*, Dispositivo Terminal.

4.1.1. Camada Física

A camada física deste protocolo foi já apresentada, mas é possível escolher entre várias opções, que de seguida se apresentam.

De acordo com o módulo selecionado (e que é apresentado no capítulo seguinte), o protocolo possibilita a selecção de 16 canais entre as frequências dos 2.4 GHz aos 2.4835 GHz, a uma taxa

de transmissão de 250 kbps com os correspondentes -92 dBm de sensibilidade na recepção, e com modulação O-QPSK (ver Capítulo 2, IEEE 802.15.4, Camada Física (PHY)). Existia igualmente a possibilidade de selecção da gama dos 868 MHz, mas dado que esta frequência apenas tem um canal disponível e a uma taxa de transmissão mais baixa (100 kbps), optou-se pela gama dos 2.4 GHz.

O módulo seleccionado(71) permite escolher entre uma série de potências transmitidas, dos 4 e aos 20 dBm, tendo-se optado pelos 4 dBm para dispositivos terminais, visto é que para esta potência a corrente consumida pelo módulo é de 34 mA a 3,3 V (71), o que, tal como foi atrás discutido, é um valor considerável para dispositivos alimentados a bateria, cuja corrente máxima debitada poderá ir tipicamente até aos 50 mA a 3,3 V.

É também seleccionável o número de canais disponíveis, dentro dos 16 possíveis, e o modo de selecção do canal inicial. Esse canal poderá ser indicado, devendo fazer parte da lista de canais permitidos, ou omitido, ocorrendo um varrimento inicial de todos os canais da lista de permitidos, por parte do Coordenador, sendo escolhido aquele que tiver o nível RSSI mais baixo.

São portanto esses os parâmetros disponíveis para selecção:

Tabela 6 - Parâmetros seleccionáveis na camada física (PHY).

Parâmetro
Potência de transmissão
Lista de canais permitidos
Canal Inicial

4.1.2.Camada de Enlace / Acesso ao Meio

Tal como descrito no capítulo 2, a camada de acesso ao meio do protocolo *802.15.4* – que serve de base ao protocolo *ZigBee* – contempla um mecanismo de acesso ao meio designado de CSMA/CA. Foi consequentemente usado o seu modo *unslotted*, por ser concordante com as necessidades de baixo consumo definidas, ao não necessitar de uma sincronização periódica.

Em termos de encaminhamento de mensagens e identificação de dispositivos, é utilizado o endereço de 64 bits que provém do protocolo *IEEE 802.15.4*, o chamado endereço MAC, e que é único para cada dispositivo criado, sendo gravado em fábrica na memória do dispositivo. Não é portanto um campo editável, tal como o do endereço de rede, apresentado no subtópico Reencaminhamento de Mensagens.

4.1.3.Camada de Rede (NWK)

4.1.3.1. Topologia

O protocolo *ZigBee* permite a criação de redes emalhadas entre os dispositivos *Router*, e redes em estrela entre dispositivos terminais e *Router*s, que permitem o seu acesso à rede.

É também possível a criação de redes em árvore (ver Topologias de rede), mas foi selecionada a outra opção por permitir uma maior versatilidade ou robustez da rede, ao possibilitar que a rede se adapte a falhas dos seus elementos.

A topologia emalhada do protocolo *ZigBee* não é na realidade totalmente emalhada, sendo-o apenas entre dispositivos FFD (*Routers* e *Coordenador*), mas criando ligações em estrela entre unidades FFD e RFD, tal como está apresentado na Figura 49.

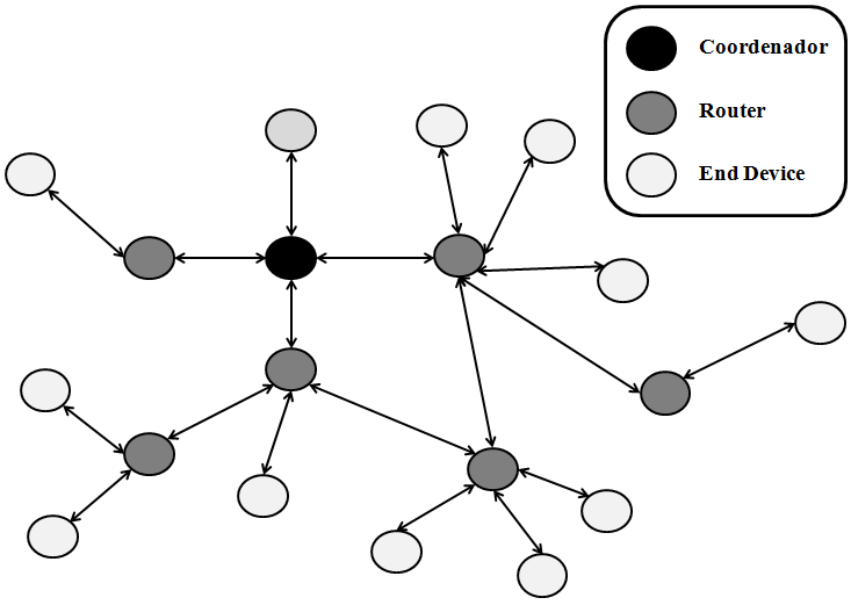


Figura 49 - Representação de uma rede *ZigBee* com topologia emalhada.

Este tipo de topologia é preferível em relação a uma rede em árvore por possibilitar uma maior resistência a falhas – robustez – mantendo caminhos possíveis mesmo em caso de falha de um dos nós da rede.

No caso apresentado na Figura 50, representativo de uma situação de falha de um nó da rede acima apresentada, a comunicação dos dispositivos terminais que se encontravam por este ligados mantém-se por via de outro *Router*, havendo uma redistribuição dos DT que lhe estavam associados.

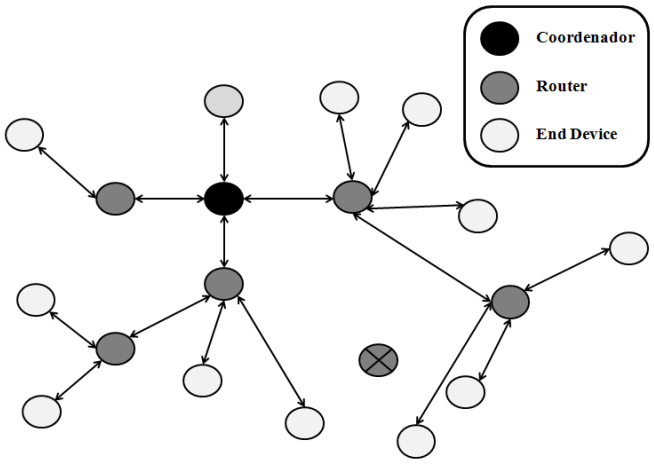


Figura 50 - Representação de uma rede *ZigBee* onde ocorreu falha de um dispositivo *Router*.

4.1.3.2. Reencaminhamento de Mensagens

O reencaminhamento de mensagens, ou *routing*, na rede *ZigBee* é feito com base nos endereços de rede, de 16 bits. Este endereço é único para um dispositivo numa determinada PAN, mas é atribuído pela sua unidade mãe – a unidade que permite o acesso à rede e atribui as constantes de rede – no momento da inicialização (ver Associação), pelo que é um valor volátil, guardado em memória RAM, e que poderá ser diferente caso o dispositivo sofra um *reset*.

O endereçamento poderá ser de diferentes tipos:

- *broadcast*, onde não existe um destinatário específico e a mensagem se dirige assim a todos os dispositivos da rede;
- grupo dos FFD, podendo a mensagem ser dirigida ao grupo de todos os FFD (*Full function devices* da rede, o conjunto de *Routers* e Coordenador);
- *unicast*, sendo a mensagem dirigida a um dispositivo com um endereço de rede e endereço MAC únicos naquela rede PAN.

O endereçamento das mensagens em si é feito com base no algoritmo "*Distance Vector*" (DV). O algoritmo consiste na determinação de uma "distância lógica" entre dois dispositivos, que estão inscritos nas tabelas de endereçamento dos diferentes FFD pertencentes à rede, sendo que a distância lógica corresponde ao número de dispositivos que se encontram entre o emissor e o receptor, através dos diferentes caminhos possíveis que as unidades ligadas à rede possibilitam.

Esta determinação ocorre a pedido (pelo dispositivo que pretende endereçar um dado destinatário, pela sua primeira vez), espoletando o processo de descoberta de rota, que consiste no *broadcast* de uma mensagem de pesquisa do dispositivo destinatário (75).

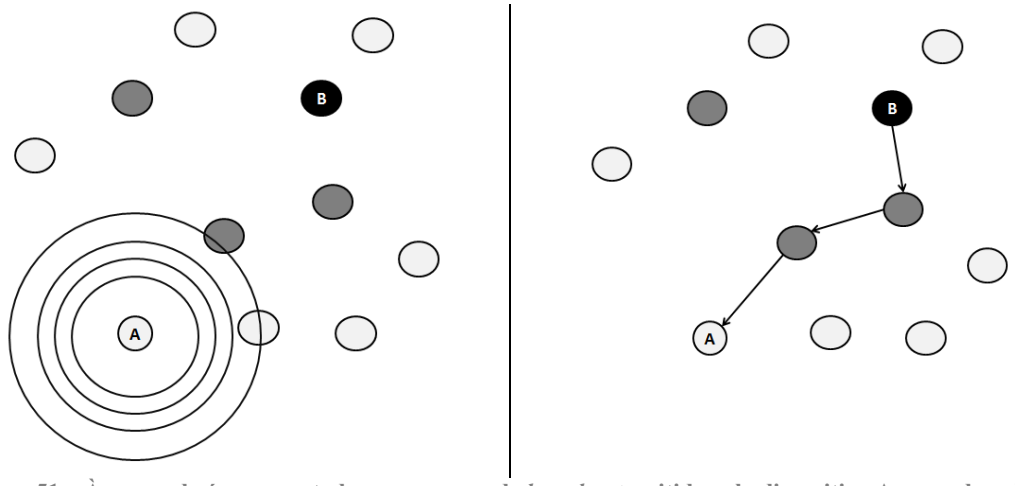


Figura 51 – À esquerda é representada a mensagem de *broadcast* emitida pelo dispositivo A, para descoberta da rota para o dispositivo B. À direita é representada a resposta dos dispositivos intermediários e de A, permitindo a actualização de tabelas de reencaminhamento e a transferência de dados entre os dois nós.

Sobre o algoritmo de base do protocolo *ZigBee* podem-se adicionar funcionalidades, para casos específicos de rede, e que reduzem principalmente a memória necessária nos dispositivos.

Uma delas é a que implementa a figura do "agregador", um caso típico em que todo o tráfego de uma rede é direccionado para um único dispositivo, que assim se denomina. Neste caso, não é necessário que todos os *Routers* mantenham as tabelas de reencaminhamento, mas que apenas tenham uma entrada com o agregador. Como tal, as mensagens transmitidas neste formato de *routing* a partir do agregador e dirigidas a qualquer outro dispositivo terão de incluir os endereços de todos os dispositivos que intermediam agregador e receptor (75).

Este tipo de esquema é denominado de *routing* de fonte ou de emissor, onde apenas no agregador é necessário guardar a informação que possibilita transmitir dados para o destinatário. Veja-se que este esquema é especialmente útil para redes grandes, onde as tabelas de reencaminhamento nos *Routers* – no formato DV – mais próximos do agregador têm um tamanho considerável quando comparadas com as dos restantes.

O *routing* de fonte parece cumprir exactamente as necessidades enumeradas para a arquitectura de rede definida, onde o Coordenador de rede funciona também como *gateway* para o exterior da rede, onde existirá uma interface de utilizador, e como tal todo o tráfego é direccionado. No entanto, várias razões levaram à escolha do esquema de DV.

Tal como foi referido nos capítulos 1 e 2, esta arquitectura de rede foi definida tendo em vista, em primeiro lugar, soluções de monitorização, onde não existem actuadores, e como tal todos os dados são enviados para uma única unidade, para posterior apresentação a um utilizador ou sistema de monitorização automático. Apesar disso, pretende-se que esta primeira solução venha a desenvolver-se para níveis maiores de envolvimento, onde as funcionalidades vão à

introdução de actuadores, sendo que o objectivo final será o de obter uma solução de automação, onde sensores e actuadores estão ligados entre si, sem intervenção humana.

Deste modo, foi escolhida a opção de manter uma rede com o esquema de reencaminhamento de DV, por:

- possibilitar a avaliação da sua performance, necessária para um cenário onde a matriz de dispositivos geradores e consumidores de informação na rede é mais complexa;
- apesar de o esquema de *routing* de fonte ser mais próximo de uma rede com um fluxo de informação como a actual, o facto de esta não ser de grande dimensão faz com que os *Routers* mais próximos do agregador/Coordenador não sejam tão sobrecarregados nas suas tabelas de reencaminhamento, perdendo-se assim a utilidade associada a este esquema.

4.1.3.3. Formação

Antes de descrever o processo de formação de rede *ZigBee*, é importante referir que esta é formada por um Coordenador de rede que, tal como já foi referido para a camada MAC, permite a configuração de certos parâmetros. Ao nível da camada de rede, é possível configurar a profundidade máxima da rede, ou seja, o número de nós entre um determinado dispositivo e o Coordenador – na imagem do lado direito da Figura 51, o dispositivo A está a uma profundidade de 3 em relação ao Coordenador.

É possível configurar também o número de dispositivos filhos que um FFD pode ter. Ao contrário do parâmetro anterior, este tem um maior interesse para a solução desenvolvida, uma vez que vários *Router*s na rede terão um tipo diferente de filhos, os dispositivos que estão ligados através da rede *fieldbus* local referida, identificados como dispositivos terminais cablados no subtópico Os dispositivos do Capítulo 3. Como tal, grande parte do seu tráfego de rede estará dedicado a estes dispositivos, cujo volume de dados é tipicamente superior ao das suas congéneres sem fios.

Daí, é interessante que estes *Routers* tenham o seu número de dispositivos filhos reduzido em relação a outros que são instalados apenas com o propósito de alargar o alcance da rede sem fios.

É também configurável o número de dispositivos filhos *Router* que um nó da rede pode ter, parâmetro este também interessante para a solução, pois permite repartir o tráfego de dados da rede por vários *Routers*. Considerando uma rede com uma área onde existe um maior volume de dados, devido ao facto de nessa área existirem equipamentos que necessitam de uma monitorização mais constante, com maior taxa de actualização de dados, e que poderia levar a

que todo esse volume de dados passasse num único *Router* da rede. Seria útil determinar o número de *Routers* associados a este, obrigando o tráfego a ser desviado por outra rota, tal como representado na Figura 52. Apesar de a configuração deste parâmetro não ser tão óbvia quanto a do anterior, poderá ser igualmente útil, tal como o parâmetro associado ao número de dispositivos filho, no dimensionamento e configuração da rede.

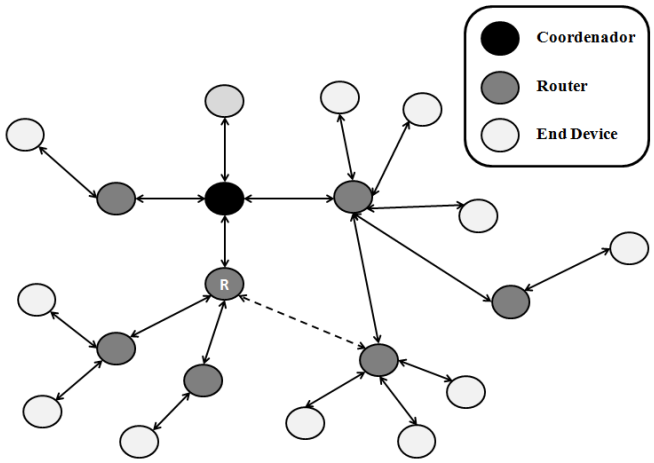


Figura 52 - Representação das possíveis associações ao *Router* identificado com R. A ligação a tracejado representa uma associação que poderia ter existido, caso o *Router* R não tivesse sido configurado para ter apenas dois *Router*s como filhos. Este conhecimento deve ser tido de antemão, para definição da rede na sua instalação.

Outros parâmetros de rede são configuráveis no Coordenador de rede: o canal em que a rede vai operar, já referida no subtópico Camada de Enlace / Acesso ao Meio e os PAN ID, simples e extensos, relativos aos identificadores da rede PAN. O primeiro consiste num valor de 16 bits, que pode ser configurado previamente na memória do Coordenador ou colocado em modo automático, sendo escolhido um valor que seja simplesmente diferente do escolhido para outras redes *ZigBee* presentes nas imediações. Este endereço é usado nas comunicações entre dispositivos *ZigBee* pertencentes à mesma rede. O segundo é necessário aquando da formação de rede, e poderá ser pré-definido, sendo o mais comum coloca-lo a zero, opção que leva a que seja igual ao endereço MAC do Coordenador, sendo uma forma de evitar que existam PAN ID extensos iguais (76). A utilidade deste segundo identificador prende-se com da tentativa de um dispositivo se ligar a uma rede, tendo duas opções:

- ligar-se à rede com PAN ID extenso pré-definido na sua memória, sendo tipicamente o endereço MAC do Coordenador;
- ligar-se à primeira rede detectada, sendo que o dispositivo vai guardar na sua memória o PAN ID extenso desta rede, caso venha a perder a ligação e seja necessário ligar-se novamente.

Foi escolhida a segunda opção, uma vez que traz simplicidade ao processo de ligação dos dispositivos à rede, e que as redes são previamente (à instalação no terreno) inicializadas, para configuração.

A colocação automática destes três parâmetros tem relevância no que toca à maior ou menor facilidade de instalação de rede em locais onde existem ou poderão vir a existir outras redes *ZigBee*.

No que toca ao canal escolhido, o Coordenador executa sempre uma "Detecção de Energia" do intervalo de canais que foi definido para operar. Este intervalo de canais pode incluir apenas um, vários, ou todos os canais cobertos pela gama dos 2.4 GHz da norma *802.15.4*. Adiante explicar-se-á o funcionamento deste processo de detecção, que de forma sucinta consiste na verificação da intensidade de sinal pré-existente nos canais permitidos. Poderá interessar ter um intervalo reduzido de canais para operação, para determinar facilmente o canal onde a rede estará a operar. No entanto, caso exista ruído num destes canais, que não seja reconhecido pelo instalador, o resultado será a formação da rede num canal ruidoso. Fontes de ruído comuns nos 2.4 GHz são outras redes que operam naquela gama do espectro electromagnético, especialmente redes *Wi-fi*.

Uma boa estratégia para previamente evitar canais *Wi-fi* é a de definir um intervalo que inclua os canais que não se sobrepõem a qualquer canal desta norma, sendo esse conjunto de canais representado a verde na Figura 53.

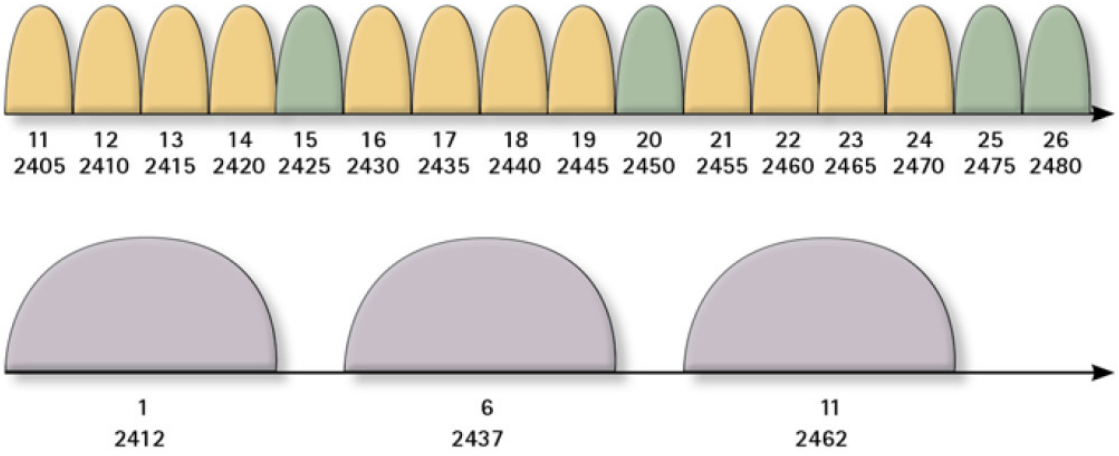


Figura 53 – Figura superior: distribuição de energia por canal *ZigBee*/*802.15.4*; figura inferior: distribuição de energia por canal *Wi-fi*, entre os 2405 MHz e os 2485 MHz. Os canais 15, 20, 25 e 26 (a verde) referentes ao protocolo *ZigBee* não se sobrepõem a qualquer canal *Wi-fi* (b/g). Fonte: (75).

Outra estratégia, que permite uma maior liberdade na definição do canal, é a simples definição de um intervalo que inclua todos os canais permitidos, e deixar o processo de detecção de energia reconhecer o canal mais "silencioso". Foi escolhida esta última estratégia como normal

(o modo *default* de funcionamento), podendo haver situações onde o ambiente tem reconhecidamente grande actividade comunicações Wi-fi, definindo-se para esses o intervalo mencionado.

O dispositivo Coordenador inicia a rede com as definições e opções acima descritas, de acordo com o seguinte processo (75):

1. selecciona o seu PAN ID extenso de acordo com o endereço MAC, e coloca o seu endereço de rede de 16 bits igual a 0x000;
2. selecciona o canal a operar, de acordo com o processo de detecção de rede, que contém os seguintes passos:
    a. "escuta" de cada canal presente no intervalo pré-configurado;
    b. de entre estes, selecção do canal com menor actividade, ou RSSI mais baixo.
3. Escolhe o PAN ID da rede, seguindo os passos:
    a. "escuta" o canal escolhido para detectar o tráfego de outras redes já ali instaladas;
    b. calcula com um gerador de números aleatórios o seu PAN ID, excluindo PAN ID iguais aos das redes que detectou.
4. inicializa o processo de aceitação de filhos, podendo adicionar outros dispositivos à sua rede, a partir desse momento.

4.1.3.4. Associação

A associação de dispositivos a uma rede só pode acontecer a partir do momento em que um Coordenador está devidamente inicializado naquela área, sendo portanto necessário que o processo de formação de rede esteja terminado e o Coordenador se mantenha ligado.

O processo consiste nos seguintes passos:

1. o dispositivo em inicialização pode seleccionar dois tipos diferentes de detecção de rede (77):
    a. *scan* passivo: o dispositivo "escuta" durante um período de tempo inicialmente determinado cada um dos canais pré-definidos no seu intervalo de canais;
    b. *scan* activo: o dispositivo envia para a rede um pedido de associação (*beacon request*), ao qual responderão todos os FFD dentro do seu alcance;
2. com grande probabilidade o dispositivo irá detectar dispositivos de diferentes redes, sendo que poderá ligar-se a qualquer uma delas, de acordo com um dos seguintes critérios, configuráveis em memória (76):
    a. liga-se à rede com melhor sinal (valor RSSI mais elevado);

   b. liga-se à rede com *extended PAN ID* igual ao que tem definido em memória (esta opção é ideal para não ocorrerem falhas aquando da associação, e tem em conta o endereço MAC (igual ao *extended PAN* ID) do Coordenador, conhecido previamente);

3. de seguida o dispositivo ainda terá de seleccionar o dispositivo pai (aquele que correrá o seu processo de aceitação de associação), sendo que escolherá o dispositivo com menor profundidade na rede (caso o Coordenador esteja dentro do alcance, ligar-se-á a este);
4. o dispositivo envia um pedido de ligação para o FFD seleccionado (camada de rede);
5. o FFD seleccionado responde ou não, sendo que apenas não responderá no caso de não estar a aceitar associações, seja por:
   a. não ter este modo activo desde a sua inicialização;
   b. ter entretanto desligado esse modo, por ter preenchido todas as vagas disponíveis (já mencionado no início do subtópico Formação);

   enquanto o dispositivo a tentar associar-se aguarda durante um período de tempo definido;
6. caso o FFD responda, gerará um novo identificador de rede de 16 bits, e enviará essa informação para o dispositivo a associar-se, junto com o PAN ID. Caso não responda, o dispositivo envia um pedido de ligação para outro dos FFD;

Tal como foi referido, é uma boa prática para a correcta formação de uma rede num ambiente onde se espera que coexista com outras a configuração dos dispositivos a associar com o *extended PAN ID* esperado, relativo ao endereço MAC do Coordenador. Este endereço ficará guardado na memória do dispositivo, sendo que o mesmo acontece depois de um dispositivo perder a ligação, possibilitando-lhe voltar a associar-se à mesma rede.

Nesse caso de perda de ligação, existe uma funcionalidade importante do protocolo *ZigBee*, que consiste na omissão de verificação da *flag* que determina se um FFD aceita ou não dispositivos filhos, por parte desse FFD. Esta função permite que, em qualquer caso (falha permanente do dispositivo pai), o dispositivo filho se possa associar de novo à rede.

4.1.4.Camada de Aplicação (APL)

Tal como foi referido no subtópico Camada de Aplicação (APL da secção *ZigBee*, Capítulo 2), este protocolo tem uma camada de aplicação, onde são definidas estruturas de aplicações tipo, sendo nomeadas algumas delas. Temos especial interesse, tendo em conta a área de aplicação, o perfil *Industrial Plant Monitoring*, um perfil público direccionado para a área da Monitorização Industrial. Os perfis consistem numa linguagem comum de camada de aplicação, que contêm entidades lógicas para dispositivos, conjuntos de comandos trocados entre esses dispositivos e o formato de dados que é trocado entre os dispositivos a cada comando. Os dispositivos terminais

poderão ser geradores ou consumidores de informação, sendo que estão agrupados em grupos de acordo com as suas funcionalidades (designados de *clusters*) e são associados através dos comandos; por exemplo, um sensor de temperatura enviará um comando de leitura de temperatura para um termóstato, onde este comando é de saída para o sensor e de entrada para o termóstato. Cada perfil, *cluster*, dispositivo, e comando tem um identificador de 16 bits.

A configuração destas associações é feita através da função de *binding*, sendo esta uma ligação lógica entre dois dispositivos ao nível da camada de aplicação, que tem a vantagem em relação a uma ligação de camada de rede de não necessitar de conhecer o identificador de rede do dispositivo para ser executada, mas apenas através do processo de aceitação por parte dos dispositivos em questão. Basta para isso implementar uma estratégia do tipo "botão", activando a aceitação de *binding* no dispositivo destinatário, e fazendo o mesmo no dispositivo emissor, mas neste caso activando o pedido de *binding*. Uma vez que apenas estes dois dispositivos estarão a aceitar a ligação, esta dar-se-á entre eles. Num cenário de monitorização pura, com um único destinatário, este poderá ter o modo de aceitação permanentemente ligado, sendo o modo de pedido activado em cada dispositivo que se inicia (78).

Após a primeira ligação a informação de *binding* é guardada em memória não-volátil do dispositivo, sendo recuperada caso algum dos dispositivos sofra um *reset*.

Como tal, a função de *binding* é especialmente útil quando não é conhecida a estrutura da rede, e são assim também desconhecidos os identificadores de rede.

No entanto, e como foi referido no capítulo anterior, a rede de campo para a qual foi desenvolvido este sistema tem já os seus próprios identificadores, retirando a necessidade de fazer ligações entre dispositivos sem conhecer os seus endereços. Tendo em mente o que foi descrito no subtópico Reencaminhamento de Mensagens, de que existe uma tabela de associação entre endereço de rede geral e endereço de rede sem fios no Coordenador de rede, não existirão situações, nos tipos de redes desenvolvidas, em que seja necessário efectuar ligações sem o conhecimento de endereços, uma vez que só existem ligações Coordenador – dispositivo e que o primeiro conhece em qualquer altura (à excepção da inicialização, que está prevista e é descrita no mesmo subtópico, sendo aí a identificação feita com base no número de série do dispositivo) o identificador de rede geral e de rede sem fios do dispositivo.

Deste modo, e tendo em conta que a rede cablada – presente tanto no *backbone* da rede geral como nas "ilhas" de sensores – é constituída apenas por camadas de mais baixo nível, que não suportam funcionalidades de rede ou de aplicação, foi tomada a decisão de prescindir destas funções da camada de aplicação por:

- não ser necessária a função de descoberta de dispositivo sem conhecimento do seu identificador;
- a rede cablada de *backbone* não suportar funcionalidades acima da camada de acesso ao meio;
- as redes sem fios desenvolvidas serem puramente de monitorização, e como tal quase a totalidade do fluxo de informação (à excepção de mensagens de configuração de dispositivos de campo) se processar no sentido dispositivo – Coordenador.

Como tal, e uma vez que numa rede *ZigBee* é necessário configurar todos os parâmetros de camada de aplicação, foi definido um único perfil, com um único *cluster* e com dois tipos de dispositivos: um para o Coordenador e outro para todos os restantes dispositivos. Assim, todo o endereçamento é feito ao nível da camada de rede, através dos endereços de rede de 16 bits.

Como foi atrás indicado, caso um dispositivo sofra um *reset* e lhe seja atribuído um identificador diferente do que tinha anteriormente, este enviará a mensagem de inicialização bem sucedida para o dispositivo central da rede geral, que passará pelo Coordenador, actualizando a tabela de endereçamento que associa endereço de rede geral e endereço de rede sem fios. Deste modo, não há o risco – sob este esquema – de um dispositivo ficar inalcançável devido a uma alteração no seu identificador.

4.1.5.Comunicação com dispositivos "adormecidos" na rede *ZigBee*

Tal como foi apresentado na secção Funcionalidades comuns aos dois protocolos desenvolvidos, a comunicação com dispositivos adormecidos na rede *ZigBee* é feita através de um processo de *polling*, em que o dispositivo adormecido é em qualquer caso um Dispositivo Terminal / *End Device*, com funções de sensor inteligente. O dispositivo adormecido tem um parâmetro em memória que é configurável, e que consiste no período de tempo que passa entre ligações à sua unidade pai.

Este processo foi já descrito na referida secção, podendo adicionar-se mais dois parâmetros configuráveis associados a este processo, e que consistem em:

a) para a unidade pai, no tempo máximo permitido para manter uma mensagem para uma unidade filho em memória;
b) para a unidade filho, no número máximo de processos de *polling* falhados por erro de comunicação com a unidade pai sem iniciar o processo de associação à rede.

O parâmetro descrito em a) tem uma restrição associada, a de não poder ser superior ao período de *polling* mais longo de um Dispositivo Terminal seu filho, correndo-se o risco de haver perda de dados devido à sua eliminação da memória da unidade pai.

Também o parâmetro b) deve ser configurado com conhecimento do seu impacto na performance da rede, uma vez que, caso seja elevado, poderá levar a que ocorram falhas de comunicação no sentido utilizador (ou unidade Coordenador) – sensor/dispositivo. Por outro lado, também não deverá ser igual pois sendo possível que ocorram falhas de comunicação, (devido à natureza ruidosa do ambiente industrial e distorção multi-caminho resultante da grande quantidade de massas metálicas), e portanto o sensor não deverá iniciar o processo de associação à rede à primeira falha, pois poderá não ter ocorrido qualquer falta do lado da sua unidade pai, e o processo de associação é altamente consumidor de energia, uma vez que requer a detecção de possíveis unidades pai, em diferentes canais, e a consequente troca de mensagens de associação com estas unidades. Como tal, deverá existir uma correcta definição deste parâmetro, de acordo com o ambiente em que o dispositivo se enquadra, e tipicamente considerando como aceitáveis 1 a 2 falhas.

Estas questões apenas afectam realmente só os dispositivos adormecidos, pois apenas para estes existe um processo de *polling*. Um FFD não necessita de *buffering* de dados na sua unidade pai, por estar constantemente em modo activo, e como tal permanentemente acessível para a recepção de mensagens. O mesmo acontece na transmissão de mensagens no sentido sensor – o Coordenador também têm o seu próprio processo de detecção de falhas, anteriormente descrito.

4.1.6.Segurança

A configuração de dispositivos da rede *ZigBee* permite dois modos de configurar a encriptação de dados. No formato mais "seguro", todos os dispositivos são configurados com a mesma chave de segurança, pelo que quando um dispositivo se associa à rede, já o fará com dados encriptados, uma vez que tanto esse dispositivo como o FFD que o associará conhecerão a chave.

No outro formato, apenas é necessário que o Coordenador conheça a chave, pelo que a associação de qualquer dispositivo à rede será feita através de uma troca de mensagens não encriptadas, sendo a chave de segurança atribuída pelo FFD ao dispositivo filho na resposta ao pedido de associação.

O primeiro modo apresenta-se como mais seguro, pois não há necessidade de troca de mensagens não encriptadas na rede, que permitem que dispositivos mal-intencionados tenham acesso a essa informação. Assim, cada dispositivo é configurado antes da sua instalação com a chave de segurança pretendida, pelo que todas as comunicações que ocorrem no terreno já se encontram encriptadas.

No protocolo *ZigBee*, a activação da encriptação de mensagens é feita através de uma mensagem de configuração, sendo a função utilizada a ZCD_NV_PRECFGKEY. A chave

estabelecida tem 16B, e quando a função de configuração é invocada ficará automaticamente activa. Para desactivar a encriptação, é necessário invocar novamente a mesma função.

Adicionalmente, para seleccionar o modo de funcionamento – se por difusão da chave de encriptação se por conhecimento geral – é necessário utilizar a função ZCD_NV_PRECFGKEYS_ENABLE, também utilizada através da função de configuração ZB_WRITE_CONFIGURATION, sendo que apenas tem um parâmetro associado, que quando colocado a 0 activa o modo de difusão e quando colocado a 1 activa o modo de conhecimento geral.

4.2. Protocolo 433 MHz

O protocolo 433 MHz foi desenvolvido para aplicações onde é necessário um maior alcance (em comparação como protocolo *ZigBee*) e maior resistência a interferência devida a reflexões em grandes massas metálicas no ambiente circundante.

Assenta num típico esquema em camadas, onde as camadas Física, MAC e Rede estão definidas com base no protocolo *SimpliciTI* da *Texas Instruments*, tendo sido introduzidas funcionalidades nas camadas MAC e de Rede para que o protocolo cumprisse com as necessidades. Sobre estas, foi introduzida uma camada de Transporte, para associação de mensagens de dados de sensores num mesmo pacote (tal como já tinha sido feito para o protocolo *ZigBee*, usando o mesmo esquema, que foi adaptado a este protocolo).

O *SimpliciTI* é um protocolo para redes de sensores sem fios, desenhado para ser usado em qualquer uma das bandas de frequência ISM, e com o mínimo de funcionalidades de rede, de maneira a ser bastante pequeno, em termos de espaço ocupado na RAM, e facilmente implementável.

Desta forma, sacrifica a flexibilidade que poderia ter um protocolo mais complexo, bem como a capacidade de suportar outras topologias de rede para além da estrela. É um protocolo interessante para aplicações onde existam vários sensores sem fios do mesmo tipo, e apenas um ponto de recolha de informação, dentro de uma área onde exista sempre ligação entre as fontes e o ponto de recolha de dados.

Analisando em maior detalhe, o dispositivo sobre o qual se desenvolveu o protocolo (79) integra no mesmo encapsulamento dois *chips*: uma unidade rádio e um microcontrolador, pelo que existem *drivers* preparados na memória não volátil do microcontrolador para o controlo da interface física entre as duas unidades, concretamente ao nível da SPI (*Serial Peripheral Interface*) que os liga, tal como está representado na Figura 54. Apesar de estas questões não parecerem importantes no que toca ao protocolo, elas influenciam-no, na medida que, segundo o

protocolo sob o qual se trabalhou, as camadas Enlace e Física encontram-se fundidas, numa camada designada de MRFI (*Minimal Radio Frequency Interface*). A relação entre este esquema e a ligação física entre os dispositivos constituintes do controlador de comunicações utilizado prende-se com o facto de as mensagens serem recebidas do rádio através da interface SPI já formatadas.

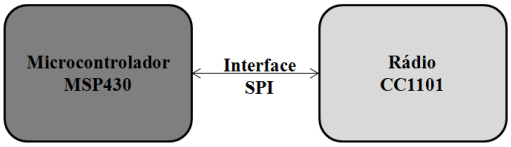


Figura 54 - Representação dos módulos constituintes do dispositivo CC430, base do protocolo 433 MHz.

O protocolo *SimpliciTI* consagra apenas ligações par-a-par, isto é, na realidade apenas possibilita redes em estrela, onde o nó central se relaciona directamente com todos os restantes dispositivos. Foi portanto necessário introduzir alterações no protocolo, para que seja possível introduzir *Routers,* não só para um ainda maior alcance da rede mas também para possibilitar ultrapassar barreiras físicas que impossibilitassem as comunicações. Como se verá nas subsecções Camada de Rede, alterações ao nível da camada de rede possibilitaram a selecção de unidades pai e o reencaminhamento de mensagens com base em *Routers*, numa rede deste tipo.

4.2.1.Camadas Física e de Enlace (Camada MRFI)

Apesar de ser uma camada única, pode-se considerar que a camada MRFI do protocolo 433 MHz está dividida em duas, uma vez que assenta numa base física, sobre a qual estão criadas funções (apesar de pré-programadas no dispositivo rádio), tal como é representado na Figura 55.

Figura 55 - Representação da Camada MRFI, que permite uma melhor separação das funções que congrega.

Quanto à camada Física, foi estabelecida durante o desenvolvimento do presente trabalho, uma vez que o protocolo *SimpliciTI* se destina a qualquer dispositivo controlador de comunicações, que poderá operar em qualquer frequência. Desta forma, a base física escolhida estabeleceu-se na gama dos 433 MHz, como já foi referido, mais concretamente em torno do canal 433,92 MHz. Em torno deste canal são definidos outros 4 canais, com um espaçamento de 250 KHz, pelo que a gama coberta pelo rádio é na verdade entre os 433,42MHz e os 434,42MHz, existindo um total de 5 canais. A taxa de transmissão de dados é de 100 kbps, sendo que o dispositivo rádio permite taxas de transmissão entre 1kbps e 500 kbps. Foi escolhida esta taxa por estabelecer um bom compromisso entre velocidade e sensibilidade, uma vez que as duas são

inversamente proporcionais. À taxa escolhida corresponde uma sensibilidade de cerca de -98 dBm, sendo que para uma taxa de 250 kbps corresponderia uma sensibilidade de -92 dBm, consideravelmente inferior. Uma vez que este parâmetro é bastante importante na comunicação entre dois dispositivos, afectando o alcance, principalmente para dispositivos com antenas de menor dimensão (e consequentemente ganho), tais como são os sensores inteligentes desenvolvidos. A questão da relação entre alcance e os parâmetros físicos do dispositivo será novamente aflorada no capítulo Plataformas de Hardware desenvolvidas.

O esquema de modulação usado é o 2-GFSK, sendo aquele permitido pelo dispositivo rádio selecionado.

Todos estes parâmetros são estáticos, estando guardados na memória não-volátil do dispositivo e não sendo assim possível alterá-los por configuração inicial do dispositivo. Pretende-se com esta opção libertar o instalador de questões de muito baixo nível, simplificando a instalação, ao mesmo tempo que são criadas condições para a reconfiguração automática das questões mais vitais, como o canal de operação. Este ponto será desenvolvido em maior detalhe no subtópico seguinte, aquando da descrição da funcionalidade *Frequency Agility*. Relativamente à potência de transmissão, que afecta directamente o consumo do dispositivo, foi selecionada a potência mais alta possível sem comprometer as baterias usadas (pontos a desenvolver no capítulo Plataformas de Hardware desenvolvidas), uma vez que uma potência de 10 dBm corresponde a uma corrente consumida pela unidade rádio de 28,8 mA, perfeitamente dentro da corrente máxima debitável de uma bateria da tecnologia Cloreto de Tionilo ($LiSOCl_2$).

O tamanho máximo permitido para uma trama é de 255 B, tendo-se optado por um tamanho variável de trama, mais adaptado às diferentes aplicações em que o protocolo será implementado, podendo ser necessário transmitir 1B ou vários KB de dados, que terão obviamente de ser seccionados.

Relativamente à "Sub-Camada de Enlace", que compreende a função de acesso ao meio, é implementado também o esquema de *CSMA*, tal como no protocolo *ZigBee*. O dispositivo rádio implementa este esquema automaticamente, sendo apenas configurável o número de tentativas para aceder ao meio, um valor que indica o número máximo permitido de sucessivas falhas por parte do dispositivo rádio para aceder ao meio, até "desistência" (a forma como esta desistência é tratada é apresentada no subtópico Camada de Rede, uma vez que é tratada por essa camada de nível superior a esta).

O formato da trama implementado pelo protocolo consagra na sua base 12 diferentes campos, sendo que a área dedicada à camada de aplicação ainda se subdivide, de acordo com a função em questão (ver Aplicações de rede).

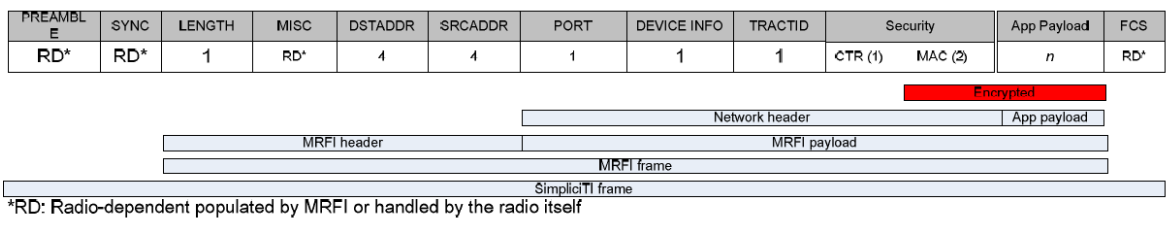


Figura 56 - Formato da trama *SimpliciTI*, implementado no protocolo 433 MHz.

Tabela 7 - Legenda da Figura 56.

Preamble	Preâmbulo da mensagem, inserido pela unidade rádio (1B)
Sync	Byte de sincronização, inserido pela unidade rádio (1B)
Length	Tamanho da mensagem (1 B)
MISC	Parâmetro de rádio, inexistente no rádio seleccionado
DSTADDR	Identificador do dispositivo destinatário (4B)
SRCADDR	Identificador do dispositivo emissor (4B)
Port	Porto para o qual a mensagem é transmitida (qual a aplicação de rede responsável pela mensagem)
Device Info	Este campo contém informação sobre o dispositivo emissor e a mensagem: se se trata de um *acknowledgement*, se é uma mensagem normal que requer *acknowledgement*, qual o tipo de receptor (se se trata de um ED adormecido o dispositivo sempre ligado) e qual o tipo de dispositivo do emissor (AP, ED, *Router*).
Tract ID	Identificador da ordem da mensagem – valor incrementado a cada mensagem, para evitar a recepção de mensagens duplicadas
Security	Campos de segurança (ver aplicações de rede)
App Payload	Espaço para dados de aplicação (ver aplicações de rede)
FCS	*Frame Control Sequence* – no caso do rádio selecionado um CRC de 16 bit

Esta é a base da camada MRFI, sendo as restantes funções de interface directa com o dispositivo rádio, responsável pela camada física e de acesso ao meio (referenciada como "Sub-Camada de Enlace").

4.2.2.Camada de Rede (NWK)

4.2.2.1. Dispositivos

Esta camada possibilita uma ligação entre os diferentes nós da rede, numa topologia tipicamente em árvore. A rede é normalmente em árvore, existindo os seguintes tipos de unidade:

- *Access Point* (AP): é a unidade que define os parâmetros de rede, e que recebe posteriormente os pedidos de ligação dos *End Devices* e *Routers*. Detém as funções de:
    - criação de rede;
    - permissão de acesso à rede ;
    - armazenamento de mensagens destinadas a *End Devices* em modo adormecido;
    - *routing* entre outros tipos de unidades;
- *End Device* (ED): um dispositivo que normalmente se encontra desligado, não tendo portanto capacidades de *routing*. Funciona como uma unidade geradora de informação, que posteriormente é enviada para o AP;
- *Router/Range Extender*: tal como está definido no protocolo *SimpliciTI*, é um dispositivo que recebe dados de todas as unidades dentro do seu alcance e os retransmite (é portanto um repetidor puro), mas foram feitos acrescentos às suas funcionalidades de forma a poder cumprir funções de um verdadeiro *Router*, para poder cumprir as necessidades atrás definidas (ver Os dispositivos).

Está definido na arquitectura de base dos protocolos desenvolvidos que a rede deverá ser híbrida, possibilitando a introdução de "ilhas" de redes cabladas, e ainda o reencaminhamento de mensagens de dispositivos mais distantes do ponto central da rede por parte de outros dispositivos, designados de *Routers*.

O protocolo *SimpliciTI*, tal como está definido, não possibilita estas duas funcionalidades de uma forma eficiente, uma vez que os dispositivos *Range Extender* são simples repetidores, que apesar de possibilitarem o reencaminhamento de dados o fazem para todas as mensagens que recebem, o que diminui a largura de banda disponível, ao introduzir uma maior repetição de mensagens na rede.

Como tal, o protocolo foi alterado de maneira a que um *Range Extender*, a partir deste momento designado de *Router*, tenha algumas funcionalidades de base, que lhe permitem:

- a associação à rede através de um AP, fazendo assim parte daquela rede sem fios (associação como unidade filha, obtenção de identificador de rede próprio, obtenção de identificador geral de rede);
- a disponibilização da função de associação a outros dispositivos;
- através do identificador próprio, transmissão de mensagens com origem em si, provenientes dos dispositivos de rede cablada que integra na rede sem fios;
- o reencaminhamento de dados das suas unidades filhas.

Estas características foram adicionadas na forma de blocos funcionais ao esquema do protocolo *SimpliciTI*, em que um *Range Extender* não chega a fazer parte da rede, sendo apenas um

dispositivo que retransmite as mensagens (quaisquer que sejam, num determinado canal) que recebe, tal como é apresentado na Figura 57.

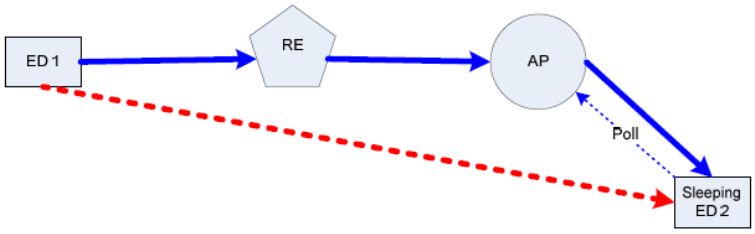


Figura 57 - Representação da ligação de um *End Device* a outro através de um *Range Extender* e de um *Access Point*, numa rede *SimpliciTI*. Fonte: *Texas Instruments*.

4.2.2.2. Topologia

Como foi apresentado anteriormente, o protocolo *SimpliciTI* possibilita apenas ligações par-a-par, o que implica que a sua forma mais complexa consiste numa rede em estrela, em que todos os dispositivos se emparelham com um nó central, que consiste num *Access Point*.

Com as funcionalidades adicionadas aos dispositivos *Range Extender*, o protocolo passou a permitir uma rede em árvore, no formato apresentado na Figura 58.

A topologia em árvore do protocolo 433 MHz permite um máximo de duas ligações de distância do nó central. Esta opção será desenvolvida em maior detalhe no subtópico seguinte.

No que toca à topologia em si, esta permite a ocupação de uma área maior em comparação com uma rede em estrela, sem implicar uma maior ocupação de largura de banda com a transmissão de mensagens de gestão de camada de rede, como a manutenção de tabelas de reencaminhamento e a procura de caminhos.

Por outro lado, em comparação com uma rede emalhada, torna-se um esquema mais inflexível, que não permite a falha de dispositivos intermédios, com funções de reencaminhamento de mensagens. No entanto, e uma vez que o protocolo assenta sobre uma gama de frequências mais baixas – em comparação com os seus congéneres nos 2.4 GHz –, o alcance que estas frequências permitem joga um papel importante, ao possibilitar que na condição de falha de um *Router*, o *End Device* que dele dependia possa reiniciar o processo de associação à rede, tentando consegui-lo através de outro dispositivo com a função de associação ligada, que se encontre dentro do seu alcance alargado (as questões ligadas ao alcance e à gama de frequência foram tratadas no Capítulo 2, sendo os valores obtidos com as soluções desenvolvidas apresentados no Capítulo 6). Como tal, o *handicap* que a topologia em árvore poderia implicar é compensado por um maior alcance, que permite diferentes associações entre dispositivos.

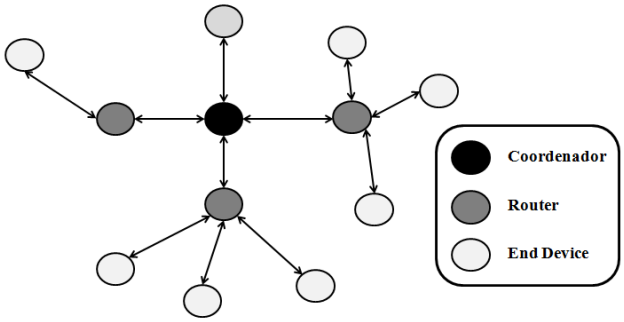


Figura 58 - Topologia em árvore do protocolo 433 MHz.

4.2.2.3. Aplicações de rede

Apesar de serem apresentadas como funcionalidades de aplicação (ver Figura 59), as diferentes funções que o protocolo consagra cumprem na verdade propósitos de rede, pelo que são apresentadas neste subtópico. O protocolo consagra 5 diferentes funções úteis à criação e manutenção de uma rede, permitindo diferentes topologias, podendo-se mesmo prescindir de um Coordenador de rede. As funções são as seguintes:

- *Ping* – verificação do estado de um dispositivo (ligado ou desligado da rede), através de uma mensagem de "*ping*";
- *Link* – ligação protocolar/lógica entre dois dispositivos de uma rede, tipicamente um sensor e a unidade AP (se bem que poderá utilizar-se entre quaisquer outros dispositivos);
- *Join* – associação de um dispositivo à rede, através de um *Access Point* ou de um *Router*;
- *Frequency Agility* – alteração do canal da rede, por verificação de ruído no actual;
- *Security* – funções de encriptação de mensagens, para evitar a sua intercepção por dispositivos não autorizados (definido pelo AP);
- *Management* – habilita um AP a alterar parâmetros aplicacionais num *End Device*, mas tem como principal função o processo de *sleep*/*poll* por parte de um ED. É esta aplicação que lhe permite fazer o *polling*.

As "aplicações" acima sucintamente descritas possibilitam criar as funcionalidades base de rede: reencaminhamento de mensagens, formação de rede, associação de novos dispositivos, segurança e comunicação com dispositivos "adormecidos". Relativamente à aplicação *Ping*, tem como função a transmissão de uma mensagem para determinado destinatário, que responderá com a mesma mensagem, sendo útil para detecção de unidades AP a operar num canal e para a recuperação de mensagens para ED, usando a função *Ping* para transmitir uma mensagem à sua unidade pai.

A aplicação *Link* consiste naquela que permite que uma ligação par-a-par de aplicação seja criada. Possibilita que dois dispositivos sejam emparelhados, sendo que existe um dispositivo emissor do pedido de *link*, feito com base no identificador do dispositivo receptor. É feito com base num *link token*, enviado pelo emissor, e estabeleceu-se que é feito a partir de um dispositivo filho para o seu dispositivo pai, imediatamente a seguir ao *Join*, ou a função que permite a associação à rede, sendo que o dispositivo receptor do pedido de *link* é aquele que permitiu a associação. O *link token* do dispositivo filho deverá ser igual ao do dispositivo pai, pelo que todos os dispositivos na rede têm o mesmo *link token*.

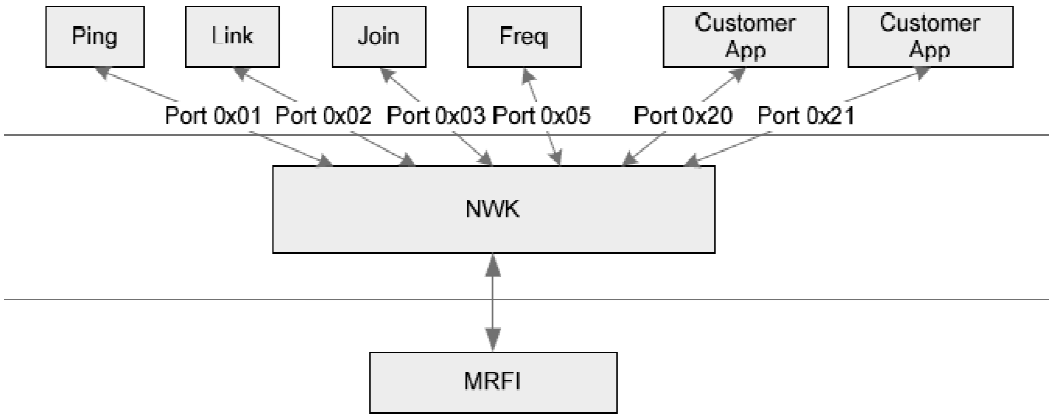


Figura 59 - Camadas do protocolo *SimpliciTI*. Fonte: *Texas Instruments*.

A partir do momento em que dois dispositivos têm um *link* entre si, pode-se associar uma aplicação a esse mesmo *link*. Uma vez que o protocolo 433 MHz tem como função apenas o controlo de comunicações, estando todas as funcionalidades de aplicação num microcontrolador dedicado, a aplicação dada aos *links* baseia-se apenas na recepção e transmissão de dados.

O número máximo de *links* foi definido como o número máximo de dispositivos filho que o dispositivo pode ter mais um, uma vez que *Routers* terão de formar *links* com todos os seus dispositivos filho e com o AP, e que os ED não permitem associação de outros dispositivos, podendo apenas fazer um *link* (74) (80). A cada *link* feito por um dispositivo é atribuído um valor na sua memória, ao qual corresponde a uma determinada aplicação residente no dispositivo com o qual foi feito o *link*.

Request	TID	Link Token	Local Port	Rx Type	Protocol Ver	CTR Value
1 (0x01)	1	4	1	1	1	4

Figura 60 - Formato da trama de camada de rede para a função *link*. Fonte: Texas Instruments.

Este ponto será desenvolvido no subtópico Reencaminhamento de mensagens e Associação, uma vez que é a partir da função *link* que dados são reencaminhados num *Router*, e que é na associação de um dispositivo à rede que se executa o *link*.

Tabela 8 - legenda da Figura 60.

Request	Indicativo de pedido
TID	*Id* da transacção
Link Token	Valor residente em memória de todos os dispositivos da rede
Local Port	Valor identificador do dispositivo com o qual se executou o *link*, usado para a camada de "aplicação"
Rx Type	Tipo de dispositivo: sempre ligado ou necessita de suporte de dispositivo adormecido (armazenamento de dados até *polling*, como no protocolo *ZigBee* – ver Comunicação com dispositivos adormecido)
Protocol Ver	Versão do protocolo 433 MHz do emissor
CTR	Valor referente à função de segurança - contador

A aplicação *Join* está presente nos dispositivos que permitem a função de associação à rede, AP e *Routers*. A aplicação é iniciada por um dispositivo que tenta ligar-se à rede, ao transmitir uma mensagem com a função *join*, sabendo de antemão (pela aplicação *Freq*, como se verá), que existe um AP naquele canal. Para que o dispositivo possa ligar-se a uma determinada rede, deverá conhecer o *join token* da rede, de forma a ser reconhecido pelo dispositivo que lhe concederá acesso – que o associará. No subtópico Associação demonstra-se como se implementou este esquema de forma a possibilitar flexibilidade para dispositivos produzidos em fábrica e remetidos para um cliente, onde não se conheça o *join token*. Caso se trate de um *End Device* – que está grande parte do tempo em modo adormecido e como tal necessita que a sua unidade pai armazene mensagens que lhe são endereçadas – na mensagem de pedido de *join* introduz no campo *device info* informação indicativa de que se trata de um ED adormecido.

Request	TID	Join Token	Number of connections	Protocol Ver
1 (0x01)	1	4	1	1

Figura 61 - Formato da trama de camada de rede para a função *link*. Fonte: Texas Instruments.

A aplicação *Freq*, que corresponde à funcionalidade designada no protocolo *SimpliciTI* como *Frequency Agility*, apenas pode ser iniciada pelo *Access Point*, podendo ser reencaminhada por outros dispositivos (caso do *Router*). A aplicação é normalmente usada, no protocolo

SimpliciTI, como uma consequência à detecção, por parte do AP, de que o canal actual é "demasiado" ruidoso, sendo que demasiado significa acima de um limite pré-definido.

No entanto, no âmbito do protocolo 433 MHz, foi feita uma alteração, de modo a implementar também o algoritmo de impedimento de comunicação em canais ruidosos logo na inicialização de rede.

Tabela 9 - Legenda da Figura 61.

Request	Indicativo de pedido a aplicação
TID	*Id* da transacção
Join Token	Valor residente em memória de todos os dispositivos da rede, usado na aceitação do pedido de *join*
Number of connections	Número de ligações – usado no protocolo *SimpliciTI* para o AP reconhecer dispositivos que não executam ligações – caso dos *range extenders* – pelo que não tem de aguardar pelo pedido de *link*
Protocol Ver	Versão do protocolo 433 MHz do emissor

Apesar de a probabilidade de encontrar um canal ocupado ou com ruído elevado na gama dos 433 MHz ser baixa, quando comparada com as suas congéneres na gama ISM dos 2.4 GHz, é importante manter este esquema para evitar possíveis canais ruidosos, para além de possibilitar a criação de várias redes 433 MHz numa mesma área geográfica.

Assim, a função *Freq* tem dois possíveis comandos:

- alteração de canal, emitida por um AP, para informar os restantes dispositivos da alteração para o novo canal, indicado na mensagem (de acordo com o seu índice na tabela de canais);
- eco, uma mensagem de *ping* usada para avaliar um canal – o dispositivo que a emite espera uma resposta de um AP que esteja a operar nesse canal e guarda o nível de RSSI (sendo esta segunda informação apenas utilizada pelo AP).

A aplicação *Security* contém apenas um tipo de mensagem, sendo que para uma rede com segurança activada (definiram-se todas como tendo), terá de existir uma chave de encriptação geral, que serve para encriptar e desencriptar mensagens transmitidas entre pares. No protocolo *SimpliciTI*, essa chave é definida pelo AP, que a transmite em *broadcast* para todos os outros dispositivos. No entanto, uma vez que esta prática traz uma falha de segurança para a rede, na medida em que essa mensagem poderá ser interceptada, a chave de segurança é gravada em

memória antes da sua instalação – aquando da fase de configuração em laboratório/oficina, tal como foi referido na secção Funcionalidades comuns aos dois protocolos desenvolvidos do capítulo anterior. A chave poderá ser alterada, sendo que o dispositivo ficará identificado com a chave associada.

A encriptação em si é apenas aplicada aos dados de aplicação, sendo todos os outros dados transmitidos sem aplicação. O algoritmo de encriptação usado é o XTEA (*eXtended Tiny Encryption Algorithm*), sendo que a encriptação e desencriptação são feitas ao nível da camada de aplicação.

Finalmente, a aplicação *Management* possibilita a gestão de dados destinados a dispositivos adormecidos. Esta função é comum a todos os dispositivos que permitem associação de outros à rede. Um dispositivo pai, na informação que tem guardada em memória relativamente aos filhos, dispõe da informação sobre o tipo de dispositivo, podendo tratar-se de um dispositivo sempre ligado ou de um ED com *polling*. O segundo caso aplica-se à aplicação *management*, e nesse caso transmite periodicamente uma mensagem de *polling* de possíveis dados armazenados para si, de acordo com o formato apresentado na Figura 62.

Request	TID	Port	Address
1	1	1	4

Figura 62 - Formato de trama de aplicação *management*.

Tabela 10 - Legenda da Figura 62.

Request	Tipo de pedido
TID	*Transaction id*
Port	O mesmo *port* que aquele do *link* que o ED tem com a unidade pai
Address	O endereço da unidade pai

4.2.2.4. Formação

A rede é iniciada pelo *Access Point*, num esquema que utiliza as aplicações de rede *Freq*, *Security* e *Join* (80).

Numa forma semelhante à descrita para o protocolo *ZigBee*, o protocolo 433MHz permite uma selecção de canais, sendo que foi definido um conjunto inalterável de 5 canais. Esse conjunto serve de base para a inicialização de uma rede 433 MHz, sendo que o *Access Point* executará a função de escuta de todos os canais na tabela definida, seleccionando aquele que tiver o nível de

RSSI mais baixo. No caso remoto de medições idênticas, o canal selecionado será o da frequência de base, 433,92 MHz.

Tal como para o protocolo *ZigBee*, é configurável o número de dispositivos filho que um outro dispositivo com funções de gestão de rede pode aceitar. Este apenas é limitado pelo espaço em memória do dispositivo, pelo que não foram colocados impedimentos no que toca a este número. Como medida de precaução, manteve-se o valor máximo nos 30 para o AP e 5 para um *Router*, valores que, como se verá no capítulo Testes, teve bons resultados. Este valor foi assim definido devido ao limite de tamanho do código-fonte que o compilador usado permite, tendo-se usado o valor máximo permitido. No caso do *Router*, escolheu-se um valor consideravelmente inferior pela mesma razão apontada no protocolo *ZigBee*: uma vez que os *Routers* deverão ainda reencaminhar dados de ilhas cabladas que integram na rede sem fios, terão de possibilitar o acesso à rede a um número inferior de ED, comparando com um AP.

O esquema de formação de rede, apenas executável pelo AP, é o seguinte (80):

- execução do comando eco da aplicação *Freq* para todos os canais disponíveis na lista – com transmissão de uma mensagem –, armazenando os resultados de RSSI e possíveis respostas de AP já inicializados no referido canal;
- o canal com o menor nível de RSSI e onde não tenha ocorrido resposta à mensagem de eco é escolhido (apenas o AP responde, pelo que é indicativo de que já existe uma rede a operar naquele canal);
- estabelecimento de operação da rede no canal escolhido;
- estabelecimento da chave de encriptação, guardada em memória do dispositivo (ver subtópico Aplicações de rede;
- inicialização do suporte de *Join* para novos dispositivos;
- inicialização do suporte de armazenamento de mensagens para dispositivos adormecidos;
- transmissão de uma mensagem *broadcast*, indicativa da inicialização da rede no referido canal.

Caso ocorra um caso em que o AP é reinicializado, por falha de energia ou qualquer outra razão, os restantes dispositivos da rede tomarão conta desta ocorrência através da transmissão de mensagens *freq*, no primeiro passo do método acima indicado.

4.2.2.5. Associação

A associação de dispositivos só pode ocorrer a partir do momento em que o AP se encontra correctamente inicializado, e dentro da sua área de alcance. A partir desse momento,

dispositivos *Router* ou ED podem associar-se à rede através de mensagens *Join*, sendo que um *Router* que esteja associado também poderá permitir o acesso de ED. Um *Router* nunca poderá permitir o acesso à rede de outro *Router*, por condição de verificação após a recepção de um pedido *join*. Como será descrito em maior detalhe no subtópico seguinte, o identificador de 4B que todos os dispositivos têm contém informação relativa ao tipo de dispositivo – AP, ED, *Router.* Desta forma, o *Router* detecta se se trata de um ED ou de outro *Router* a tentar aceder à rede, determinando assim se responderá ao pedido de *join* ou se descartará a mensagem. O *join token*, parâmetro fundamental para que um dispositivo possa associar-se à rede, é definido em fábrica, tal como o *link token*. Serve como medida adicional de protecção contra dispositivos maliciosos ou sem permissões de acesso à rede, e é desta forma igual para todos os dispositivos, permitindo diferentes associações, o que melhora a robustez em caso de falha de dispositivos com filhos.

O método de associação de um dispositivo à rede processa-se na seguinte forma:

- o novo dispositivo transmite uma mensagem *ping* em todos os canais permitidos em modo *broadcast*, até obter resposta – note-se que apenas obterá resposta de um dispositivo pertencente à rede que tem o mesmo *join token* que a mensagem de *join* original, evitando assim que se ligue a uma rede não pretendida a operar na área;
- todos os dispositivos com capacidade de associação que se encontrem dentro do alcance do primeiro responder-lhe-ão, na condição de:
    - ainda disporem de espaço livre, de acordo com o seu número máximo de dispositivos filho permitidos;
    - não se tratarem de dois dispositivos *Router*;
- o novo dispositivo armazena todas as mensagens recebidas dentro de um determinado período de tempo, seleccionando o identificador de rede do dispositivo de acordo com as seguintes regras, ordenadas por de importância:
    - se tratar do AP;
    - no caso de comparação entre *Routers*, aquele cuja mensagem tiver o valor de RSSI superior;
- de seguida, o novo dispositivo efectuará um pedido de *link* com o dispositivo selecionado, indicando para isso o *link token*;
- do lado dos dispositivos que responderam à associação, terminarão o processo de resposta a *join* e ficarão a aguardar um pedido de *link* por parte do novo dispositivo, com base no seu identificador (presente no pedido de *join*);

- os dispositivos que tenham respondido ao pedido de *join* e não tenham obtido como resposta um *link* descartarão aquele dispositivo da sua lista de filhos, possibilitando a associação de outro no seu lugar.

4.2.2.6. Reencaminhamento de mensagens

Como foi descrito na secção Topologia, a rede 433MHz desenvolvida permite a criação de redes em árvore até dois níveis de distância do nó central.

Essa limitação não é feita ao nível da funcionalidade de *routing* mas, tal como já foi descrito, através do impedimento no processo de associação de que um *Router* responda ao pedido de *join* de outro *Router*.

Esta escolha deve-se à intenção de manter o protocolo simples, implicando a ocupação de pouca largura de banda devido a gestão de rede.

O objectivo foi alcançado ao libertar o protocolo de mensagens de gestão de tabelas de *routing*, tal como existem no protocolo *ZigBee*, limitando as mensagens de gestão de rede à formação de rede – uma única mensagem, emitida pelo *Access Point*, para anunciar o estabelecimento da rede num determinado canal – associação de dispositivos – troca de pelo menos 3 mensagens entre novo dispositivo e possíveis dispositivo(s) pai (desenvolvido no subtópico Associação) – e mensagens de dados trocadas entre dispositivos, bem como os respectivos *acknowledgement* (já descritos em Funcionalidades comuns aos dois protocolos desenvolvidos).

Mais concretamente, no que toca ao reencaminhamento de mensagens, este é feito com base nos já apresentados identificadores de 4B. Os identificadores são criados a partir dos identificadores de rede geral, no seguinte formato:

Byte 1	**Byte 2**	**Byte 3**	**Byte 4**
Identificador de rede geral	Tipo de dispositivo (AP = 1, *Router* = 2, ED = 3)	Tipo de dispositivo (AP = 1, *Router* = 2, ED = 3)	Identificador de rede geral

Figura 63 - Formato dos identificadores de rede 433 MHz.

Como se verá no capítulo Aplicações desenvolvidas, antes da instalação no terreno é atribuído um identificador de rede geral a cada dispositivo, sendo que esse identificador é pedido pelo controlador de comunicações ao respectivo controlador de aplicação, a cada inicialização.

Assim, e uma vez que todos os dispositivos de uma rede geral têm um identificador único naquela rede híbrida, também os identificadores da rede sem fios serão únicos.

Tentou-se que o esquema de *routing* fosse o mais simples possível, para facilitar a sua implementação e tendo em conta as limitações já referidas. Desse modo, o reencaminhamento de dados é feito de acordo com o seguinte método:

- o dispositivo emissor encripta a mensagem, através do algoritmo XTEA (brevemente descrito abaixo);
- o dispositivo emissor transmite a mensagem, indicando para o efeito qual o identificador emissor e qual o identificador receptor (ver Figura 56);
- os vários dispositivos dentro do seu alcance e em modo ligado verificam o campo identificador e filtram a mensagem com base no seu próprio identificador;
- o dispositivo receptor desencripta a mensagem e verifica se o valor referente ao identificador de rede geral (referente a um controlador de aplicação, ver Figura 36) corresponde ao primeiro byte do seu próprio identificador de rede sem fios (que é igual ao identificador de rede geral do controlador de aplicação que lhe corresponde);
- caso seja igual, armazena a mensagem no *buffer* de envio para o controlador de aplicação;
- caso seja diferente, armazena a mensagem no *buffer* de envio para outro dispositivo, com o referido identificador de rede sem fios, através da rede.

Veja-se que um ED apenas necessita de conhecer o identificador de rede sem fios da sua unidade pai, que se encarregará, no caso de ser um *Router*, de a encaminhar para o AP. No caso do AP, este tem em memória uma tabela de correspondências de todos os identificadores de rede geral, e qual o identificador de rede sem fios do dispositivo mais próximo que lhe corresponde, na mesma forma da tabela descrita na secção Reencaminhamento de mensagens do protocolo *ZigBee*. Essa tabela é dinâmica, verificando a cada mensagem recebida da rede sem fios qual o identificador de rede geral do dispositivo emissor original e qual o identificador de rede sem fios do dispositivo mais próximo.

O caso restrito do *broadcast*, cujo identificador de rede é, na nomenclatura acima apresentada (e em hexadecimal) FF FF FF FF, é tratado de acordo com o tipo de mensagem. No caso de se tratar de um pedido de associação à rede, o dispositivo *Router* ou AP não reencaminhará a mensagem, uma vez que não se trata de uma mensagem a propagar pela rede mas sim um pedido de um dispositivo que ainda não pertence à rede.

No outro caso possível de *broadcast*, considerando as mensagens de dados – e que apenas o AP pode emitir –, apenas os *Routers* reencaminham mensagens do AP, para que não ocorram repetições indevidas. Desse modo, um *broadcast* executa-se de acordo com o seguinte método:

- armazenamento da mensagem em memória do AP;

- *broadcast* emitido pelo dispositivo AP;
- recepção de todos os *Routers*;
- armazenamento da mensagem em memória de cada *Router*;
- transmissão da mensagem para o controlador de aplicação correspondente a cada *Router*;
- retransmissão do *broadcast* a cada *poll* de *ED* por parte do seu dispositivo pai;
- eliminação da mensagem em memória de cada dispositivo pai, após todos os ED seus filhos terem executado o *poll* a mensagem.

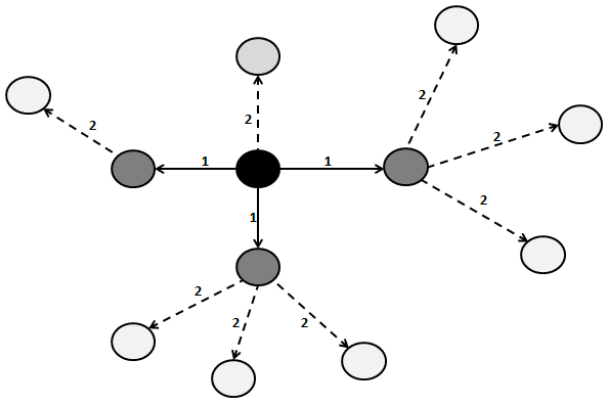


Figura 64 - Esquema representativo de um *broadcast*.

Com este esquema, representado na figura acima, a mensagem é disseminada na rede sem repetições uma vez que o *broadcast* só ocorre "localmente": inicialmente entre AP e *Routers* e de seguida entre dispositivos pai sempre ligados e dispositivos filho em modo adormecido (ED). Nesta figura os índices pretendem representar as duas fases da transmissão, primeiro do AP (a preto) para os *Router*s (a cinzento escuro), e depois (2) dos dispositivos pai para os seus dispositivos filho adormecidos (ED), a pedido de *polling* (a tracejado).

4.2.2.7. Comunicação com dispositivos "adormecidos"

Tal como foi apresentado na secção Funcionalidades comuns aos dois protocolos desenvolvidos, e tal como novamente referido para o protocolo *ZigBee*, a comunicação com dispositivos adormecidos na rede 433 MHz é feita através de um processo de *polling*, em que o dispositivo adormecido é em qualquer caso um Dispositivo Terminal ou *End Device*, com funções de sensor inteligente. O ED adormecido corre periodicamente a seguinte rotina:

- passagem para o modo ligado, com activação da unidade rádio;
- envio de uma mensagem de aplicação *management* para a sua unidade pai (dispositivo sempre ligado);

- caso existam dados em espera, resposta da unidade pai com os referidos dados, numa mensagem normal de dados;
- caso não existam dados em espera, a unidade pai não tem resposta;
- no caso de o ED ter recebido dados por parte da unidade pai, reencaminha-os para o controlador de aplicação, que estava até esse momento também em modo adormecido;
- o controlador de comunicações regressa ao modo adormecido.

Na unidade pai, e tal como foi descrito para o processo de *broadcast*, aquando da recepção de dados destinados à sua unidade filho, armazenam-se os referidos dados em *buffers* dedicados, aguardando pela mensagem de aplicação *management*, quando ocorrer o próximo *poll* periódico por parte da unidade filho.

4.2.3. Interface controlador de Comunicações – controlador de Aplicação

O controlador de comunicações foi desenvolvido para, primariamente, funcionar como periférico de um controlador de aplicação, que regula o seu funcionamento. Apesar disso, e tal como já foi atrás referido, pretendeu-se que o controlador de comunicações fosse o mais autónomo possível, tratando automaticamente das funções de ligação a outros dispositivos na rede sem fios.

Como tal, os seguintes comandos estão disponíveis para a operação do controlador de comunicações:

- inicialização de *stack* – ordem para inicialização de *stack* protocolar, emitida após a inicialização do controlador de aplicação;
- transmissão de mensagem para a rede – o controlador de aplicação envia a mensagem no formato de rede geral, sem qualquer campo adicional, cabendo ao controlador de comunicações identificar na mensagem o endereço de rede geral do destinatário, e a partir dele descobrir (a partir da tabela que tem em memória) qual o endereço do dispositivo da rede sem fios correspondente, de acordo com o algoritmo de reencaminhamento de dados atrás descrito;
- *reset* do controlador de comunicações.

Do lado do controlador de comunicações, apenas pode ser feito o seguinte pedido:

- configuração de identificador – pedido feito pelo controlador de comunicações ao controlador de aplicação, pedindo o identificador de rede geral para definição do seu identificador de rede 433 MHz, com base no esquema atrás descrito.

Sendo que, por sua iniciativa, o controlador de comunicações transmite as mensagens:

- transmissão de dados provenientes da rede e destinados ao controlador de comunicações – carece de resposta;
- confirmação da inicialização de *stack* – é uma resposta a pedido;
- confirmação da recepção de *acknowledgement* (ou da falha deste) correspondente a uma mensagem transmitida para a rede a partir do controlador de aplicação .

Estas mensagens seguem o seguinte formato:

Tamanho	Tipo de mensagem	Função	Identificador do destino	Identificador do emissor	Dados
1B	1B	1B	1B	1B	n B

Figura 65 - Formato de uma trama controlador de comunicações - controlador de aplicação

O tipo de mensagem consiste na informação sobre o tratamento a dar à mensagem pelo controlador receptor:

Tabela 11 - Tipos de mensagem no protocolo SPI entre controlador de comunicações e de aplicação.

Tipo de mensagem	Valor	Descrição
MSG_CONFIGURAÇÃO	1	Deverá ser tratada pelo próprio controlador, é uma mensagem interna ao próprio dispositivo
MSG_DADOS	2	Relativa a comunicações com a rede sem fios

O campo função poderá incluir funções de aplicação, apenas conhecidas dos controladores de aplicação, ou funções de configuração, relativas a mensagens de configuração locais (MSG_CONFIGURAÇÂO). Essas funções são:

Tabela 12 - Funções de configuração interna.

Função	Descrição	Valor
RESET	Reset ao controlador de comunicações.	1
DESLIGAR_RADIO	Desligar o dispositivo rádio e colocar o controlador de comunicações em modo adormecido.	2
LIGAR_RADIO	Ligar o dispositivo rádio e colocar o controlador de comunicações em modo activo.	3
OK_AP	Indicativo de sucesso na implementação do pedido efectuado.	4
ERRO_AP	Indicativo de erro na implementação do pedido efectuado.	5

As mensagens de configuração seguem o seguinte formato de trama:

Tabela 13 - Formato das tramas de configuração interna.

Tamanho	Tipo de mensagem	Função
2	MSG_CONFIGURAÇÃO	1, 2 ou 3

Sendo a resposta ao pedido de configuração (enviada pelo controlador de comunicações):

Tabela 14 - Formato da trama de resposta a uma mensagem de configuração.

Tamanho	Tipo de mensagem	Função
2	MSG_CONFIGURAÇÃO	4 ou 5

Tanto do lado do controlador de comunicações como do lado do controlador de aplicação existem *buffers* de recepção e de transmissão nos quais são guardadas as mensagens recebidas e mensagens para transmissão, no formato identificado na Figura 66.

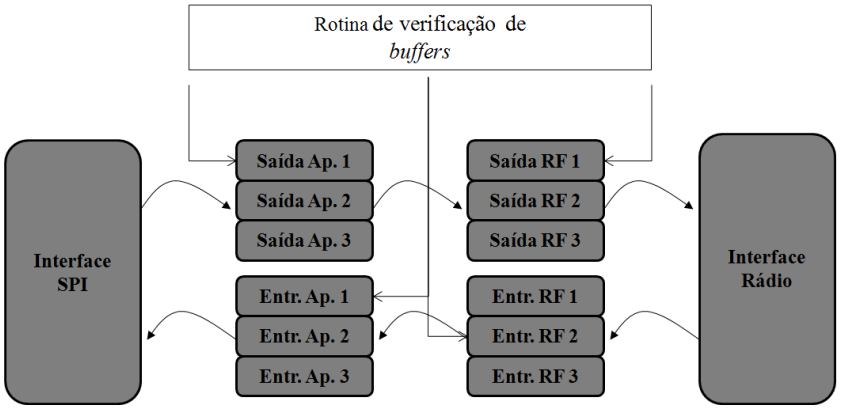


Figura 66 - *Buffers* internos do controlador de comunicações, de entrada e saída, para gestao de dados entre a rede sem fios e o controlador de aplicação.

Existem dois tipos de *buffer* distintos, de acordo com a interface da qual provêm os dados, precisamente para distinguir os dados provenientes da rede sem fios dos dados provenientes da memória do microcontrolador, aquando da execução da rotina de verificação.

A comunicação entre o controlador de comunicações e o controlador de aplicação é baseada numa interface série, mais concretamente numa SPI (*Serial Peripheral Interface*). Nesta comunicação, o controlador de aplicação tem o papel de SPI *Master*, enquanto o controlador de comunicações tem o papel de SPI *Slave*.

4.2.4.API do protocolo 433 MHz

4.2.4.1. Introdução

Pretendeu-se implementar uma camada de interface de aplicação com base no protocolo *SimpliciTI* que permitisse a abstracção de camadas inferiores, de acesso a meio físico. Esse acesso é feito nas comunicações série com o dispositivo rádio e com o dispositivo controlador de aplicação, sendo que em termos de camadas de baixo nível foi necessário:

- alterar algumas funções protocolares de acesso à rede;
- criar as funções de interface série com o controlador de aplicação.

Nesta secção apresentam-se assim não só as funções de aplicação do protocolo 433 MHz como as funções de baixo nível desenvolvidas, para além dos serviços implementados pelas funções de alto nível.

Tal como já foi apresentado atrás, as mensagens trocadas entre quaisquer dois dispositivos na rede são feitas no formato de pedido, um nó emissor emite um pedido para um nó receptor que deverá ser correspondido, ficando o nó emissor a aguardar essa resposta. Nó, neste contexto, significa controlador de comunicações, uma vez que o controlador de aplicação não está envolvido nos processos de comunicações com a rede.

Assim o nó emissor, ao fazer um pedido de um dos tipos descritos na secção anterior (resumidos em Aplicações de rede), está a fazer um pedido do qual aguardará uma resposta, como se verá na descrição das diferentes aplicações.

As respostas possíveis aos pedidos são apresentadas na Tabela 15.

Tabela 15 - Respostas aos pedidos protocolares - códigos devolvidos a cada pedido e sua descrição.

Código	Definição	Valor
SMPL_SUCCESS	Operação bem sucedida.	0
SMPL_TIMEOUT	O tempo permitido para resposta a um pedido síncrono terminou.	1
SMPL_BAD_PARAM	Parâmetro introduzido não existe para a função indicada.	2
SMPL_NOMEM	Memória cheia.	3
SMPL_NO_FRAME	O *buffer* de entrada está livre.	4
SMPL_NO_LINK	Não foi recebida resposta ao pedido de *link.*	5
SMPL_NO_JOIN	Não foi recebida resposta ao pedido de *join.*	6
SMPL_NO_CHANNEL	Não se identificou qualquer dispositivo pai nos canais pesquisados ou todos os canais estão ocupados.	7
SMPL_TX_CCA_FAIL	Não foi possível aceder ao meio, CCA falhou.	9
SMPL_NO_PAYLOAD	A mensagem recebida não tem dados no campo *payload.*	10
SMPL_NO_ACK	O *acknowledgement* referente à mensagem transmitida não foi recebido.	12

4.2.4.2. Inicialização da base protocolar e inicialização/acesso à rede – *SMPL_Init*

Esta função compreende os seguintes passos:

1. a inicialização da interface com o dispositivo rádio, através das funções de baixo nível *MRFI_Init* e *MRFI_WakeUp*;
2. inicialização das aplicações de rede suportadas, através da função de camada de rede *nwk_nwkInit*;
3. estabelecimento de canal base, através da função de camada de rede *nwk_setChannel*(canal) e:
    a) no caso de ser um AP, tentativa de criação da rede no canal estabelecido, enviando uma mensagem de inicialização de rede *SMPL_SendOpt*;
        i. caso não obtenha resposta, prossegue para o próximo passo (resposta SMPL_SUCCESS);
        ii. caso obtenha resposta de outro AP, regressa ao passo 3;
        iii. no caso de todos os canais estarem ocupados, retorna o parâmetro SMPL_NO_CHANNEL.
4. colocação do dispositivo rádio em modo de recepção, através da função *MRFI_RxOn*;
    a) no caso de ser um ED ou *Router*, pedido de associação à rede, através da função *nwk_join*, retornando o valor bem sucedido SMPL_SUCCESS ou falha na associação à rede SMPL_NO_JOIN.
5. Saída da função, com um dos valores indicados na tabela abaixo.

Tabela 16 - Códigos de saída da função *SMPL_Init.*

Códigos de saída
SMPL_SUCCESS
SMPL_NO_CHANNEL
SMPL_NO_JOIN

4.2.4.3. Associação à rede – nwk_join, smpl_send_join_reply, SMPL_Link e SMPL_LinkListen

Apesar de as funções *nwk_join* e *nwk_processJoin* não fazerem parte da API do protocolo 433 MHz, são aqui apresentadas como peças constituintes do processo de associação à rede.

A função *nwk_join* não tem qualquer entrada, e processa-se de acordo com os seguintes passos:

- envio em *broadcast* de uma função *ping* em cada canal, até receber uma resposta de dispositivos já activos – caso não detecte algum retorna SMPL_NO_CHANNEL;

- estabelecimento do canal com dispositivo(s) detectado(s) cujo *join token* seja igual;
- envio de mensagem *join* (porto *join*) para um (dos) dispositivo(s) que tenha(m) respondido de acordo com a seguinte regra:
    - trata-se do AP;
    - tem o RSSI mais baixo;
- aguarda resposta a pedido *join* durante um período de tempo pré-determinado;
    - caso receba a resposta ao pedido, esta incluirá o *link token*, e a saída será SMPL_SUCCESS;
    - caso não receba resposta, a saída da função será SMPL_NO_JOIN;
- saída da função, com um dos valores da tabela abaixo.

Tabela 17 - Códigos de saída da função nwk_join.

Códigos de saída
SMPL_SUCCESS
SMPL_NO_CHANNEL
SMPL_NO_JOIN

A mensagem *join*, transmitida pela função anterior, tem o seguinte formato, colocado na *application payload*:

Pedido	TID	*Join token*	Número de ligações	Versão protocolar
1 B (0x01)	1 B	4 B	1 B	1 B

Figura 67 - Pedido *join*.

Um dispositivo que permita associação à rede corre constantemente, como se verá na descrição do sistema operativo, a função de verificação de mensagens recebidas. Ao receber um pedido *join*, resultante da sua resposta a *ping*, verifica o número de dispositivos filho que já tem e caso ainda não tenha sido atingido o limite executa a função *nwk_processJoin*, que não tem qualquer saída, e tem como entrada a mensagem de pedido de *join*. A resposta ao pedido *join* consiste na transmissão da seguinte mensagem para o endereço do dispositivo que o requereu:

Pedido	TID	*Link token*
1 B (0x81)	1 B	4 B

Figura 68 - Resposta a pedido *join*.

A resposta tem um pedido com MSB (*most significant byte*) diferente de 0, indicando que se trata de uma resposta e não de um pedido, o mesmo TID do pedido original e o *link token* da rede. Finalmente, soma o valor 1 ao número de filhos actual.

A função *SMPL_Link* é executada pelo dispositivo (excepto AP) que acabou de terminar com sucesso a função *SMPL_Init*, consistindo no pedido *link* ao dispositivo do qual acabou de receber a resposta ao pedido *join*, o novo dispositivo pai. Tem como entrada o parâmetro *linkID*, que memorizará caso o pedido seja bem sucedido. Este parâmetro foi referido na secção anterior, consistindo no identificador de camada de aplicação ao qual corresponde o identificador do par com o qual se estabeleceu uma ligação lógica.

O pedido de *link* é endereçado para o novo dispositivo pai, sendo a mensagem transmitida a seguinte:

Pedido	**TID**	***link token***	**Porto local**	**Tipo de dispositivo**	**Versão protocolar**	**Valor CTR**
1 B (0x01)	1 B	4 B	1 B	1 B	1 B	1 B

Figura 69 - Mensagem de pedido *link*.

O tipo de dispositivo é indicativo se a unidade que se associa à rede é um ED, e o valor CTR corresponde ao contador da função de segurança.

Da função *SMPL_Link* resulta uma das seguintes saídas:

Tabela 18 - Códigos de saída da função *SMPL_Link*.

Códigos de saída	**Descrição**
SMPL_SUCCESS	*Link* bem sucedido
SMPL_NO_LINK	*Link* falhou
SMPL_NOMEM	O dispositivo pai não aceita mais dispositivos, ou não tem memória para mais ED
SMPL_TX_CCA_FAIL	Não foi possível aceder ao meio

Após um pedido de *join*, o dispositivo pai ficará a aguardar a recepção de um pedido de *link,* durante um período de tempo pré-estabelecido. Aquando da sua recepção, responde através da mensagem *SMPL_LinkListen* que contém a verificação da recepção de uma mensagem de *link* e a correspondente resposta, com a mensagem apresentada abaixo:

Pedido	**TID**	**Porto local**	**Tipo de dispositivo**	**Valor CTR**
1 B (0x81)	1 B	1 B	1 B	1 B

Figura 70 - Mensagem de resposta a pedido link.

Sendo que da função *SMPL_LinkListen* resulta uma das seguintes possíveis saídas:

Tabela 19 - Códigos de saída da função *SMPL_LinkListen*.

Códigos de saída	Descrição
SMPL_SUCCESS	Recepção e resposta a *link* bem sucedidas
SMPL_TIMEOUT	Não foi recebida qualquer mensagem durante o último período.

4.2.4.4. Comunicação de dados para um par – *SMPL_SendOpt* e *SMPL_Receive*

A transmissão de mensagens de um dispositivo para outro só é possível após completar as funções acima descritas: inicialização de base protocolar, associação à rede e ligação lógica com o par.

A função *SMPL_SendOpt* executa o processo de transmissão de dados, tendo como entrada:

- o *link id* do destinatário;
- a mensagem a transmitir;
- a dimensão da mensagem;
- as opções de transmissão, que poderão ser:
    - mensagem com *acknowledgement*;
    - mensagem sem *acknowledgement* (apenas para *broadcast*).

- **Tabela 20 - Códigos de saída da função *SMPL_SendOpt*.**

Códigos de saída	Descrição
SMPL_SUCCESS	Transmissão bem sucedida e *acknowledgement* recebido
SMPL_BAD_PARAM	Parâmetro inválido introduzido - *acknowledgement*
SMPL_NOMEM	Sem memória para transmitir a mensagem
SMPL_TX_CCA_FAIL	Acesso à rede falhou
SMPL_NO_ACK	*Acknowledgement* não foi recebido

A função executa os seguintes passos:

- verificação de existência do *link id* na tabela de dispositivos emparelhados (com os quais tem ligações lógicas);
- verificação de mensagem nula ou demasiado extensa (maior do que o valor permitido para a dimensão do *payload* de aplicação);

- verifica se o destinatário é *broadcast*, sendo que essa opção é incompatível com o pedido de *acknowledgement* – nesse caso sai da função com o código SMPL_BAD_PARAM;
- cria a trama 433 MHz (ver Camadas), de acordo com o destinatário e guarda-a em *buffer* de saída rádio;
- encripta a mensagem, através da função *nwk_setSecureFrame*;
- verifica se o destinatário é um ED, nesse caso manterá a mensagem em memória, até ao pedido *management*;
- transmissão da mensagem através da função *nwk_frame*;
- sai da função, com uma das saídas apresentadas na Tabela 20.

A função de recepção *SMPL_Receive* é chamada em dois casos possíveis:

- após a resposta a interrupção de recepção de uma mensagem do dispositivo rádio. Nesse caso, o ponteiro *sPeerFrameSem* é alterado para um valor diferente de zero, o que faz com que a rotina de recepção de mensagem por parte da aplicação se inicie;
- após o fim de um período adormecido de um ED, onde correrá a função para verificar a existência de mensagens armazenadas no seu dispositivo pai;

A função tem como entradas o *link id* correspondente ao do dispositivo do qual se receberá a mensagem, a própria mensagem e o seu tamanho, sendo que os dois últimos serão preenchidos pelos valores recebidos.

Tabela 21 - Códigos de saída da função *SMPL_Receive*.

Códigos de saída	Dispositivo	Descrição
SMPL_SUCCESS	ED/*Router*	Recepção bem sucedida, mensagem recebida
SMPL_NO_FRAME	ED/*Router*	Não foi recebida qualquer mensagem do *link id* indicado
SMPL_NO_PAYLOAD	ED	Não existia qualquer mensagem no AP
	Router	Erro, mensagem deveria ter *payload*
SMPL_TIMEOUT	ED	Não houve resposta do AP
SMPL_TX_CCA_FAIL	ED	Não foi possível aceder ao meio para fazer o pedido de *polling*

Os seguintes passos são executados:

- no caso de ser um dispositivo sempre ligado:

  - recupera a mensagem do *buffer* de saída da unidade rádio, onde estava guardada, através da função *nwk_retrieveFrame*;
- no caso de ser um dispositivo ED, que executa *polling*:
  - verifica qual o estado da unidade rádio;
  - executa a função *nwk_poll*;
  - aguarda um período;
  - recupera a mensagem de resposta do *buffer* de saída da unidade rádio, onde estava guardada, através da função *nwk_retrieveFrame*;
- sai da função, com um dos códigos da Tabela 21.

4.2.4.5. Encriptação de dados

Como foi atrás referido, o protocolo contém um esquema de encriptação de dados de aplicação, com base no algoritmo XTEA (*eXtended Tiny Encription Algorithm*). Este algoritmo era já implementado pelo protocolo *SimpliciTI*, tendo-se incluído no protocolo 433 MHz.

Trata-se de um algoritmo de encriptação simétrico, sendo que existe uma única chave de 128 bits definida para toda a rede. Com base nessa chave, a mensagem é encriptada na transmissão e desencriptada na sua recepção, existindo um valor inicial de 32 bits e um contador de 32 bits que incrementa a cada bloco de 64 bits criado.

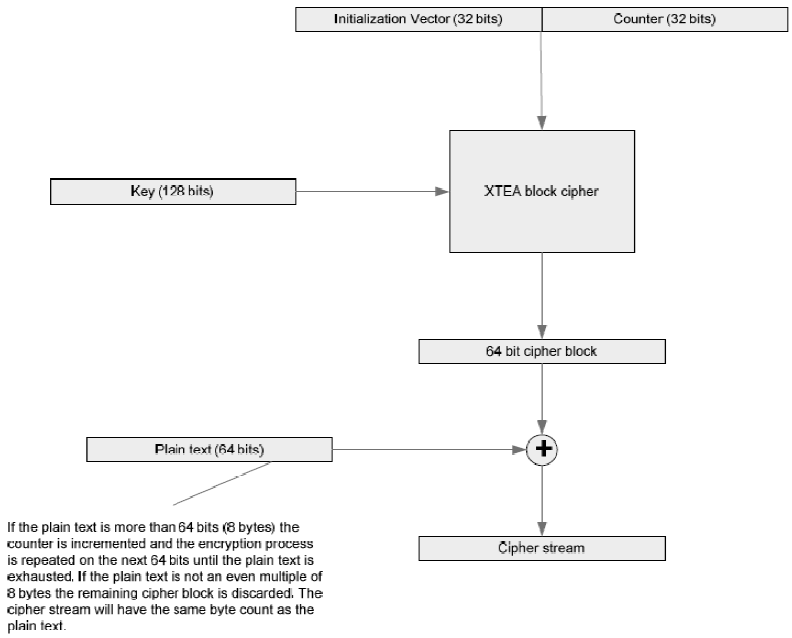


Figura 71 - Processo de encriptação de um bloco de dados de 64 bits através do algoritmo XTEA. Fonte: *Texas Instruments*.

Na verdade, o valor de inicialização e o contador são encriptados através do algoritmo XTEA, com a chave de encriptação, sendo o resultado – um bloco de 64 *bits* – disjunto (através de um

ou exclusivo) com um bloco de 64 bits do *payload* de aplicação. O resultado será um conjunto de blocos de 64 bits.

A função *msg_encipher*, que tem como entradas a mensagem a transmitir, a sua dimensão e o contador de entrada faz a encriptação, guardando no mesmo *buffer* onde se encontrava a mensagem original a sua correspondente encriptada. O valor do contador de 4 Bytes é transmitido na mensagem, tal como foi indicado atrás.

Do lado da recepção da mensagem, existe um bloco de desencriptação equivalente, implementado pela função *msg_decipher*. Esta função tem igualmente como entradas a mensagem recebida, a sua dimensão e o contador de entrada para desencriptação. O algoritmo é apresentado na Figura 72.

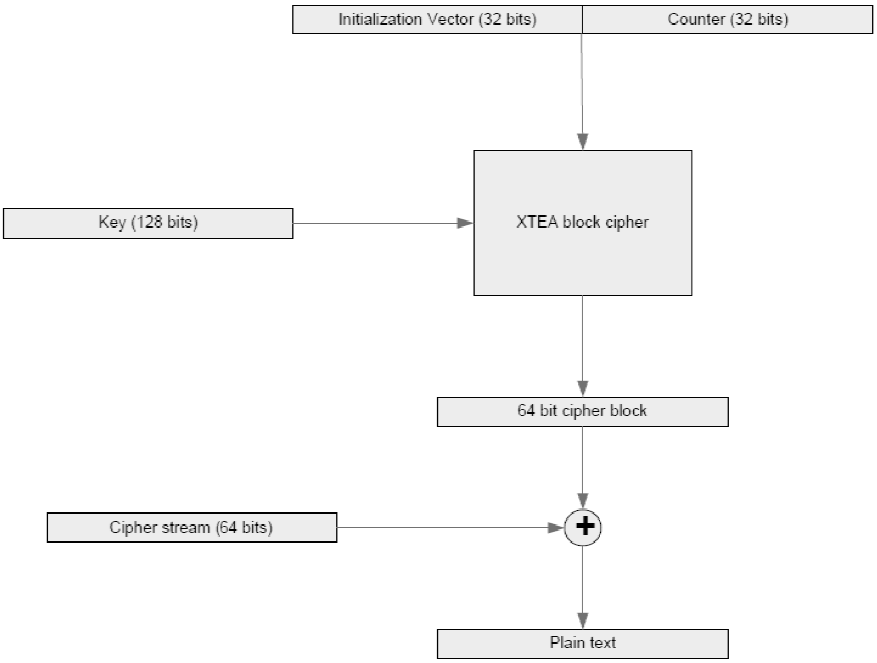


Figura 72 - Processo de desencriptação de um bloco de dados de 64 bits através do algoritmo XTEA. Fonte: *Texas Instruments*.

4.2.4.6. *Polling* de *End Device*s

O *polling* de dispositivos adormecidos já foi largamente apresentado atrás, restando agora apresentar a forma como este é implementado.

Um dispositivo adormecido sai periodicamente desse estado, verificando se existem mensagens pendentes para si no seu dispositivo pai, necessitando para isso de transmitir uma mensagem *management,* com o seguinte formato:

Pedido	TID	Porto remoto	Endereço local
1 B	1 B	1 B	1 B

Figura 73 - Formato de pedido *management*.

A resposta não é transmitida para o porto de *management*, sendo em vez disso transmitida uma mensagem, que corresponderá à mensagem que se encontrava guardada em memória e a aguardar o pedido de *poll* ou uma mensagem vazia, indicativa de que não existiam dados a aguardar.

A função que executa a transmissão da mensagem *management* é *nwk_poll*, referida na Comunicação de dados para um par – *SMPL_SendOpt* e *SMPL_Receive* fazendo simplesmente a transmissão de uma mensagem para o porto *management* do seu dispositivo pai. Tem como entradas o porto remoto e o endereço do destinatário. Tem como saída um dos seguintes códigos:

Tabela 22 - Códigos de saída da função *nwk_poll*.

Códigos de saída	Descrição
SMPL_SUCCESS	Transmissão bem sucedida e *acknowledgement* recebido
SMPL_NOMEM	Sem memória para transmitir a mensagem
SMPL_TX_CCA_FAIL	Acesso à rede falhou

O controlador de comunicações de um *End Device* segue o esquema apresentado no Fluxograma 9, sendo que cada período em que o dispositivo se encontra em modo adormecido é regrado através do RTC (*Real Time Clock*), que gera uma interrupção por segundo. O processo de entrada e saída do modo adormecido segue o seguinte método:

- interrupção de RTC;
- incremento do ponteiro de segundos;
- verificação do estado do dispositivo:
    - caso esteja ligado à rede:
        - se valor de segundos = MINUTO (60 contagens):
            - incrementa ponteiro minutos;
            - coloca *flag_wake* a 1;
        - se valor de minutos = HORA (60 contagens)
            - incrementa ponteiro horas;
        - caso *flag_wake* = 1:
            - sai do modo adormecido;
    - caso não esteja ligado à rede (encontra-se em processo de *join*, na inicialização):

        - se segundos = SEGS_P_NOVA_TENT_LIGACAO:
            - sai do modo adormecido;
    - sai da função.

4.2.4.7. Gestão e acesso a tabelas de conversão de identificadores

Foi referido na secção Funcionalidades comuns aos dois protocolos desenvolvidos do capítulo 3 que AP/Coordenadores e *Routers* gerem tabelas de reencaminhamento de dados, mantendo tabelas em memória que associam identificadores de rede geral com identificadores de rede sem fios, para apoio à transmissão de dados em dispositivos de interface com outras redes (*Gateways*). Nas *gateways* ou dispositivos com funções de *routing* do protocolo 433 Mhz essas tabelas são mantidas e acedidas através de duas funções: *verifica_id433*, para verificação e gravação em memória de pares de identificadores e *procura_GW*, para pesquisa de identificadores correspondentes em memória.

A função *procura_GW* tem como entrada o identificador de rede sem fios *id_433* e o identificador de rede geral *id_geral*. Verifica qual deles foi introduzido ao determinar qual é diferente de 0, percorrendo de seguida as tabelas em memória pelo identificador correspondente. O fluxograma descritivo do processo da função *verifica_id433* está no Anexo I, sob a referência Fluxograma 4.

Por sua vez, a função *verifica_id433* tem as mesmas entradas que a função descrita acima, o identificador de rede sem fios *id_433* e o identificador de rede geral *id_geral*, verificando se existe vaga na tabela de correspondência para armazenar mais um identificador de rede.

4.2.5.Estrutura do *Firmware* do controlador de comunicações

4.2.5.1. Inicialização e Programas de controlo

O *firmware* controlador de comunicações corresponde à implementação prática do protocolo 433 MHz que tem vindo a ser apresentado, tendo sido esse *firmware* estruturado de forma a criar funções independentes sobre as quais um sistema operativo pudesse operar de forma simples.

Significa isto que o *firmware* foi implementado de acordo com um esquema em que as áreas funcionais estão agrupadas nos seguintes grupos:

- Comunicações sem fios, que incluem:
    - Aplicações de rede;
    - Gestão de rede – funções de camada de rede;

- Interface com a unidade rádio;
- Comunicações locais – porta série, que incluem:
  - Gestão de *buffers* de entrada e saída para comunicação com o controlador de aplicação;
  - Interface com o controlador de comunicações;
- Funções internas – temporizador e RTC.

A razão da organização das funções neste formato prende-se com as interfaces existentes no controlador de aplicação: com o controlador de comunicações, a unidade rádio e o seu relógio interno ou temporizador, criado a partir de um cristal de quartzo de 32 MHz.

Todas as aplicações desenvolvidas com base na plataforma 433 MHz partilham deste esquema, com variações que derivam apenas da configuração inicial do dispositivo, feitas a partir da Tabela 48 do Anexo I.

O programa de controlo de dispositivo, após a inicialização de todos os componentes, executa a verificação de *flags* referentes aos diferentes *buffers*, incluindo:

- associação de dispositivos à rede (apenas para AP e *Router*);
- recepção de mensagens de dados da rede sem fios;
- recepção de mensagens do controlador de aplicação.

As referidas *flags* são alteradas com base em rotinas de serviço de interrupção (ISR, do inglês *Interrupt Service Routine*), sendo essa a base para o funcionamento do programa de controlo.

Deste modo, o firmware do controlador de comunicações funciona por estímulo externo em todas as situações exceptuando o *polling* dos *End Devices*, que acontece por estímulo interno, ao se ter alcançado um valor de contagem do temporizador, de acordo com o esquema da Figura 74.

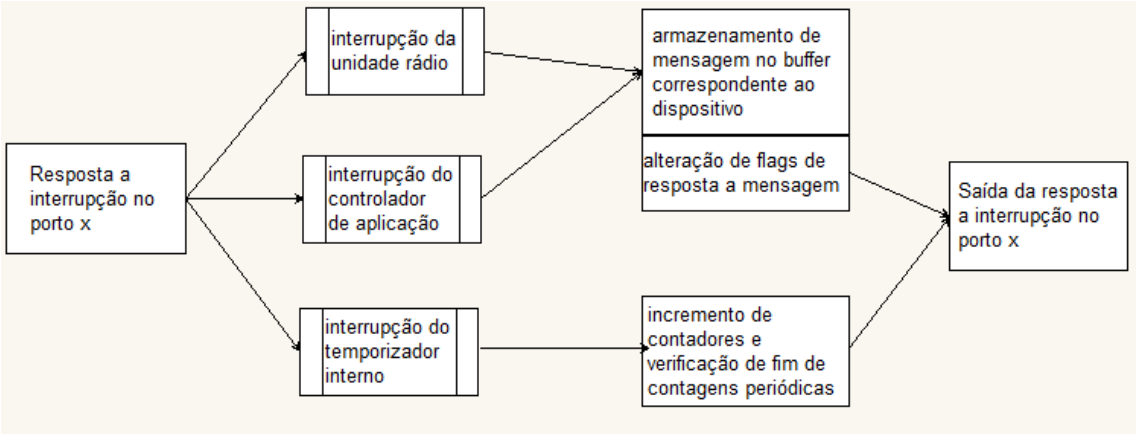


Figura 74 - Rotina de resposta a interrupção do controlador de comunicações.

O que corresponde a um *loop* de programa de controlo que consiste na verificação de *flags* de recepção de mensagens de uma das interfaces, tal como representado na Figura 75, para um AP ou *Router*.

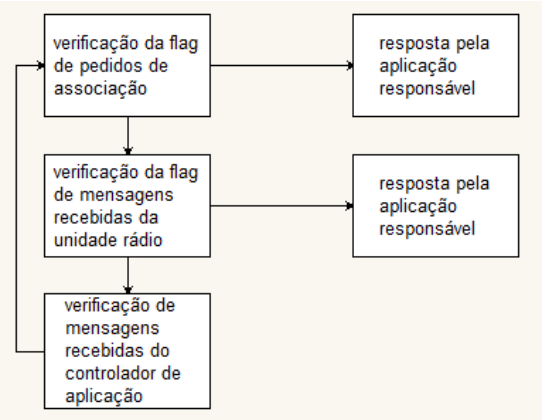


Figura 75 - *Loop* de um dispositivo AP ou *Router*.

O programa de controlo de um ED é ligeiramente diferente, uma vez que não tem verificação de pedidos de associação ou protocolo de reencaminhamento de dados, e que transmite mensagens periódicas de *polling* para verificação de mensagens armazenadas na memória do dispositivo pai, e destinadas para si.

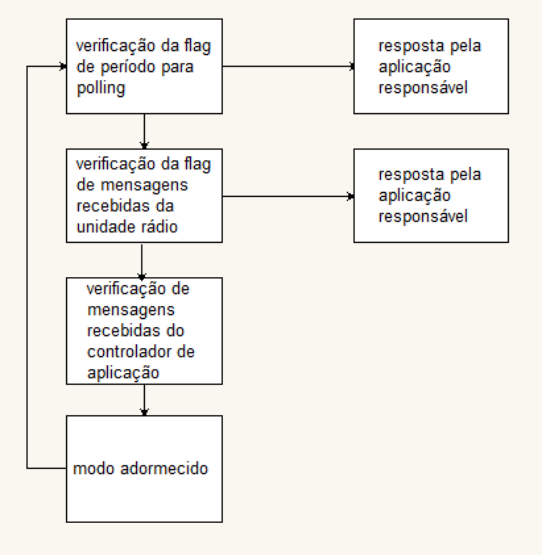


Figura 76 - *Loop* de programa de controlo de um *End Device*.

Os fluxogramas que representam os processos de inicialização e funcionamento normal dos três diferentes dispositivos constituintes do protocolo de plataforma 433 MHz estão apresentados no Anexo I.

Nos referidos fluxogramas são apresentadas diferentes variáveis que constituem *flags* auxiliares do programa, estando descritas na Tabela 23.

Tabela 23 - Variáveis do programa de controlo de AP, *Router* e ED (Fluxograma 8 e Fluxograma 9 do Anexo I).

Variável	Descrição
sJoinSem	*Flag* identificadora de pedido de *join* recebido
sPeerFrameSem	*Flag* identificadora de pedido de mensagem de dados recebida
msgSPI	*Flag* identificadora de pedido de mensagem recebida da SPI
contador_link	Contador de tentativas para efectuar *link*
link id	Identificador de *link* com dispositivo remoto
sNumCurrentPeers	Número de *links*/ligações efectuadas
misses	Número de falhas na transmissão de uma mensagem
acknowledgement	Identificador de pedido de *acknowledgement* de resposta
length link id	Tamanho da mensagem recebida e destinada a este dispositivo
length BROADCAST	Tamanho da mensagem recebida com identificador *broadcast*

Tabela 24 - Variáveis do programa de controlo de ED (Fluxograma 9 do Anexo I).

Variável	Descrição
falhas_poll	Contador de falhas na comunicação com dispositivo pai para *polling*
temporizador	Contador de tempo, para verificação de período de *polling*

Nos mesmos fluxogramas são apresentados valores de comparação, em maiúsculas. Os seus valores típicos são apresentados no Anexo I, Protocolo 433 MHz, Valores de Configuração Inicial.

São ainda referidos os diferentes estados do controlador de comunicações. Este pode ter diferentes estados, para conhecimento do controlador de aplicação (para controlo de casos em que a unidade rádio se encontra ligada e o controlador de comunicações emite novo comando de activação desta unidade – o que leva a bloqueio da comunicação entre microcontrolador de comunicações e unidade rádio), apresentados e descritos na Tabela 25.

Tabela 25 - Funções de estado da unidade rádio.

Código	Valor	Descrição
RADIO_OFF	1	Função de estado da unidade rádio – unidade rádio em modo adormecido
RADIO_ON	2	Função de estado da unidade rádio – unidade rádio em modo ligado

4.2.5.2. Programa de interface com controlador de aplicação

A comunicação entre controlador de comunicações e controlador de aplicação executa-se, tal como no caso da comunicação com outros dispositivos na rede de sensores sem fios, no formato pedido-resposta.

Essa comunicação é baseada em pedidos síncronos, sendo que a transmissão de bytes através da SPI parte sempre do controlador de aplicação – o *master* – apesar de a mensagem poder ser transmitida do lado do controlador de comunicações. Ambos os controladores têm pinos de sinalização que regulam a comunicação: o pino SRDY – *slave ready* – do lado do controlador de comunicações e o pino SS ou MRDY – *slave select ou master ready* – do lado do controlador de aplicação.

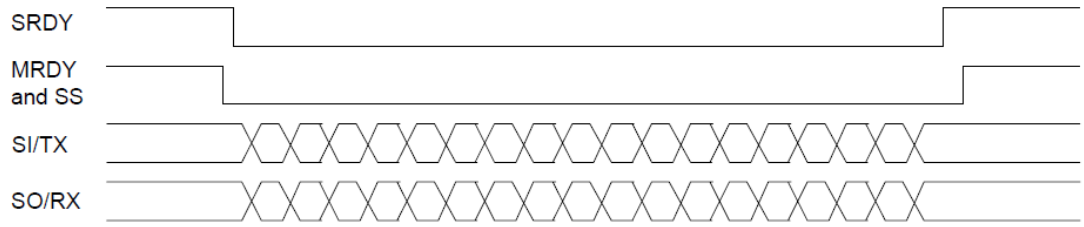


Figura 77 – Comunicação SPI iniciada por *master*.

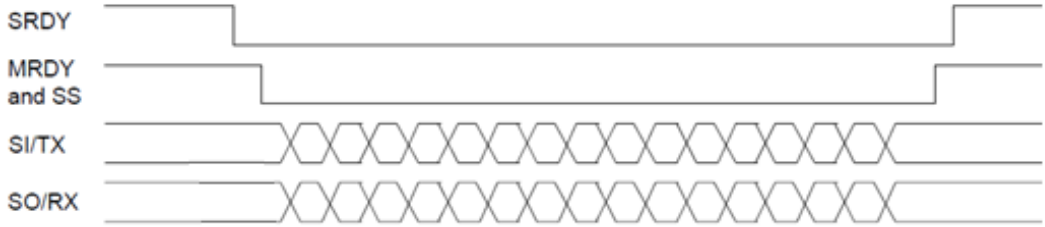


Figura 78 - Comunicação SPI iniciada por *slave*.

Na Figura 77 e na Figura 78 são apresentados os sinais SRDY, SS, SIMO (*Slave In Master Out*, pino de dados de saída do *master*) e SOMI (*Slave Out Master In*, pino de dados de saída do *slave*). Estes são os esquemas de base da comunicação SPI entre *master* e *slave*, sendo a sua descrição mais detalhada apresentada abaixo.

Tal como foi referido no tópico Interface controlador de Comunicações – controlador de Aplicação, existe um conjunto de mensagens trocadas entre os dois dispositivos. As funções *envia_msg_uAp* e *recebe_msg_uAp* são responsáveis pelo direccionamento de mensagens de e para as aplicações do controlador de comunicações, em relação ao controlador de aplicação.

A função *envia_msg_uAp* tem como entradas a mensagem a transmitir, o seu tamanho e o tipo de mensagem. O processamento da função é simples, transfere a mensagem do *buffer* de saída da interface com a unidade rádio para o *buffer* de entrada da interface do controlador de comunicações, executando de seguida chamadas de uma outra função, *envia_SREQ_uAp*, que faz a gestão da interface SPI (ver Fluxograma 1, no Anexo I).

A função de recepção de mensagens, *recebe_msg_uAp*, é ligeiramente diferente, interagindo directamente com a interface SPI. A trama apresentada na Figura 65 corresponde apenas aquela que é interpretada pelos controladores, sendo que na verdade são transmitidos antes dois bytes de *debug*, para ter a certeza de que o *slave* (controlador de comunicações) está sincronizado com o *master* (controlador de aplicação) quando os dados estiverem a ser transmitidos. Adicionalmente, verifica-se a igualdade a 0, para evitar situações em que o controlador de aplicação ainda não esteja a transmitir.

Campo Sincronismo	Tamanho	Tipo de mensagem	Restante mensagem
FF FF (hex)	**1B**	1 B	n B

Figura 79 - Trama da interface SPI explicitando os bytes de sincronismo.

Assim, a função processa-se na forma representada no Fluxograma 2 do Anexo I, sendo que as suas saídas poderão ser:

Tabela 26 - Códigos de saída da função *recebe_msg_uAp*.

Códigos de saída	Descrição
OK_SPI	Recepção SPI bem sucedida
ERRO_SPI	Erro na transmissão SPI

A função de transmissão de uma mensagem – *envia_SREQ_uAp* – sobre a interface SPI tem um esquema semelhante ao da mensagem de recepção, na medida em que o controlador de comunicações inicia a comunicação através da sinalização do pino SRDY, aguardando de seguida a resposta do controlador de aplicação, ao baixar por sua vez o pino de sinalização SS. A função processa-se na forma apresentada no Fluxograma 3 do Anexo I.

A saída da função é uma das seguintes:

Tabela 27 - Códigos de saída da função *envia_SREQ_uAp*.

Códigos de saída	Descrição
OK_SPI	Transmissão SPI bem sucedida
ERRO_SPI	Erro na transmissão SPI

4.3. API de funções comuns – Microcontrolador de aplicação

Os dois tipos de sistema desenvolvidos foram apresentados e descritos nas últimas secções – ao nível das comunicações –, sendo agora necessário apresentar as aplicações que deles derivaram. Estas prendem-se naturalmente com a monitorização de equipamentos industriais, através da sua sensorização com dispositivos sem fios, mas também com dispositivos cablados, dependendo das necessidades de captura e transmissão de dados de medições e o acesso a alimentação de rede eléctrica.

São apresentadas primeiramente as funções que são usadas pelas aplicações desenvolvidas sobre os dois protocolos, uma vez que serão depois nomeadas ao longo da descrição das respectivas API.

4.3.1. Gestão de *buffer*s em *gateway*s

O controlador de aplicação dispõe de *buffers* internos dedicados às respectivas interfaces de comunicações que controla. Relativamente aos dispositivos *gateway*, dispõem de *buffers* dedicados a mensagens do controlador de comunicações sem fios e a mensagens para o controlador de comunicações *CANbus*, tendo cada *buffer* 11 B disponíveis e existindo 15 *buffers* de cada tipo.

Quando uma mensagem é recebida de um controlador de comunicações, é implementado o seguinte método:

- Verificação do destinatário;
- Caso a mensagem seja destinada ao próprio dispositivo:
    - Corre a função de interpretação de mensagens;
- Caso seja para outro dispositivo:
    - Guarda a mensagem em *buffer* de transmissão do outro controlador de comunicações (no caso de receber a mensagem por *CANbus*, coloca no *buffer* do dispositivo sem fios, e no caso de receber a mensagem via sem fios, esta é colocada no *buffer CANbus*).

Este esquema é semelhante ao representado na Figura 66, tal como está na Figura 80.

Este esquema é implementado pelas funções *carregar_lista_envio_RF* (para colocação em memória de uma mensagem proveniente de um dispositivo da rede CAN e destinada a outro dispositivo da rede sem fios), carregar_lista_envio_CAN (para colocação em memória de uma mensagem proveniente de um dispositivo da rede sem fios e destinada a outro dispositivo da rede CAN), e *executar_lista_envio_RF* (para passar a mensagem do *buffer* interno do controlador de aplicação para o *buffer* associado à função de transmissão sem fios) e

executar_lista_envio_RF (para passar a mensagem do *buffer* interno do controlador de aplicação para o *buffer* associado à função de transmissão CAN).

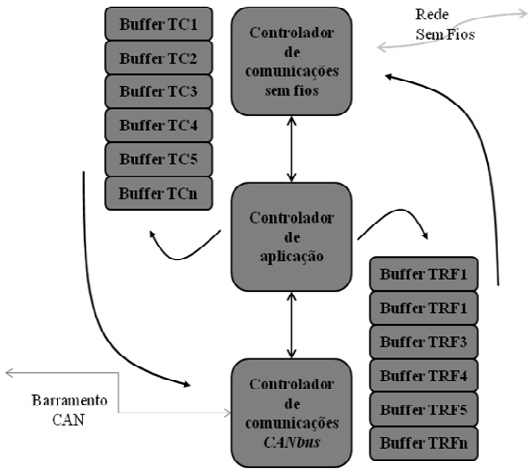


Figura 80 - Representação da interface do controlador de aplicação de uma *gateway* com os controladores de comunicações, e alocação de mensagens nos respectivos *buffers*. TC corresponde a *transmissão* CAN e TRF a *transmissão* de rádio-frequência, correspondendo aos controladores.

Como se verá na secção seguinte, o controlador de aplicação, apesar de aguardar que o controlador de comunicações esteja livre para transmitir a próxima mensagem, não o faz sem continuar as suas restantes tarefas. O método implementado obriga a que o primeiro byte de cada *buffer* corresponda ao seu "estado", indicativo de se existe uma mensagem guardada naquele *buffer* e se sim, se já ocorreu alguma operação sobre ela. Os três estados possíveis são: BUFFER_LIVRE, não se encontra qualquer mensagem guardada naquele *buffer*, BUFFER_OCUPADO, encontra-se uma mensagem no *buffer*, que ainda não foi transmitida, e BUFFER_EM_TX, indicativo de que é a mensagem guardada naquele *buffer* que se encontra actualmente em transmissão. Adicionalmente, sempre que uma mensagem é transmitida para o controlador de comunicações, o ponteiro *radio_livre* é colocado a 1, e não é permitida a transmissão de novas mensagens para aquele controlador até ser recebida a sua resposta, na qual o ponteiro é novamente colocado a 0.

Veja-se que assim apenas uma mensagem está em transmissão de cada vez, pelo que não poderão existir confusões entre qual o *buffer* correspondente. Este sistema permite que o controlador de aplicação de um *Router* ou AP continue as suas tarefas até receber uma mensagem de *acknowledgement* ou de erro na transmissão (falta de recepção do *acknowledgement* da rede) por parte do controlador de comunicações. No primeiro caso, o estado do *buffer* é colocado a BUFFER_LIVRE. No segundo caso, é novamente colocado a BUFFER_OCUPADO, para que aquela mensagem possa vir a ser retransmitida.

Tabela 28 - Estados possíveis de um *buffer.*

Referência	Valor	Descrição
BUFFER_LIVRE	0	O *buffer* está livre para armazenar uma nova mensagem
BUFFER_OCUPADO	1	O *buffer* tem uma mensagem guardada, que não se encontra em transmissão
BUFFER_EM_TX	2	O *buffer* tem uma mensagem guardada, que se encontra em transmissão

As funções acima referidas são implementadas para mensagens de dimensão entre 1 e 6 B, o limite máximo permitido para uma mensagem CAN (ver Capítulo 3, Rede de Campo). Adicionalmente, existe outra função, que consiste na transmissão sobre a rede sem fios de uma mensagem de tamanho superior a 11 B e consequente separação em mensagens de 11B, aquando da sua recepção no dispositivo *gateway* com a rede CAN.

Assim, nos dispositivos *End Device* são transmitidas mensagens com tamanho n, que percorrem a rede sem fios com esse mesmo tamanho, sendo "descompactadas" na *gateway* com o *backbone* da rede. Por outro lado, nos dispositivos *Router* são agregadas mensagens, que são igualmente "descompactadas" na *gateway* que aloja o dispositivo AP.

Existem 15 *buffers* para mensagens de dimensão superior a 11 B na memória da referida *gateway*, podendo essas mensagens ter até 37 B.

As seguintes funções implementam este mecanismo:

- *gravaEnviaFFT3E*: armazena uma mensagem de grande dimensão em memória (quando o seu tamanho é superior a 11 B);
- *executa_lista_envio_433M2* (apenas se for um *Router*);
- *interpreta_mensagem – FUNÇÃO_FFT_X*: separa a mensagem em outras de 11B.

4.3.2. Dados de configuração de fábrica – memória *flash*

A informação que qualquer dispositivo tem em memória e que permite a sua identificação única em relação a qualquer é-lhe atribuída após o término de testes feitos em fábrica, por meio de instruções enviadas através de uma interface de comunicações. Essa informação é guardada em memória *flash,* assim como outros parâmetros de dispositivo (presentes no tópico de secção Memória *Flash* do Anexo I), que são carregados a qualquer inicialização.

Todos os microcontroladores utilizados são da família da MSP430 da *Texas Instruments*, que dispõem de memória *flash* integrada de pelo menos 32 KB, dimensão mais que suficiente para o armazenamento de dados de configuração e identificação de um dispositivo.

O acesso e leitura da memória *flash* é feito, para qualquer dispositivo desenvolvido, através das funções *read_flash* e *write_flash*, que não têm qualquer entrada ou saída, sendo que apenas executam a actualização de ponteiros, no seguinte formato:

- os ponteiros x, y e z (globais) estão guardados em *flash*, ao correr a função *write_flash*:
    - os valores actuais dos ponteiros (não os que estão necessariamente guardados na memória *flash*) são gravados em *flash*;
- os ponteiros x, y e z (globais) estão guardados em *flash*, ao correr a função *read_flash*:
    - os valores actuais dos ponteiros x, y e z são substituídos pelos guardados em *flash*.

4.3.3. Temporizadores

Todos os dispositivos desenvolvidos têm temporizadores para regulação das suas operações internas. Sendo baseados em microcontroladores da família MSP430 da *Texas Instruments*, é possível gerar frequências de *clock* a partir de fontes externas de alta frequência (ordem das dezenas de MHz) ou baixa frequência (cerca de 32 KHz), bem como de fontes internas, que poderão ser da ordem dos MHz, no caso de se usar um DCO (*Digital Clock Oscillator*) ou de cerca de 12 KHz, no caso de ser usado um gerador de *clock* interno ao microcontrolador, designado de VLO (*Very-Low-Power Low-Frequency Oscillator*).

Apenas a partir dos geradores de *clock* de baixa frequência é possível desenvolver dispositivos de baixo consumo, uma vez que a contagem de períodos é feita através de resposta a interrupção. Deste modo, e tendo em conta que os registos de valor de contagem apenas permitem a configuração de 2 B (máximo de 65535 períodos de *clock*), uma frequência de 1 MHz corresponderia a uma interrupção a cada 65 µs. Como tal, são sempre configurados dois *clocks*, sendo que o principal – que regula a contagem durante os períodos adormecidos dos dispositivos sensores – é sempre de baixa frequência.

Para os controladores de aplicação dos dispositivos *gateway*, o único *timer* é configurado com base num cristal externo de quartzo, de 4 MHz, sendo a frequência configurada de 2 MHz.

Para os controladores de aplicação dos dispositivos sensores, associados a controladores de comunicações configurados como *End Devices*, são configurados dois *timers*, sendo que o primeiro, gerado a partir do DCO interno de 4MHz, é usado apenas para calibrar o segundo

timer, uma vez que este é gerado a partir do VLO, um *clock* de baixa fiabilidade. Adicionalmente, DCO interno é usado para gerar os *clocks* de interface série SPI.

Quanto ao controlador de comunicações para a rede *ZigBee*, este contém todos os periféricos necessários, pelo que não carece de configuração adicional.

Quanto ao controlador de comunicações de rede 433 MHz, tem nas suas entradas de geradores de *clock* um cristal de 26 MHz a partir do qual se obtém um *clock* de 12 MHz, e um RTC gerado a partir de um cristal de 32 KHz, sendo este o que se mantém ligado durante os períodos de "adormecimento" do microcontrolador.

4.3.4. Verificação do nível de bateria

O nível de bateria é controlado através de uma função interna dos microcontroladores MSP430, e que consiste na conversão para o domínio digital da tensão de entrada no pino Vcc (pino de alimentação). Esta funcionalidade designa-se de SVS (*Supply Voltage Supervisor*), e a função associada é configurada para comparar o valor de entrada com 3 V. Apesar de, tal como se verá, esta tensão ser bastante inferior à tensão de alimentação, de 3,3 V, e de a performance da bateria escolhida ser bastante alta, foi configurado um valor mais baixo para combater o efeito de abaixamento da tensão fornecida pela bateria após aumento da carga imposta pelo sistema. Desse modo, e com base nos testes feitos, verificou-se que a medição de 3 V após um período adormecido permite ainda uma autonomia do dispositivo de algumas semanas (para as aplicações consideradas), possibilitando o agendamento de manutenção. Quando o valor medido for inferior a 3 V, e tendo em conta que um microcontrolador MSP430 apenas funciona com tensões de 2,8V, será gerado um alarme e enviada uma mensagem de alerta para o servidor. A referida mensagem é enviada diariamente, para não incorrer num factor de gasto adicional de bateria. A função que implementa este processo é designada de *verifica_SVS*.

4.3.5. Modo adormecido

Todas as referências a modos adormecidos de microcontroladores programados no âmbito destes projectos referem-se ao modo LPM3 (*Low Power Mode 3*) do microcontrolador MSP430. Neste modo de funcionamento do microcontrolador, apenas o *clock* auxiliar (ACLK), se mantém ligado, servindo para fazer contagens do temporizador, e podendo assim programar períodos para acordar novamente o dispositivo. No LPM3, os módulos CPU, *Main clock* e gerador de *clock* DCO encontram-se desligados. Na figura seguinte são apresentados os consumos típicos em cada modo adormecido, para alimentações de 3 e 2,2V.

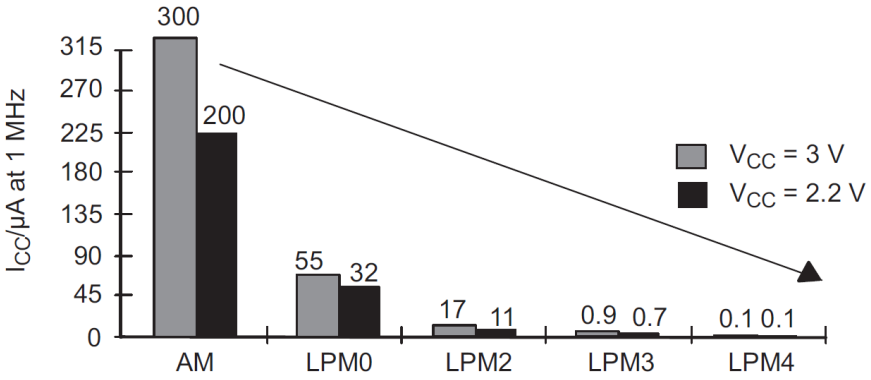


Figura 81 - Consumos dos diferentes modos de baixa potência.

4.4. Aplicações integradas sobre o protocolo *ZigBee*

Sobre a rede *ZigBee* foi desenvolvido um sistema para monitorização de estado técnico de equipamentos de transmissão de movimento em ambiente industrial, através da medição de variáveis de vibração segundo 3 eixos e de temperatura. A aquisição de valores de vibração – aceleração ou velocidade RMS (*Root Mean Square* – Valor Quadrático Médio, ou valor eficaz), calculadas com aquisições de dados durante cerca 2 segundos – é feita através de medição periódica, existindo a possibilidade de efectuar pedidos de aquisição de um conjunto contínuo de dados, para análise de vibrações no domínio das frequências, por parte do utilizador. Adicionalmente, existem tipicamente equipamentos que necessitam de uma taxa de transmissão de dados na casa dos 0,5 Hz e outros que aceitam valores bastante inferiores, na casa de 1 por minuto.

Como tal, e tendo em conta estes constrangimentos, trata-se de um sistema que necessita de todas as valências de uma rede de tipo híbrido, tal como foi descrita no capítulo Arquitectura Geral do Sistema. Sensores alimentados pela rede eléctrica local monitorizarão os equipamentos que necessitam de uma taxa de transmissão mais elevada (desde que exista alimentação próxima) e equipamentos com necessidades de refrescamento de dados mais baixas serão equipados com sensores sem fios, alimentados a bateria. Adicionalmente, os dados adquiridos pelos sensores de rede cablada serão integrados na rede sem fios via *Routers* com funções de *gateway* para rede cablada, que permitem ainda o aumento do alcance da rede, possibilitando a instalação de sensores em posições mais remotas.

Este sistema foi primeiro implementado através do protocolo *ZigBee*, com base nos dispositivos:

- Coordenador, que para além da criação e gestão de rede executa funções de *gateway* entre a rede sem fios e o *backbone* da rede geral;

- *Router*, que para além de permitir a associação de dispositivos à rede sem fios executa a integração de sensores de rede cablada, sendo uma *gateway* rede sem fios/rede cablada, para além do reencaminhamento de sensores sem fios sem alcance para comunicação directa com o Coordenador;
- *End Device*, para monitorização de equipamentos remotos, com baixas taxas de aquisição de dados e sem acesso a rede eléctrica;
- Sensor de rede cablada, para monitorização de equipamentos remotos com necessidade de alta taxa de aquisição.

O último dispositivo – sensor de rede cablada – não pertence formalmente à rede sem fios, estando apenas "pendurado" num dispositivo *Router*, através do mecanismo de endereçamento descrito na secção Encaminhamento de mensagens em redes sem fios híbridas do capítulo 3.

Um dispositivo Coordenador ou *Router* tem o mesmo *hardware*, variando apenas o programa de controlo que irá correr, de acordo com as funções permitidas que serão carregadas aquando da sua configuração. Assim, um dispositivo deste tipo tem a função de gerir as duas interfaces de comunicações que detém, tal como apresentado na Figura 82.

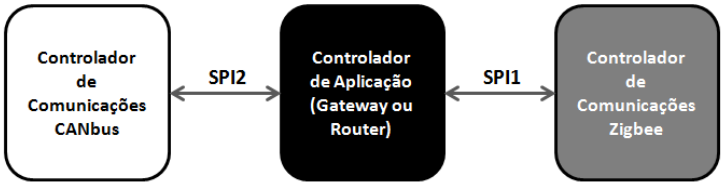


Figura 82 - Interfaces da *gateway ZigBee* para AP e *Routers*.

Quanto ao controlador de aplicação de um *End Device*, tem como função a recolha periódica de dados de dois sensores, que controla através de SPI, e sua transmissão através do controlador de comunicações (bem como a respectiva recepção de dados). O esquema representativo desta arquitectura está apresentado na Figura 83.

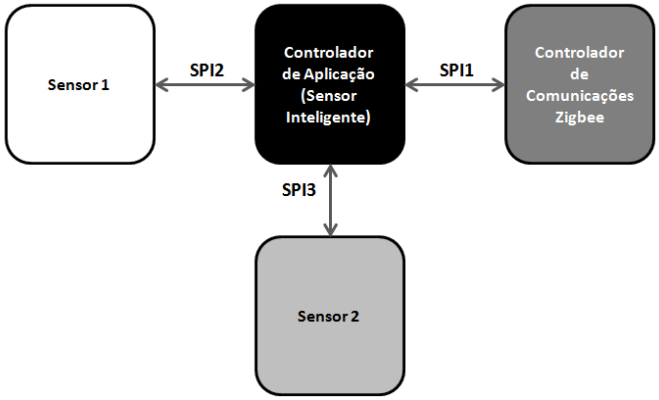


Figura 83 - Interfaces do *End Device ZigBee*.

A rede segue o esquema descrito na secção Protocolo *ZigBee PRO* do capítulo 2.

Nos seguintes tópicos de secção são descritas as diferentes funções que definem o funcionamento dos dispositivos acima descritos (exceptuando os sensores de rede cablada), não sendo descritas tão aprofundadamente as questões relacionadas com as comunicações CAN e de interface com sensores quanto as que estão associadas à interface com o controlador de comunicações *ZigBee*, a gestão do dispositivo e de *buffers* internos de informação, uma vez que aquelas não foram desenvolvidas no âmbito deste trabalho, tendo sido feito um esforço de para a sua compatibilização.

4.4.1.API para controlador de comunicações *ZigBee*

A comunicação com controlador de comunicações CC2530 é possível através de um conjunto de funções que constituem a sua API. Estas estão divididas por:

- *SYS INTERFACE* – baixo nível: para configuração de periféricos (ADC, GPIOs), *reset* por *software*, manutenção de dados em memória após *reset*, etc.
- *CONFIGURATION INTERFACE* – para configuração de registos de inicialização, sejam dedicados à rede ou ao dispositivo;
- *SIMPLE API INTERFACE* – conjunto básico de comandos que permitem criar uma rede *ZigBee*;
- *AF INTERFACE (APPLICATION FRAMEWORK)* – *stack ZigBee* completa – opção implementada;
- *ZDO INTERFACE* – interface à camada ZDO, não foi implementada pelas razões já apresentadas.

Basicamente, são usadas funções dos quatro primeiros conjuntos, sendo que se optou por usar a *AF Interface* (inclui funções de transmissão e recepção de mensagens, bem como serviço de *acknowledgement* e registo de aplicação na rede) por ter mostrado melhores resultados em termos de performance – menos erros em comunicações SPI – apesar da maior simplicidade da *Simple API Interface*.

Segue-se a descrição do conjunto de funções desenvolvidas e comandos da API de interface com o dispositivo CC2530 da *Texas Instruments*, controlador de comunicações já programado com *stack ZigBee*, num dispositivo *gateway* que efectuasse uma interface entre a rede cablada *CANbus* e uma rede *ZigBee*.

4.4.1.1. Inicialização do módulo CC2530 - *inicia_CC2530*

Esta função executa a inicialização do módulo CC2530, a sua configuração e consequente inicialização da *stack ZigBee*. A função não tem qualquer entrada. É ainda determinado se se

mantêm as anteriores configurações de rede e de utilizador (valores guardados em memória do controlador de comunicações) ou se são apagadas:

- Reset por *hardware* ao módulo, através do pino de *reset* correspondente;
- Verificação do ponteiro *reset_estado*, se está activo (igual a 1);
    - apaga a anterior configuração de rede e utilizador, correndo:
        - a função *guarda_config*, com o parâmetro ZCD_NV_STARTUP_OPTION e o valor a este associado de 3 (eliminação de configurações);
        - a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI, retornando OK_SPI ou NOK_SPI;
- caso a saída tenha sido NOK_SPI, sai da função com a saída NOK_SPI;
- volta a colocar a manutenção de dados após *reset* correndo:
    - a função *guarda_config*, com o parâmetro ZCD_NV_STARTUP_OPTION e o valor a este associado de 0 (manutenção de configurações em memória);
    - a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI retornando OK_SPI ou NOK_SPI;
- caso a saída tenha sido NOK_SPI, sai da função com a saída NOK_SPI;
- executa a função de configuração de parâmetros *configura_RF*, retornando OK_SPI ou NOK_SPI;
- caso a saída tenha sido NOK_SPI, sai da função com a saída NOK_SPI;
- executa a função de inicialização da *stack*, retornando OK_STACK ou NOK_STACK;

Finalmente, a função tem os seguintes parâmetros de saída:

Tabela 29 - Códigos de saída da função *inicia_CC2530*.

Código	Valor	Descrição
OK_STACK	1	Todas as funções de configuração e inicialização foram bem sucedidas
NOK_STACK	2	Erro na inicialização da *stack*
NOK_SPI	3	Erro numa das etapas de configuração

4.4.1.2. Inicialização da *stack* - *inicia_ZB*

Esta função envia a invocação de início da *stack ZigBee*, após configuração do dispositivo controlador de comunicações. A função não tem qualquer entrada.

- Corre a função *guarda_config*, com o parâmetro ZB_START_REQUEST e o valor a este associado de 0 (iniciar a *stack*);
- Corre a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI retornando esta o valor OK_SPI ou NOK_SPI;
- Aguarda durante o tempo AGUARDA_INIT que o controlador de comunicações envie a resposta monitorizando o pino SRDY (as interrupções encontram-se desactivadas);
- Caso baixe durante o tempo previsto:
    - Responde à descida com a função *poll*, de recuperação de dados do dispositivo *slave*;
    - Caso a função *poll* tenha a saída OK_SPI:
        - Sai da função com o valor OK_STACK;
    - Caso contrário
        - Sai da função com o valor NOK_STACK;
- Caso contrário:
    - Sai da função com o valor NOK_STACK.

Tabela 30 - Códigos de saída da função *inicia_ZB*.

Código	Valor	Descrição
OK_STACK	1	Inicialização da *stack* bem sucedida
NOK_STACK	2	Erro na inicialização da *stack* do lado do controlador de comunicações ou erro na comunicação SPI

4.4.1.3. Configuração inicial do controlador de comunicações - *configura_RF*

Esta função executa a configuração inicial de parâmetros do módulo de comunicações, tendo como entradas:

Tabela 31 - Variáveis de entrada da função *configura_RF*.

Código	Dimensão	Descrição
panid	2 B	Identificador de rede *pan id*
canal1	4 B	Máscara para definir o conjunto de canais para operação - valor MS
canal2	4B	Máscara para definir o conjunto de canais para operação - valor LS

Sendo o processo associado o seguinte:

- Corre a função *guarda_config*, com o parâmetro SET_TX_POWER e o valor a este associado de *potencia_rf* (potência de transmissão);
- Corre a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI retornando esta o valor OK_SPI ou NOK_SPI;
- Caso a função *envia_SREQ_RF* tenha a saída NOK_SPI:
    - Sai da função com o valor NOK_SPI;
- Corre a função *guarda_config*, com o parâmetro ZCD_NV_PRECFGKEY e o valor associado de chave de encriptação (16 B);
- Corre a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI retornando esta o valor OK_SPI ou NOK_SPI;
- Corre a função *guarda_config*, com o parâmetro ZCD_NV_PRECFGKEYS_ENABLE e o valor associado de 0 (difusão de chave de encriptação);
- Corre a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI retornando esta o valor OK_SPI ou NOK_SPI;
- Corre a função *guarda_config*, com o parâmetro ZCD_NV_LOGICAL_TYPE e o valor associado de *func_rede_ZB* (tipo de dispositivo de rede);
- Corre a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI retornando esta o valor OK_SPI ou NOK_SPI;
- Caso a função *envia_SREQ_RF* tenha a saída NOK_SPI:
    - Sai da função com o valor NOK_SPI;
- Verificação do ponteiro *reset_estado*, se está activo (igual a 1);
    - apaga a anterior configuração de rede e utilizador, correndo:
        - a função *guarda_config*, com o parâmetro ZCD_NV_STARTUP_OPTION e o valor a este associado de 2 (eliminação de configurações de rede);
        - a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI, retornando OK_SPI ou NOK_SPI;
    - Caso a função *envia_SREQ_RF* tenha a saída NOK_SPI:
        - Sai da função com o valor NOK_SPI;
- Corre a função *af_register* (registo da aplicação microcontrolador no controlador de comunicações, para acesso de outros dispositivos da rede), e caso tenha a saída NOK_SPI:
    - Sai da função com o valor NOK_SPI;
- Corre a função *config_dev_specific* (configuração de parâmetros únicos ao dispositivo), e caso tenha a saída NOK_SPI:

    - Sai da função com o valor NOK_SPI;
- Sai da função com o valor OK_SPI.

A função tem como saída um dos seguintes parâmetros:

Tabela 32 - Códigos de saída da função *configura_RF*.

Código	Valor	Descrição
OK_SPI	1	Configurações bem sucedidas.
NOK_SPI	2	Erro na comunicação de configurações.

4.4.1.4. Função de verificação de associação à rede e obtenção de dados associados - *get_CC2530_info*

A função *get_CC2530_info* permite a verificação de associação à rede ou inicialização à rede (caso do Coordenador), através da obtenção de parâmetros associados a uma correcta inicialização (identificador de estado de ligação à rede – CC2530_STATE, PAN ID, identificador de rede, etc.). Esta verificação serve para aguardar que o dispositivo controlador de comunicações tenha tempo para se ligar à rede, uma vez que a inicialização correcta da *stack* não implica uma finalização dos processos de formação e/ou associação de rede. A função não tem qualquer entrada.

- Enquanto tempo de verificação for inferior a TEMPO_VER_LIGAÇÃO e estado_ZB (ponteiro igual ao parâmetro CC2530_STATE) for diferente do seu correspondente de ligação (Coordenador = DEV_ZB_COORD, *Router* = DEV_*ROUTER*, *End Device* = DEV_END_DEVICE):
    - Executar *get_dev_info*(CC2530_STATE);
    - Aguardar um período de 1000 ciclos;
- Caso tempo de verificação = TEMPO_VER_LIGAÇÃO:
    - Reset ao controlador de aplicação;
- Caso dispositivo seja o Coordenador:
    - Executar *get_dev_info*(CC2530_SHORT_ADDRESS) – endereço de rede;
    - Executar *get_dev_info*(CC2530_CHANNEL) – canal de operação;
    - Executar *get_dev_info*(CC2530_PANID) – PAN ID da rede;
    - Executar carregar_lista_envio_CAN (carregar *buffer* de transmissão *CANbus*) destinado ao dispositivo central com informação de rede (função INSCRICAO com dados de AP);
- Caso contrário;
    - Executar *get_dev_info*(CC2530_SH_ADD_PARENT);

- Executar carregar_lista_envio_ ZB (carregar *buffer* de transmissão *ZigBee*) destinado ao dispositivo central com informação de dispositivo (função INICIALIZACAO_OK com dados de inicialização do dispositivo);

- Sai da função

4.4.1.5. Registo de aplicação na rede - *af_register*

- Carrega parâmetros de registo em *buffer msg_out* (usado pela função *envia_SREQ_RF*;
- Corre a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI retornando esta o valor OK_SPI ou NOK_SPI;
- Aguarda por sinalização do pino SRDY, indicador de mensagem do controlador de comunicações;
- Executa função *recebe_msg_RF,* de recepção por SPI da unidade rádio retornando esta o valor OK_SPI ou NOK_SPI;
- Retorna OK_SPI ou NOK_SPI;

Os códigos de saída são os seguintes:

Tabela 33 - Códigos de saída da função - *af_register*.

Código	Valor	Descrição
OK_SPI	1	Aplicação foi registada.
NOK_SPI	2	Registo de aplicação falhou por erro na SPI.

4.4.1.6. Gestão e acesso a tabelas de conversão de identificadores - verifica_idzb e procura_GW

Estas funções são partilhadas com a rede 433 MHz, sendo aplicável a descrição feita em Gestão e acesso a tabelas de conversão de identificadores, no capítulo anterior.

4.4.1.7. Transmissão e recepção de mensagens da rede – af_data_request e pedidos AF_DATA_CONFIRM E AF_INCOMING_MSG

A função *AF_DATA_REQUEST,* na terminologia da API do controlador CC2530 permite a transmissão de uma mensagem de uma aplicação *ZigBee* para outra aplicação *ZigBee*, tendo sido esta a função usada para transmissão de dados entre nós. Foi desta forma implementada uma função com a mesma denominação, que tem como entrada apenas a função a implementar pela aplicação remota, uma vez que os restantes parâmetros necessários são comuns a todas as mensagens (*end point destinatário, end point emissor, cluster id, trans id, options-acknowledgement*, *radius – raio máximo*) ou estão guardadas na mensagem guardada no *buffer* de transmissão (tamanho da mensagem, id geral de rede do destinatário, *payload* da mensagem).

Na figura seguinte é apresentado o formato da trama enviada através da função *af_data_request*.

1	1	1	2	1	1
Length = 0x0A-0x5E	Cmd0 = 0x24	Cmd1 = 0x01	DstAddr	DestEndpoint	SrcEndpoint

2	1	1	1	1	0-128
ClusterID	TransID	Options	Radius	Len	Data

Figura 84 - Formato da trama enviada através da função *af_data_request*.

Relativamente à função implementada no controlador de aplicação, executa o seguinte processo:

- Carrega parâmetros fixos ((*end point destinatário, end point emissor, cluster id, trans id, options- acknowledgement*, *radius – raio máximo*);
- Se se trata da *gateway* central, que também consiste no AP:
    - Corre a função *procura_GW*(id geral do destinatário,0), que devolve o identificador de rede *ZigBee* do destinatário;
    - Caso o resultado seja 0, devolve o parâmetro ID_INEX, indicativo que o identificador não existe em memória, e sai da função;
- Caso contrário, carrega o único identificador de rede *ZigBee* conhecido, que será a *gateway* central;
- Carrega os últimos parâmetros no *buffer* de saída msg_out;
- Corre *envia _SREQ_RF*
    - Caso devolva NOK_SPI, sai da função com o respectivo código de saída;
- Sai da função, a resposta (com o *acknowledgement*) virá por interrupção;

Deste modo, o código de saída da função poderá ser um de:

Tabela 34 - Códigos de saída associados da função *af_data_request*.

Código	Valor	Descrição
OK_SPI	1	Mensagem transmitida.
NOK_SPI	2	Erro na comunicação SPI.
ID_INEX	3	Identificador de rede geral inserido é desconhecido.

À função *AF_DATA_REQUEST*, o controlador de comunicações responde sempre com a função *AF_DATA_CONFIRM*, que indica o resultado da transmissão, com um dos dois seguintes valores:

Tabela 35 - Códigos de saída associados à resposta a AF_DATA_CONFIRM, indicativos da recepção (ou não) de *acknowledgement*.

Código	Valor	Descrição
ZSUCCESS	0	*Acknowledgement* recebido.
ZAPSNOACK	2	*Acknowledgement* não foi recebido

Com a resposta *AF_DATA_CONFIRM*, o controlador de aplicação poderá limpar a *flag* de verificação de *acknowledgement* associado a um determinado dispositivo, tomando uma de duas opções:

- Caso seja o Coordenador:
    - Transmite uma mensagem para a unidade central, com a informação de falha na transmissão para o dispositivo *n*;
- Caso seja um *Router* ou ED:
    - Incrementa o ponteiro de *falhas_acknowledgement*, sendo que à terceira falha reinicia o processo de ligação à rede;

4.4.1.8. Pedido de dados de rede – get_dev_info

A função get_dev_info transmite um pedido ZB_GET_DEVICE_INFO (na API do controlador de comunicações CC2530 e estabelece automaticamente os ponteiros correspondentes em memória.

A função ZB_GET_DEVICE_INFO permite o conhecimento dos seguintes parâmetros:

Tabela 36 – Parâmetros reconhecíveis através da função ZB_GET_DEVICE_INFO.

Código	Dimensão	Descrição
0	1 B	Estado do dispositivo
1	8 B	Endereço MAC do dispositivo
2	2 B	Endereço de rede do dispositivo
3	2B	Endereço de rede do dispositivo pai
4	8 B	Endereço MAC do dispositivo pai
5	1 B	Canal de operação
6	2 B	PAN ID da rede
7	8 B	PAN ID extenso da rede

Tem como entrada o parâmetro a verificar, e processa-se de acordo com o seguinte método:

- Carrega parâmetros de pedido
- Corre a função *guarda_config*, com o parâmetro ZB_GET_DEVICE_INFO e o valor a este associado de *parâmetro*;
- Corre a função *envia_SREQ_RF* com a anterior mensagem, de transmissão por SPI retornando esta o valor OK_SPI ou NOK_SPI;
- Caso a função *envia_SREQ_RF* tenha a saída NOK_SPI:
    - Sai da função com o valor NOK_SPI;
- Devolve a resposta do CC2530, como saída, podendo ser um dos valores da seguinte tabela.

Tabela 37 - Códigos de saída associados à resposta ZB_GET_DEVICE_INFO, indicativos de estados da unidade rádio.

Código	Dimensão
CC2530_STATE	1 B
CC2530_IE3_ADDRESS	8 B
CC2530_SHORT_ADDRESS	2 B
CC2530_SH_ADD_PARENT	2B
CC2530_IE3_ADD_PARENT	8 B
CC2530_CHANNEL	1 B
CC2530_PANID	2 B
NOK_SPI	1 B

4.4.1.9. Carregamento de mensagens SPI – *guarda_config*

A função *guarda_config* tem como utilidade a preparação de mensagens de configuração a transmitir para o controlador de comunicações, carregando-as no *buffer* de transmissão, sendo de seguida apenas necessário correr a função *envia_SREQ_RF*, sem necessidade de inserção de elementos adicionais (esta função não tem qualquer entrada).

Assim, a função tem como entrada os seguintes valores:

- Função interna do CC2530;
- Parâmetros adicionais, de 1 a 4, e associados à função interna.

As funções possíveis são apresentadas na tabela seguinte.

Tabela 38 - Funções CC2530 possíveis para a função *guarda_config*.

Código	Parâmetros	Descrição
ZCD_NV_STARTUP_OPTION	1	Configuração da memória do CC2530
ZCD_NV_CHANLIST	2	Configuração do mascara para o conjunto de canais possíveis
ZCD_NV_PANID	2	Configuração do PAN ID
ZCD_NV_POLL_FAILURE_RETRIES	1	ED: tentativas possíveis de falha de *poll* até reiniciar ligação à rede
SET_TX_POWER	8 B	Configuração da potência de comunicação
GET_DEV_INFO	1 B	Pedido de informação do CC2530 / rede
ZB_START_REQUEST	2 B	Ordem de inicialização da *stack ZigBee*
ZCD_NV_INDIRECT_MSG_OUT	1 B	Tempo que um dispositivo pai mantém em memória uma mensagem destinada a um dispositivo terminal seu filho (associado a processo de *polling*)
ZCD_NV_LOGICAL_TYPE	1 B	Configuração do tipo de dispositivo

Cada uma das funções CC2530 tem um conjunto de parâmetros associados, sendo que aqueles que são inseridos através da função *guarda_config* são os que correspondem ao valor configurável.

Para escrita de configurações no CC2530 é utilizada a função *ZB_WRITE_CONFIGURATION,* da interface SYS. Esta tem o seguinte formato de trama:

Tamanho	Cmd0	Cmd1	ConfigId	Len	Parâmetros
3 – 131 B	1 B	1 B	2 B	1 B	1-128 B

Figura 85 - Trama de escrita de configuração no CC2530.

Onde o Cmd0 e Cmd1 constituem o campo de comando, sendo que o Cmd0 indica o tipo e subsistema associados à mensagem:

- O tipo corresponde ao tipo de mensagem:
  - 0: Poll
  - 1: SREQ
  - 2: AREQ
  - 3: resposta a SREQ
- O subsistema corresponde à área funcional do comando, tal como foi atrás apresentada:

- 1: Interface SYS
- 4: Interface AF
- 5: Interface ZDO
- 6: Interface *Simple API*

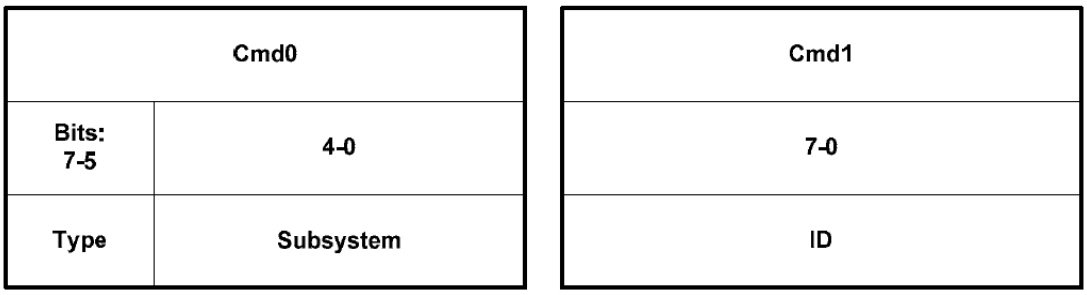


Figura 86 - Campo de comando da trama de comunicação com CC2530. Fonte: *Texas Instruments*.

O campo Cmd1 corresponde a outros parâmetros associados a cada função trocada. Relativamente à função de configuração de parâmetros, *ZB_WRITE_CONFIGURATION*, os parâmetros associados são os apresentados na Figura 85. Adicionalmente, campo *ConfigID* corresponde às diferentes configurações possíveis.

Como exemplo, a máscara de canais possíveis de operação, correspondente à função ZCD_NV_CHANLIST, é configurável através da transmissão da mensagem:

Tamanho	Cmd0	Cmd1	ConfigId	Len	Par1	Par2	Par3	Par4
0x07	0x26	0x05	0x0084	0x04	0x00	0x00	0x08	0x00

Figura 87 - Trama a transmitir para o CCC2530 para configuração da máscara associada ao conjunto de canais possíveis. Todos os valores estão em numeração hexadecimal.

Na Figura 87 é apresentado um exemplo de trama a transmitir, considerando que apenas seria possível a comunicação no canal 12 (bit 12), 2,465 GHz.

Deste modo, a função processa-se de acordo com o seguinte método:

- Verifica qual a função;
- Seleciona a opção correspondente, através de *switch*;
- Carrega os valores de cmd0, cmd1, configid e len associados à função no *buffer* de saída;
- Carrega os parâmetros introduzidos par1, par2, par3 e par4;
- Sai da função (não tem código de saída).

4.4.1.10. Transmissão e recepção de dados SPI - *poll*, envia_SREQ_RF e recebe_msg_RF

A transmissão e recepção de dados SPI com o controlador CC2530 processa-se através de três tipos de comunicação:

- SREQ: *synchronous request*, onde uma mensagem é transmitida para o controlador de comunicações CC2530, sendo que a seguir a essa mensagem será recebida uma resposta do CC2530:
- AREQ: *asynchronous request*, onde uma mensagem transmitida pelo controlador de aplicação não tem resposta;
- POLL: o controlador de comunicações tem uma mensagem para o controlador de aplicação, necessitando que lhe sejam transmitidos 3B de valor 0, para que essa mensagem seja respondida com a mensagem que tem para o controlador de aplicação.

As comunicações são regradas através de dois pinos de sinalização:

- SRDY, ou *slave ready*, controlado pelo controlador de aplicação e indicativo de que tem mensagens para transmissão ou que está preparado para recepção;
- SS e MRDY, *slave select e master ready*, pinos que estão ligados no controlador de aplicação e controlam as duas entradas do controlador de comunicações com os respectivos designadores, controlados pelo controlador de aplicação, e indicativos de mensagens para transmitir ou preparação para a sua recepção.

Os esquemas POLL e SREQ estão apresentados nas figuras seguintes. O esquema da comunicação AREQ não é apresentado, uma vez que não é utilizado:

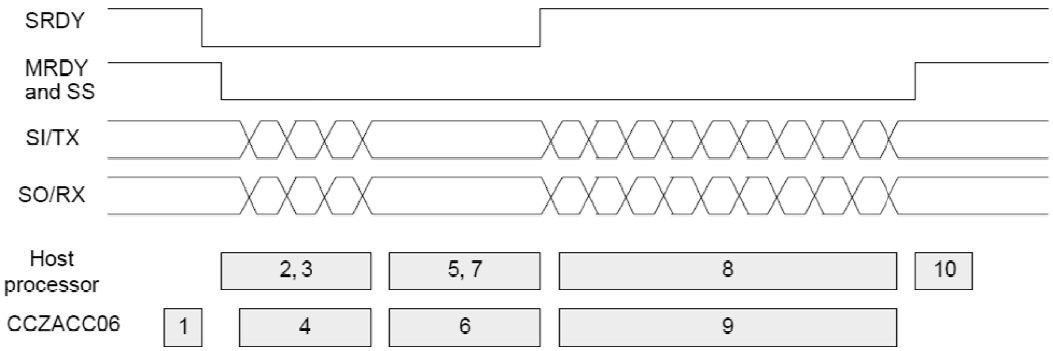


Figura 88 - comunicação POLL entre o controlador de comunicações e o controlador de aplicação. os três primeiros bytes transmitidos pelo controlador de aplicação (2, 3, na barra host processor) despoletam a *transmissão* da mensagem (9, na barra CCZACC06) por parte do CC2530.

A função *recebe_msg_RF* permite a recepção de uma mensagem do CC2530, estando também associada à função envia_SREQ_RF, uma vez que a transmissão de uma mensagem para o

CC2530 resultará sempre numa resposta a esse pedido e à função *poll*. Assim, é usada como recepção de uma mensagem após pedido síncrono e como resposta a pedido assíncrono.

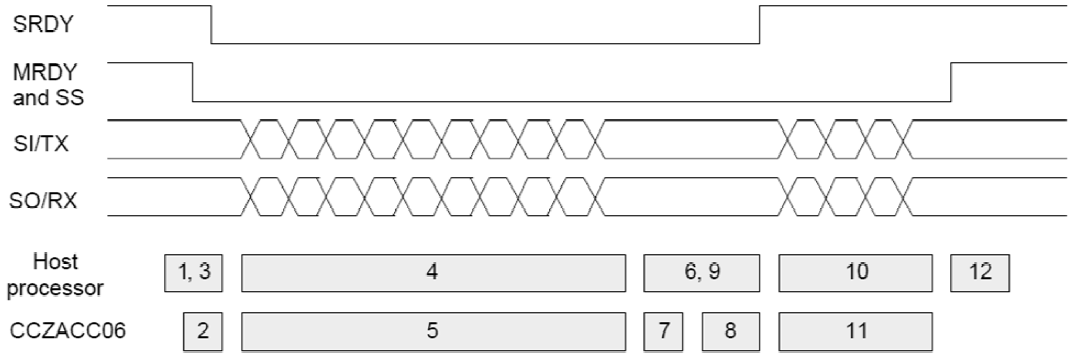


Figura 89 - Esquema da comunicação SREQ entre o controlador de aplicação e controlador de comunicações. Após a *transmissão* da mensagem pelo controlador de aplicação e subida do pino SRDY, o controlador de comunicações enviará a resposta ao pedido (11, na barra CCZACC06).

Uma vez que o esquema de recepção de dados do lado do controlador de aplicação é igual quer se trate de uma resposta a pedido (passo 11 da Figura 89) ou uma transmissão de dados do lado do CC2530 (passo 9 da Figura 88), foi implementada a função *recebe_msg_RF,* que é usada quer para a recepção de dados correspondente à função *poll* quer para a recepção de resposta da função *envia_SREQ_RF*.

Assim, a função *envia_SREQ_RF* processa-se da seguinte forma:

- Desce pino SS
- Aguarda descida do pino SRDY, enquanto não é ultrapassado o período de tempo TEMPO_SRDY;
- Caso o tempo que passou seja igual a TEMPO_SRDY:
    - Sai da função com mensagem de saída NOK_SPI;
- Coloca n = 0;
- Enquanto n < tamanho da mensagem + 3 (os três primeiros bytes não contam para o tamanho da mensagem, visto fazerem parte do protocolo entre controladores, e não da mensagem que será transmitida):
    - Corre função envia_SPI com byte n;
    - Incrementa n;
- Aguarda que pino SRDY desça, enquanto não é ultrapassado o período de tempo TEMPO_SRDY;
- Caso o tempo que passou seja igual a TEMPO_SRDY:
    - Sai da função com mensagem de saída NOK_SPI;
- *Corre função recebe_msg_RF*, recebendo valor NOK_SPI ou OK_SPI;

- Sai da função com código OK_SPI ou NOK_SPI;

Tabela 39 - Códigos de saída da função *envia_SREQ_RF*.

Código	Valor	Descrição
OK_SPI	1	Transmissão bem sucedida
NOK_SPI	2	Erro na comunicação SPI

Relativamente à função *poll*, que é usada após resposta a interrupção por descida do pino SRDY:

- Desce pino SS;
- Aguarda descida do pino SRDY (apenas para detecção de erros, uma vez que já deverá estar a 0), enquanto não é ultrapassado o período de tempo TEMPO_SRDY;
- Caso o tempo que passou seja igual a TEMPO_SRDY:
    - Sai da função com mensagem de saída NOK_SPI;
- Envia três vezes o byte 0, através da função *envia_SPI*;
- Aguarda subida do pino SRDY (apenas para detecção de erros, uma vez que já deverá estar a 0), enquanto não é ultrapassado o período de tempo TEMPO_SRDY;
- Caso o tempo que passou seja igual a TEMPO_SRDY:
    - Sai da função com mensagem de saída NOK_SPI;
- Corre função *recebe_msg_RF*, recebendo valor NOK_SPI ou OK_SPI*;*
- Sai da função com um dos seguintes códigos:.

Tabela 40 - Códigos de saída da função *poll*.

Código	Valor	Descrição
OK_SPI	1	Recepção bem sucedida
NOK_SPI	2	Erro na comunicação SPI

Finalmente, a função que suporta as duas anteriores, *recebe_msg_RF*, processa-se da seguinte forma:

- Recebe primeiro byte, e acerta através desta a variável *length*;
- Coloca $n = 0$;

- Enquanto n < *length* + 2 (uma vez que já foi recebido 1B, e que os outros dois são apenas referentes ao protocolo entre controladores, não à mensagem que está a ser recebida):
    - Recebe byte através da função *recebe_SPI*, e iguala a posição do *buffer msg_in* n ao valor recebido;
    - Incrementa n;
- Sobe pino SS;
- Aguarda subida do pino SRDY (apenas para detecção de erros, uma vez que já deverá estar a 0), enquanto não é ultrapassado o período de tempo TEMPO_SRDY;
- Caso o tempo que passou seja igual a TEMPO_SRDY:
    - Sai da função com mensagem de saída NOK_SPI;
- Sai da função com o valor OK_SPI;

Tabela 41 - Códigos de saída da função *recebe_msg_SPI*.

Código	Valor	Descrição
OK_SPI	1	Recepção bem sucedida
NOK_SPI	2	Erro na comunicação SPI

4.4.1.11. Baixo nível: SPI

A interface SPI está configurada para comunicar a 4 MHz, polaridade de clock 0 e fase 0, com o MSB a ser transmitido primeiro. São usados os seguintes sinais:

- SCK: clock de série, gerado pelo *master;*
- SS e MRDY: *slave select e master ready,* pinos de sinalização ligados entre si e controlados pelo *master*, constituindo duas entradas diferentes do *slave;*
- SIMO: *slave in master out,* saída de dados do *master;*
- SOMI: *slave out master in*, saída de dados do *slave;*
- SRDY: *slave ready*, pino de sinalização controlado pelo *slave.*

4.4.2. Estrutura do Firmware dos dispositivos desenvolvidos sobre o protocolo *ZigBee*

4.4.2.1. Coordenador e *Router – Gateways* com redes de campo

O dispositivo Coordenador de rede é, tal como já foi mencionado, o dispositivo que executa a *interface* entre o *backbone* da rede de campo, ao qual está ligado o dispositivo central, que recebe e apresenta dados a um utilizador.

Deste modo, contém um controlador de comunicações *CANbus* e um controlador de comunicações de rede *ZigBee*, sendo o seu processo de funcionamento apresentado no Fluxograma 11 do Anexo I.

4.4.2.2. *End Device* – sensor inteligente

Também como tem vindo a ser referido, o dispositivo sensor inteligente desenvolvido tem interfaces SPI com dois sensores – um de temperatura e outro de aceleração – sendo que toma o papel de *master* nos dois casos, para além da interface SPI com o controlador de comunicações *ZigBee* CC2530.

O referido controlador de comunicações, quando configurado como *End Device*, tem a particularidade interessante de entrar automaticamente em modo adormecido. Por essa razão não existe uma função na API para controlador de comunicações *ZigBee* que sirva a sua colocação em modo adormecido, ou uma instrução presente no programa de controlo que de seguida se apresenta. A entrada automática em modo adormecido ocorre imediatamente após o fim de uma comunicação SPI a qual não necessita de resposta. Não existindo tarefas para executar pelo controlador de comunicações, este entra imediatamente em modo adormecido.

O controlo de nível de bateria é efectuado através da função descrita na secção Verificação do nível de bateria.

Assim, o processo de inicialização e de funcionamento normal do dispositivo sensor estão apresentados também no Anexo I, sob as referências Fluxograma 12 e Fluxograma 13, respectivamente.

4.5. Aplicações integradas sobre o protocolo 433 MHz

Sobre o controlador de comunicações de rede 433 MHz já descrito, foi criada uma solução ao encontro das necessidades de um cliente da área da distribuição de energia, para a monitorização de equipamentos em subestações eléctricas, tal como apresentado na secção Cenários de Aplicação do capítulo 3. Essa solução inclui a monitorização de disjuntores de alta e média potência, seccionadores e transformadores de alta – média potência. Alguns destes equipamentos estão instalados dentro de edifícios, sendo simples a transmissão dos dados dos sensores associados via rede cablada.

No entanto, os equipamentos que se encontram no parque de linhas, a zona exterior da subestação eléctrica, necessitam de que os dados adquiridos sejam transmitidos sem fios, uma vez que não é possível violar os limites de segurança entre linhas de alta tensão, ao colocar cablagens de comunicação até aos dispositivos sensores, apesar de alguns pontos de medição possibilitarem instalação de uma rede de campo. Como tal, foi criada uma solução híbrida,

integrada sobre um *backbone* de rede de campo *CANbus*, que conta com os seguintes dispositivos:

- *AP – gateway* entre *backbone CANbus* e rede de sensores sem fios;
- *Router – gateway* para sensores com comunicação *CANbus* instalados no exterior, e com capacidade de reencaminhamento de dados de sensores sem fios mais distantes;
- Sensor de aceleração e temperatura sem fios – monitoriza no domínio das frequências o disparo de disjuntores de alta tensão no parque de linhas (apenas adquire dados por evento), através do sensor de aceleração, sendo configurado como *End Device*. A cada aquisição, transmite cerca de 4 KB de dados para a unidade central;
- Sensor de aceleração e temperatura cablado – monitoriza o valor RMS da vibração e a temperatura de um transformador de alta – média tensão, sendo integrado na rede sem fios através de um *Router*, e transmitindo um conjunto de dados adquiridos de 4 em 4 segundos;
- Sensor de corrente cablado – monitoriza a corrente associada a um pico de corrente num transformador de alta – média tensão (apenas adquire dados por evento), sendo integrado na rede sem fios através de um *Router*, transmitindo cerca de 50 KB a cada aquisição;
- Sensor de alinhamento para seccionadores – monitoriza seu o alinhamento – entre dois braços de um seccionador no parque de linhas, periodicamente. Consiste num dispositivo que inclui apenas um microcontrolador, sendo uma adaptação do dispositivo *End Device* do protocolo 433 MHz, que inclui os dois sensores. Visto que sai do âmbito deste trabalho – de uma plataforma modular –, não é aqui explorado.

Através deste conjunto de dispositivos criou-se uma solução para monitorização de subestações eléctricas.

Os dados transmitidos para a referida unidade central, ligada ao *backbone CANbus*, são transferidos através de ligação série para um dispositivo com capacidade de comunicação GPRS, e daí transmitidos para a base de dados de um servidor, ficando assim acessíveis a interfaces de utilizador, na forma descrita no capítulo 3, Rede Geral de Comunicações.

4.5.1.API para controlador de comunicações 433 MHz

4.5.1.1. Transmissão e recepção de mensagens - *envia_msg_CC430* e *recebe_msg_CC430*

A função *envia_msg_CC430* permite a transmissão de uma mensagem para o controlador de comunicações CC430, tendo como único parâmetro a função de camada de aplicação a enviar. Segue o processo descrito abaixo que, em caso de erro na comunicação através da SPI, tem como primeiro método de resolução um desbloqueio através da variação do pino de sinalização:

- Desliga interrupções;
- Coloca o valor i = 0;
- Enquanto i < TENTATIVAS_SPI:
    - Corre função envia_SREQ_CC430;
    - Caso a saída seja OK_SPI:
        - *Break* – sai do ciclo;
    - Caso contrário:
        - Liga interrupções;
        - Aguarda durante tempo ESPERA_REP_SPI;
        - Incrementa em 1 unidade o valor i (até TENTATIVAS_SPI);
        - Desliga interrupções;
- Se i = TENTATIVAS_SPI:
    - Baixa pino de sinalização SS;
    - Aguarda tempo ESPERA_TENTATIVAS_SPI;
    - Sobe pino de sinalização SS;
- Caso seja um *Router* ou AP:
    - Coloca ponteiro radio_livre a 1;
- Caso seja um *End Device*:
    - Aguarda que o pino de sinalização SRDY desça;
    - Corre função recebe_msg_CC430;
    - Corre interpreta_msg_CC430;
- Liga interrupções;
- Sai da função.

O ponteiro radio_livre proporciona conhecimento sobre o estado do controlador de comunicações, uma vez que o controlador de aplicação, ao efectuar qualquer pedido ao controlador de comunicações, sai da função de comunicação, ficando do lado do controlador de comunicações a responsabilidade de responder ao pedido. Desta forma, é necessário que o programa do controlador de aplicação tenha conhecimento, em qualquer momento, de que o controlador de comunicações se encontra a efectuar uma ordem – como a transmissão de uma mensagem para a rede – e que não poderá fazer outro pedido antes de receber a resposta. Trata-se de um ponteiro global, conhecido em todas as funções.

Relativamente à função recebe_msg_CC430 – que corre como consequência da resposta a interrupção no pino de entrada SS (*Slave Ready)* do controlador de aplicação (pino de sinalização controlado pelo controlador de comunicações), segue o processo abaixo descrito:

- Baixa pino de sinalização SPI *SS* (*Slave Select*);

- Coloca variável *length* igual a FF (o protocolo de sincronização SPI foi já descrito na secção Interface controlador de Comunicações – controlador de Aplicação do anterior capítulo) e variável falhas_SPI = 1;
- Enquanto *length* = FF
    - Corre função de recepção de um byte por SPI recebe_SPI_CC430, e iguala-a a *length*;
    - se *length* seja igual a 0:
        - Coloca *length* = FF;
        - Incrementa falhas_SPI;
    - Se falhas_SPI > 2:
        - Sobe pino SS;
        - Sai da função com valor NOK_SPI;
- Coloca variável *índice* = *length*;
- Enquanto *índice* < *length* +1 :
    - Iguala posição *índice* do *buffer* de recepção à saída da função recebe_SPI_CC430;
    - Incrementa índice;
- Sobe pino de sinalização SS;
- Enquanto tempo_resposta_SPI < TEMPO_SPI e pino de sinalização SRDY = 0:
    - Incrementa tempo_resposta_SPI;
- Se tempo_resposta_SPI = TEMPO_SPI:
    - Baixa pino SS;
    - Aguarda n contagens de *clock*;
    - Sobe pino SS;
    - Sai da função com código NOK_SPI;
- corre função interpreta_mensagem_CC430;
- Sai da função com código OK_SPI.

Tabela 42 - Códigos de saída da função *recebe_msg_CC430*.

Código	Valor	Descrição
OK_SPI	1	Mensagem recebida.
NOK_SPI	2	Erro na recepção SPI.

4.5.1.2. Interpretação de mensagens MSG_DADOS E MSG_CONFIGURAÇÃO – interpreta_msg_CC430

Esta função corre no seguimento da recepção de uma mensagem do controlador de comunicações, podendo essa mensagem ser de configuração ou de dados. Esta interpretação

fornece uma primeira triagem de uma mensagem recebida da rede sem fios, sendo que uma mensagem de configuração será imediatamente interpretada, e uma mensagem de dados será passada para a função de interpretação da aplicação.

A função não tem qualquer entrada, visto que a mensagem a interpretar ainda se encontra guardada no *buffer* de recepção. Segue o processo descrito abaixo:

- Se é uma mensagem de configuração (verificação do segundo byte do *buffer*):
    - Switch com as diferentes funções:
        - INICIALIZACAO_OK (função de confirmação de associação à rede – caso *Router* – ou de formação da rede – caso AP):
            - Caso seja um *Router*:
                - Carrega no *buffer* de transmissão mensagem via rede sem fios, com parâmetros do dispositivo;
            - Caso seja um AP:
                - Carrega no *buffer* de transmissão mensagem via rede CAN, com parâmetros de dispositivo;
            - Caso seja um ED:
                - Coloca ponteiro modo_funcionamento = 0;
                - Coloca ponteiro standby = 0;
            - Coloca ponteiro radio_livre a 0;
            - Sai da função;
        - RESET_EWS (confirmação da recepção da ordem de *reset*):
            - Corre função *reset* (reinicia o próprio controlador);
        - ACKNOWLEDGE (confirmação da recepção da mensagem pelo seu destinatário imediato):
            - Se é um AP ou *Router*:
                - Coloca variável ver_buffers = 0;
                - Enquanto variável ver_buffers < NÚMERO_DE_BUFFERS:
                    - variável_verifica = buffer posição *ver_buffers*;
                    - se variável_verifica = BUFFER_EM_TX (só poderá haver um *buffer* referente à mensagem em transmissão):
                        - Coloca *variável_verifica* = BUFFER_LIVRE;
                - Se é um ED:

                - Ponteiro acknowledge = CHEGOU;
            - Coloca ponteiro radio_livre = 0;
            - Sai da função;
        - ERRO_*TRANSMISSÃO* (mensagem não foi transmitida):
            - Coloca ponteiro radio_livre = 0;
            - Se for um ED:
                - Ponteiro acknowledge = NÃO_CHEGOU;
                - Sai da função;
            - Coloca variável ver_buffers = 0;
            - Enquanto variável ver_buffers < NÚMERO_DE_BUFFERS:
                - variável_verifica = buffer posição *ver_buffers*;
                - se variável_verifica = BUFFER_EM_TX (só poderá haver um *buffer* referente à mensagem em transmissão):
                    - se for um AP:
                        - carrega no buffer de transmissão CAN mensagem de erro;
                    - se for um *Router*:
                        - Coloca *variável_verifica* = BUFFER_OCUPADO;
            - Sai da função;
- Se é uma mensagem de dados (verificação do segundo byte do *buffer*):
    - Se é para o próprio dispositivo:
        - Corre processa comando;
    - Se é para outro dispositivo:
        - Se tamanho < 10:
            - Carrega em *buffer CANbus*;
        - Se tamanho > 10:
            - Implementa processo de recepção de mensagem de grande tamanho;
    - Sai da função.

O processo de recepção de mensagens de grande tamanho é descrito no tópico de secção seguinte.

4.5.1.3. Transmissão de uma mensagem de grande dimensão – gravaEnviaFFT3E, executar_lista_envio_433M_V2 e verifica_Ctransporte

A referida função é executada para a transmissão de grandes quantidades de dados – veja-se que a aquisição de FFT (*Fast Fourier Transform*) gera 1920 B por eixo, pelo que é necessário transmitir 5760B, quase 6KB. Como tal, a informação fica guardada em memória, sendo depois seccionada e transmitida através desta função, que agrega dados de duas formas:

- Uma vez que cada valor adquirido pelo sensor de aceleração tem 12 bits, sendo necessário guardá-lo em 2B, dois valores são agregados de acordo com o esquema da Figura 90, ocupando apenas 3B, em vez de 4B;
- Transmitir mensagens de n B (implementou-se 24B) de dados, ao invés de 6B;

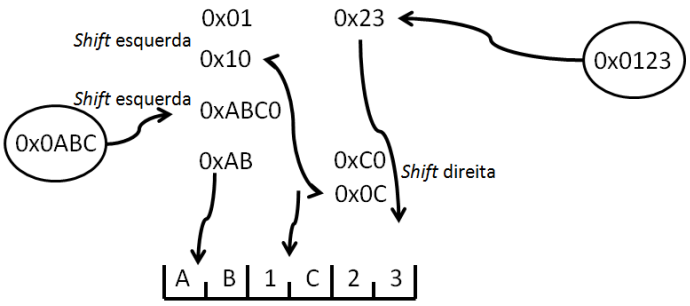


Figura 90 - Esquema de agregação de dois valores de 12 bits em três de 8 bits.

Este processo é executado pela função (adaptada) de interface com o sensor de aceleração gravaEnviaFFT3E que, antes de correr a função envia_msg_CC430, coloca em memória os dados referentes à função de grande dimensão, através do procedimento normal de utilização da função prepara_msg_CC430. O processo é o seguinte:

- Desliga interrupções;
- Agrega todos os dados dois a dois gerando um total de 1920 B por eixo;
- Coloca n = 0;
- Enquanto n < (1920/24) (isto é, enquanto houver dados para transmitir):
    - Corre prepara_msg_CC430 com indicação da função FFT_EIXO_A (sendo A igual a X, Y ou Z);
    - Corre envia_msg_CC430, com indicação de mensagem de dados e FFT_EIXO_A;
- Executa o mesmo procedimento para os restantes dois eixos;
- Liga interrupções;
- Sai da função.

Do lado da *gateway*, existe uma função correspondente, que faz o processo oposto de separação de mensagens e de dados, descrita abaixo.

Adicionalmente, os dispositivos *Routers* também têm a capacidade de criação de mensagens de dimensão superior, ao criar pacotes de 48 B a partir de mensagens de 11 B provenientes dos sensores de corrente instalados no terreno. Como foi indicado, estes sensores geram cerca de 48 KB de dados por cada aquisição, pelo que os escassos 6B de dados presentes numa mensagem normal (cerca de 8000 mensagens, reduzindo assim para 1000) criariam uma ocupação adicional de rede desnecessária.

Como tal, para mensagens com função correspondente à aquisição de dados de corrente (EA1, EA2, EA3 e EA4) existe um processo de agregação de dados em pacotes, que segue o seguinte método:

- Para cada um dos 47 *buffers* disponíveis, indicado pelo índice n:
    - Caso *buffer* = OCUPADO:
        - Se rádio_livre = 0:
            - Se flag_Ctransporte = 0:
                - Carrega conteúdo do *buffer* para tabela de saída msg_out;
                - Corre envia_msg_CC430 – MSG_DADOS, função;
                - Coloca *buffer* = BUFFER_EM_TX;
            - Se flag_Ctransporte = 1:
                - Carrega conteúdo do *buffer* na tabela de saída msg_out, começando na posição contador_Ctransporte + 9;
                - Incrementa contador_Ctransporte;
                - Coloca tamanho da mensagem = contador_Ctransporte x 9;
                - Coloca *buffer* = BUFFER_EM_TX;
                - Se contador_Ctransporte = 5:
                    - Corre envia_msg_CC430 – MSG_DADOS, função;
                    - Coloca tempo_Ctransporte = 0;
                    - Coloca contador_Ctransporte = contador_Ctransporte – 5;
    - Incrementa índice n*;*
- Sai da função.

Este método é baseado no ponteiro flag_Ctransporte*, que é colocado a 1* aquando da recepção de uma mensagem com uma das referidas funções (a partir da rede *CANbus*), sendo que apenas um dispositivo enviará essa mensagem, visto que apenas um dispositivo recebe autorização por parte da unidade central para a sua transmissão. Por outro lado, o ponteiro contador_Ctransporte efectua o controlo de mensagens recebidas, sendo que ao alcançar o limite de 5, transmite a mensagem. Os indicadores de estado de *buffer* BUFFER_EM_TX, BUFFER_OCUPADO e BUFFER_LIVRE (ver interpretação de mensagens – ACKNOWLEDGE) permitem o controlo da recepção da mensagem sem que esta seja apagada da memória. Caso ocorra uma falha, e o controlador de comunicações notifique essa falha com a função ERRO_*TRANSMISSÃO* de MSG_CONFIGURACAO, o *buffer* ficará novamente em estado BUFFER_OCUPADO, para que possa ser retransmitido (ver interpretação de mensagens – ERRO *TRANSMISSÃO*).

Finalmente, poderia ocorrer que, por alguma razão, um conjunto de mensagens ficasse incompleto, não alcançando as 5 necessárias para que fosse transmitido, para além de que é necessário que a flag_Ctransporte seja colocada a 0. Para isso existe a função verifica_Ctransporte, que corre na rotina de programa de controlo (ver Fluxograma 15), e que segue o método abaixo descrito:

- Se flag_Ctransporte = 1:
    - Se tempo_Ctransporte >= LIMITE_CTRANSPORTE:
        - Se tamanho da mensagem na tabela de saída ≠ 0:
            - Corre envia_msg_CC430 – MSG_DADOS, função;
            - Coloca flag_Ctransporte = 0;
            - Coloca tempo_Ctransporte= 0;
            - Coloca contador_Ctransporte= 0;
- Sai da função.

O ponteiro tempo_Ctransporte é incrementado na resposta a interrupção de temporizador na condição de a flag_Ctransporte ser diferente de 0, sendo incrementado a cada 1 ms. O LIMITE_CTRANSPORTE é igual a 1000, correspondendo a 1 s.

4.5.1.4. Recepção de uma mensagem de grande dimensão

A recepção de uma mensagem de grande dimensão é feita no dispositivo AP através do procedimento normal SPI, diferindo no tratamento que é dado à mensagem, na função interpreta_mensagem_CC430.

A interpretação da mensagem, que consiste no seu seccionamento, é feita de acordo com o seguinte processo:

- Se dimensão for superior a 10 (dispositivo recebeu uma mensagem com tamanho superior a 10 – norma das mensagens *standard* de rede *CANbus*, terá de se tratar de um *Access Point*):
    - Coloca n = 0;
    - Enquanto tamanho da mensagem > 0:
        - Destinatário CAN = id unidade central;
        - Destinatário final = posição 9*n+1 da tabela de mensagem de entrada;
        - Emissor = posição 9*n+2 da tabela de mensagem de entrada;
        - Função = posição 9*n da tabela de mensagem de entrada;
        - Argumento = posição 9*n+3 da tabela de mensagem de entrada e posição 9*n+4 da tabela de mensagem de entrada;
        - Número de ordem = posição 9*n+5 da tabela de mensagem de entrada e posição 9*n+6 da tabela de mensagem de entrada;
        - Extra = posição 9*n+7 da tabela de mensagem de entrada e posição 9*n+8 da tabela de mensagem de entrada;
        - Carrega_lista_envio_CAN com a mensagem anterior;
        - Incrementa n;
        - Tamanho da mensagem = 45 – 9 * n;
        - Coloca ponteiro radio_livre = 0;
    - Sai da função.
- Se função = FFT_A (sendo A = X, Y ou Z), a mensagem a receber é de FFT, e tem um desempacotamento distinto:
    - Aplica algoritmo inverso de agregação de 3B em 2B para todos os elementos de dados, para "descompactar" a mensagem;
    - Número_de_ordem = posição 9 da mensagem recebida;
    - Se ponteiro n_ordem_640 ≠ 0 (ainda existem dados para "descompactar" e transmitir):
        - Número_de_ordem = 256 + posição 9 da mensagem recebida;
        - Se posição 9 da mensagem recebida = 63:
            - ponteiro n_ordem_640 = 0;
    - se ponteiro n_ordem_640 = 255 (mensagem foi recebida):
        - ponteiro n_ordem_640 = 1;
    - coloca dados recebidos na sua posição da trama a transmitir:
        - coloca destinatário CAN = id unidade central;
        - coloca destinatário = id posição 1 da mensagem recebida;
        - coloca destinatário = id posição 1 da mensagem recebida;
        - coloca Função = função;

        - coloca argumento = primeiro número inteiro resultante da aplicação do algoritmo inverso;
        - coloca número de ordem = Número_de_ordem;
        - coloca extra = segundo número inteiro resultante da aplicação do algoritmo inverso;
        - carrega_lista_envio_CAN com mensagem anterior;
        - coloca argumento = terceiro número inteiro resultante da aplicação do algoritmo inverso;
        - coloca número de ordem = Número_de_ordem;
        - coloca extra = quarto número inteiro resultante da aplicação do algoritmo inverso;
    - carrega_lista_envio_CAN com mensagem anterior carregada;
    - coloca ponteiro radio_livre = 0, para indicar que a unidade rádio está novamente disponível;
    - sai da função;

4.5.1.5. Transmissão de mensagens SPI – envia_SREQ_CC430

A função envia_SREQ_CC430 permite a transmissão de uma mensagem via SPI – que já foi carregada no *buffer* de saída, não tendo qualquer entrada –, com o formato representado na Figura 65.

Segue o seguinte método:

- Baixa pino de sinalização SS;
- Enquanto tempo_resposta_SPI < TEMPO_SPI e pino de sinalização SRDY = 1:
    - Incrementa tempo_resposta_SPI;
- Se tempo_resposta_SPI = TEMPO_SPI:
    - Sobe pino SS;
    - Sai da função com código NOK_SPI;
- Corre função envia_SPI_CC430 com o valor FF por duas vezes (sincronismo);
- Coloca variável *índice* = 0;
- Enquanto *índice* < tamanho da mensagem (valor da posição 0 do *buffer* de saída):
    - Corre envia_SPI_CC430 com valor da posição *índice*;
    - Incrementa *índice*;
- Enquanto tempo_resposta_SPI < TEMPO_SPI e pino de sinalização SRDY = 1:
    - Incrementa tempo_resposta_SPI;
- Sobe pino SS;

- Se tempo_resposta_SPI = TEMPO_SPI:
    - Baixa pino de sinalização SS;
    - Aguarda tempo ESPERA_TENTATIVAS_SPI;
    - Sobe pino de sinalização SS;
    - Sai da função com código NOK_SPI;
- Sai da função com código OK_SPI.

Tabela 43 - Códigos de saída da função envia_*SREQ_CC430*.

Código	Valor	Descrição
OK_SPI	1	Mensagem transmitida.
NOK_SPI	2	Erro na transmissão SPI.

4.5.2. Regulação da transmissão de grandes quantidades de dados na rede

A regulação da transmissão de grandes quantidades de dados na rede é executada pela unidade central, na figura de um computador com acessibilidade exterior através de GPRS, e que recebe dados da rede através de uma *gateway CANbus* – RS232. Este dispositivo, para regular a quantidade de dados que recebe e que consegue transmitir para o servidor remoto (ver esquema apresentado no capítulo 3), tem a capacidade de controlar o momento em que um sensor que tem uma quantidade de dados na ordem dos KB possa efectivamente transmitir esses dados. Este esquema é também útil para a regulação de dados transmitidos na rede sem fios, reduzindo consideravelmente a ocupação do canal.

Esta comunicação é feita para todos os dispositivos sensores de corrente (integrados apenas pela rede *CANbus*, ou pela rede sem fios, quando instalados em "ilhas" *CANbus* da rede sem fios), para os sensores de aceleração e temperatura sem fios para monitorização de disjuntores de alta tensão, e para os sensores de aceleração e temperatura de rede *CANbus* para monitorização de disjuntores de média tensão.

Interessa-nos a comunicação com dispositivos da rede sem fios, mas é necessário apresentar todo o esquema de comunicação.

Quando um dos referidos sensores detecta um evento e adquire um conjunto de dados que o descrevem, inicia a transmissão de uma mensagem FUNCTION_TABLE_READY, a cada minuto. É importante repeti-la, uma vez que poderão existir vários dispositivos a pretender transmitir dados, por ocorrência de um evento ao longo de toda uma linha da subestação eléctrica.

A unidade central toma o seguinte procedimento para determinação de prioridade:

- O dispositivo que enviou a primeira mensagem a chegar à unidade central, recebe permissão, através da transmissão para este de uma mensagem com função FUNCTION_TABLE_SEND;
- Caso chegue entretanto um pedido de um dispositivo a bateria e o dispositivo com prioridade não o seja:
    - É enviada uma mensagem para o primeiro dispositivo, para que este páre a transmissão;
    - É dada permissão ao dispositivo a bateria, através de uma mensagem com função FUNCTION_TABLE_SEND;

Não existem outras regras de prioridade, sendo que os dispositivos a bateria têm prioridade máxima e todos os restantes uma prioridade igual, mais baixa. A regulação da transmissão de dados no sensor de aceleração e temperatura de rede 433 MHz através deste esquema é visível em algumas funções da API acima descrita e no tópico de secção *End Device* – sensor inteligente de aceleração e temperatura, na próxima secção.

4.5.3. Estrutura do *Firmware* dos dispositivos desenvolvidos sobre o protocolo 433 MHz

4.5.3.1. AP e *Router – Gateways* com redes de campo

O processo de inicialização de um AP ou *Router* implementado sobre o protocolo 433 MHz é apresentado no Fluxograma 14 do Anexo I. Segue um procedimento em que é feita uma leitura de *flash* tal como atrás descrito na secção API de funções comuns, para verificar se já foi feito o teste de fábrica e, consequentemente, se já foram guardados valores de identificação em *flash*.

É sobre este pressuposto que é executado o restante código, de seguida é verificado se de facto foi carregada informação em *flash*, seguida da configuração de controladores de comunicações e a consequente aguardar da inicialização da *stack* 433 MHz, sinalizada pelo controlador de comunicações 433 MHz. Enquanto a mensagem de ligação não é recebida, a verificação de *buffers* processa-se como no programa de controlo de modo normal (como se verá no diagrama seguinte), para que:

- no caso de se tratar de um AP, se possa verificar a sua correcta ligação, ao responder a mensagens enviadas a partir da unidade central, através da rede *CANbus*;
- no caso de se tratar de um *Router*, que terá sensores de rede *CANbus* ligados, possa iniciar o armazenamento de dados que estes já tenham transmitido, e que serão reencaminhados através da rede sem fios após a confirmação de inicialização.

Após a recepção da confirmação de inicialização de stack (função INICIALIZACAO_OK), o ponteiro modo_funcionamento é alterado para 0, o controlador de aplicação, dependendo do tipo de dispositivo, transmite uma mensagem de confirmação de inicialização para a unidade central, e segue para o ciclo de funcionamento normal.

Neste ciclo, representado no Fluxograma 15 do Anexo I, é feita a verificação contínua de *buffers* de recepção e transmissão de dados, descritos na secção API de funções comuns, sendo que, caso um único *buffer* esteja ocupado, é invocada a função correspondente de verificação e transmissão de dados (que por sua vez invocará as funções prepara_msg_CC430 e envia_msg_CC430, bem como as suas correspondentes de rede *CANbus*).

4.5.3.2. *End Device* – sensor inteligente de aceleração e temperatura

O processo que leva um sensor inteligente de aceleração e temperatura da inicialização ao funcionamento normal, instalado no terreno, pode-se dividir em três fases: inicialização, configuração e instalação e modo normal. Esta maior divisão em relação às restantes aplicações deve-se à especificidade do seu funcionamento – detecta vibrações acima de um dado limiar – pelo que poderá levar a um mau funcionamento do dispositivo sensor caso esteja em movimento quando aquele já se encontra em modo de detecção de impacto.

Assim, a primeira fase foi designada de inicialização, estando apresentada no Fluxograma 16 do Anexo I. O começo é semelhante ao apresentado para as *gateways* de terreno e de *backbone*, havendo de seguida uma fase de calibração do temporizador cujo gerador de *clock* é o VLO, e a configuração e consequente colocação em modo adormecido dos dois sensores. Após esta fase, o controlador de aplicação entra em modo adormecido, aguardando uma resposta do controlador de comunicações, indicando a correcta ligação à rede. Assim ,que a mensagem é recebida, o controlador de aplicação sai do modo adormecido (veja-se que na interpretação da mensagem INICIALIZACAO_OK o ponteiro *standby* passa a 0) e é enviada uma mensagem para a unidade central com informação da correcta inicialização do dispositivo.

De seguida, passa-se para a segunda fase, representada no Fluxograma 17 do Anexo, de configuração e instalação em terreno, onde, antes de entrar no ciclo *while(1)*, o ponteiro *standby* é colocado igual a 55. Serve esta verificação para que o sensor aguarde que seja recebida a mensagem ID_LIVE por parte da unidade central que, em caso de teste de fábrica, é transmitida pelo programa de testes e, em caso de instalação no terreno, é transmitida pelo utilizador após colocação no terreno. De seguida, é transmitida a função INICIALIZACAO_OK, que faz parte de ambos os processos (teste de fábrica ou instalação no terreno), o sensor de aceleração é colocado em modo ligado (uma vez que este é que fará a detecção, sendo que o sensor de

temperatura fará uma medição apenas na condição de detecção de impacto) e o dispositivo entra em modo de funcionamento de terreno.

Na última fase, de funcionamento normal – dividida entre o Fluxograma 18 e o Fluxograma 19 do Anexo I, o controlador vai verificando várias *flags*, que provêm da alteração de condições provenientes de várias fontes:

- wake_periodico: para informação do bom funcionamento do sensor em caso de não haver evento para detectar – gerado pelo temporizador a cada n horas;
- *Trigger*: na resposta a interrupção do sensor de aceleração, aquando do modo_funcionamento AQUISICAO (funcionamento normal em terreno), este ponteiro é colocado a 1, para que seja corrida a rotina de recepção de dados de detecção de evento;
- Flag_aviso_table_ready: após o armazenamento dos dados do sensor de aceleração, esta *flag* é colocada a 1 para que seja transmitida uma mensagem com informação de dados de detecção de evento preparados (função FUNCTION_TABLE_READY), aguardando a resposta da unidade central para consequente transmissão. Visto que a *flag* é recolocada a 0 na saída da condição, caso não haja resposta dentro de 1 minuto, e na condição de esta *flag* estar a 0 e o modo_funcionamento ser AQUISICAO, a flag é recolocada a 1, para nova transmissão de aviso;
- Esta *flag* é colocada a 1 na interpretação de uma mensagem FUNCTION_TABLE_SEND por parte da unidade central, que ordena a transmissão dos dados de FFT;

Após um evento e consequente transmissão, o ponteiro modo_funcionamento é recolocado a SLEEP, para que o programa entre na primeira verificação de condição, desligue o dispositivo rádio (modo adormecido) e entre também em modo adormecido.

O temporizador do *End Device*, para além da contagem de tempo em segundos, minutos, horas e dias, contém verificações para alteração periódica de ponteiros, mais concretamente no caso de o acordar e transmissão de uma mensagem ID_LIVE a cada n horas (foi implementado n=2 horas) e para a retransmissão da mensagem FUNCTION_TABLE_READY em caso da não recepção da mensagem FUNCTION_TABLE_SEND. O seu processo está descrito no Anexo I.

5. Plataformas de *Hardware* desenvolvidas

Nos últimos capítulos têm sido mencionadas diferentes unidades, constituídas por microcontroladores de aplicação, controladores de comunicações ou sensores, que importa agora caracterizar fisicamente em maior detalhe, na mesma perspectiva modular com que foram criadas.

Pretendeu-se desenvolver uma plataforma física que suportasse as funcionalidades de *software* atrás descritas, e que fosse modular e compacta, para facilmente ser introduzida em qualquer um dos dispositivos desenvolvidos.

Todos os controladores programados – excluindo-se assim o controlador de comunicações *CANbus* e o controlador de comunicações *ZigBee* – são da família MSP430 da *Texas Instruments*, constituindo uma base de trabalho por:

- disporem de várias interface série (3 no MSP430F2417 e 2 no CC430F5137);
- um espaço de memória mais que suficiente para a quantidade de código desenvolvido (32 KB de *flash* e 4 KB de SRAM no CC430F5137 e 92 KB de *flash* e 8KB de RAM no MSP430F2417);
- muito boa performance de consumo, aceitando tensões de alimentação até 1,8V e com consumos de modo adormecido na casa dos μA;
- número considerável de GPIO (pinos de interface entrada ou saída – *general purpose input output*).

Para além destas características técnicas entram outras – de índole prática –, tanto ou mais importantes, que consistem no facto de existir já uma base de trabalho desenvolvida sobre os microcontroladores desta família, e que se torna importante na compatibilização de sistemas e também no tempo do seu desenvolvimento.

É de referir que toda a programação de microcontroladores foi feita sobre a ferramenta de desenvolvimento da IAR, *IAR Embedded Workbench*, tendo os microcontroladores sido programados através de interface JTAG, instalada em cada placa de circuito impresso.

A plataforma física para redes de sensores sem fios contém, em ambos os casos, um controlador de comunicações e respectivo circuito de apoio, que inclui cristais geradores de sinal para *clock*,

circuito *balun* e amplificador para sinal rádio, bem como um circuito de regulação de tensão, que faz a interface com a fonte de alimentação.

Esta plataforma é ligada aos diferentes sistemas hospedeiros, que consistem nas previamente referidas g*ateways* e sensores sem fios.

5.1. Para a rede *ZigBee*

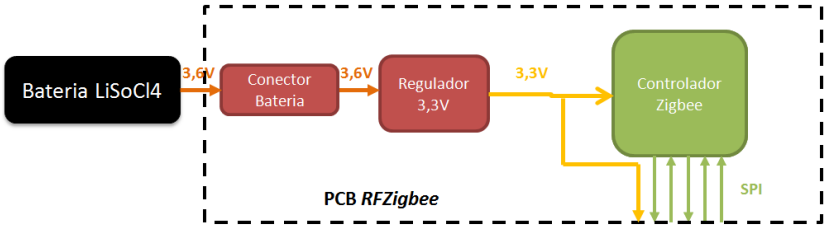


Figura 91 - Representação esquemática dos diferentes componentes de uma *gateway CANbus - ZigBee*.

5.1.1. Principais componentes

Os principais componentes destes dispositivos são os dois controladores que constituem todos os diferentes dispositivos:

- controlador de aplicação: o anteriormente mencionado microcontrolador da *Texas Instruments* MSP430F2417 (81), que desempenha funções de controlo associadas à sua aplicação: *Router*, unidade central de controlo ou sensor;
- controlador de comunicações: o módulo de comunicações *ZigBee* RC2400HP-ZNM, um dispositivo baseado no controlador da *Texas Instruments* CC2530 (70), e que desempenha funções de interface com a rede.

Interessando-nos especialmente o módulo de comunicações *ZigBee*, sendo que este consiste no módulo RC2400HP-ZNM, da *Radiocrafts*, que inclui o controlador de comunicações CC2530, da *Texas Instruments*. Sendo este último um *chip* individual, sem conter já a electrónica necessária a comunicações sem fios, é especialmente interessante poder incluir directamente um módulo que, baseando-se naquele, dispõe de um circuito *balun* e de filtragem de sinal rádio que, associados ao amplificador interno do controlador CC2530, possibilitam uma potência de saída mínima de 10 dBm. Esta foi a potência configurada para todos os dispositivos, permitindo alcances na ordem dos 100m, entre sensor e *gateway*.

Este dispositivo, sobre as funcionalidades de camada física do protocolo *ZigBee*, permite ainda uma sensibilidade de -99 dBm para a taxa de transmissão de 250 kbps, um consumo de 1,3 µA em modo adormecido e consumos de 27 mA em modo de recepção e cerca de 50 mA em modo de transmissão a 10 dBm.

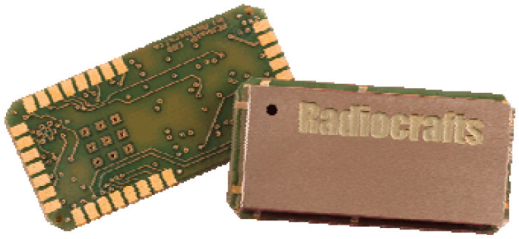


Figura 92 - Módulo RC2400HP-ZNM da *Radiocrafts*.

Apesar do consumo algo elevado (comparado, por exemplo, com os módulos apresentados na Tabela 3 do Capítulo 2), a escolha de instalar dispositivos cuja potência mínima é de 10 dBm em dispositivos alimentados a bateria permite não só que o seu alcance seja mais elevado (ver capítulo Testes Laboratoriais) – apesar do acréscimo de consumo –, mas também que seja usado apenas um componente para todos os dispositivos, baixando os custos associados devido a compra em maior escala. Esta última questão põe-se pois, nomeadamente para o módulo da *Radiocrafts* em questão, existem peças desenhadas para aplicações de muito baixa potência, como sensores, e peças para dispositivos como pontos de acesso (AP) ou *Routers*. A solução encontrada – suportada pela bateria que se seleccionou – possibilitou que o mesmo módulo fosse usado tanto para sensores como para *Routers* e AP, o que permitiu a criação de uma única plataforma.

Por outro lado, a bateria seleccionada, como se verá, tem capacidade para funcionar com uma corrente de débito até 60 mA, pelo que esta escolha é válida no que toca a alimentação.

Relativamente aos sensores, foram "herdados" nesta aplicação por via do dispositivo congénere com comunicação via *CANbus*, tendo-se o sensor de aceleração revelado (como se verá no capítulo seguinte) pouco dotado para aplicações de baixa potência, por não permitir um modo de muito baixa potência. O sensor de temperatura, quando colocado em modo adormecido, tem uma corrente de débito na casa de 1 µA, tendo-se mostrado extremamente bem adaptado a esta aplicação. Não se discutirão outras questões relacionadas com a performance dos sensores, uma vez que a aplicação que os alberga foi desenvolvida no âmbito de outro projecto, e não tem uma influência directa sobre as plataformas de comunicações desenvolvidas.

5.1.2.Circuito de Alimentação

A plataforma representada de seguida consiste em duas placas de circuito impresso, uma vez que a placa *RFZigBee* é modular, sendo compatível tanto com sensores como com *Gateways*. Veja-se que a alimentação nos 3,3V está ligada tanto ao circuito de alimentação proveniente do mesmo cabo que transmite os sinais da rede de comunicações *CANbus* como ao circuito de alimentação da placa *RFZigBee*. Esta placa tem um circuito de alimentação próprio, desenhado

para aplicações totalmente sem fios, e incorpora o seu próprio circuito, para ligação a uma bateria (que não está presente nesta aplicação).

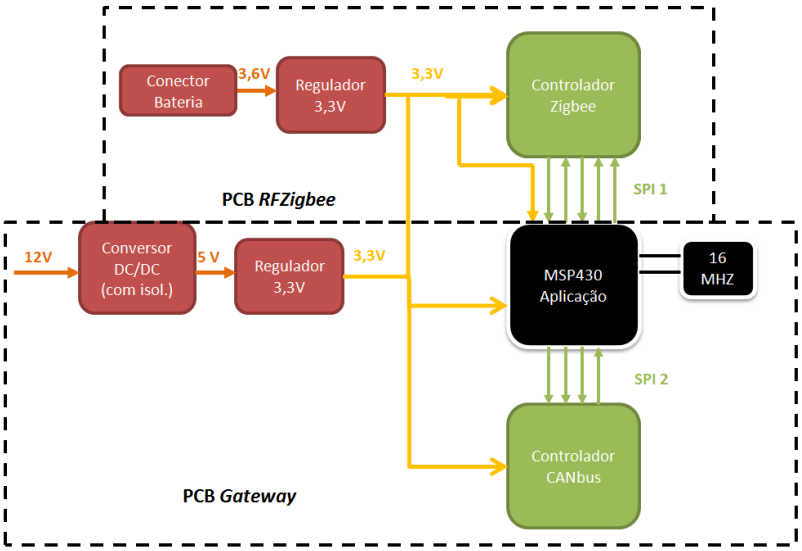


Figura 93 -Representação esquemática dos diferentes componentes de uma *gateway* de rede *ZigBee*.

A tensão transportada na rede de comunicações é de 12 V, sendo necessário, numa *gateway* deste tipo, de apenas um conversor DC/DC para 5V, tendo este conversor isolamento óptico, e de seguida um conversor para 3,3V, uma tensão adequada a todos os componentes constituintes do dispositivo. A existência de uma tensão intermédia de 5V prende-se com a utilização da mesma placa de circuito impresso para instalação de outros componentes, constituindo outros dispositivos, pelo que não é importante neste contexto.

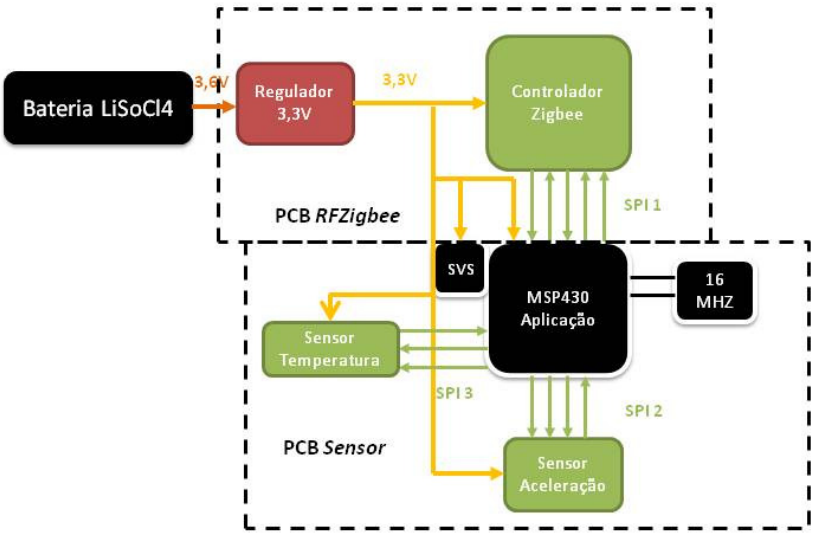


Figura 94 - Representação esquemática dos diferentes componentes de um sensor inteligente de rede *ZigBee*, bem como do circuito de alimentação.

O regulador 3,3 V seleccionado pertence à gama de reguladores LDO (*Low voltage dropout*) da Texas Instruments, tendo uma corrente quiescente extremamente baixa, na ordem dos 0,5 µA, possibilitando uma corrente de débito até 150 mA a uma tensão fixa de 3,3 V, para entradas entre 2,8V e 6V. Adicionalmente, tem um empacotamento extremamente diminuto, o que permite a sua fácil colocação numa PCB já de reduzidas dimensões.

Relativamente à bateria escolhida, pertence à gama de baterias normalizadas da Tadiran Batteries, fabricante de pilhas para aplicações de longa duração ou de alta corrente, tendo sido selecionado o modelo TL-5935, da série iXTRA, que tem uma capacidade de 1,7 A.h, uma corrente máxima debitável de 50 mA, para uma tensão de 3,6 V(82). Por outro lado, o seu formato e reduzidas dimensões – 1/6D (cerca de 33 mm de diâmetro por 15 mm de altura (82)), uma bateria tipo *wafer*, ver Figura 95 – tornaram-na numa escolha óptima para a aplicação em questão, uma vez que não implica alterações a um invólucro que se pretende cilíndrico.

Figura 95 - Bateria Tadiran TL-5135. Fonte: Tadiran Batteries.

Uma solução ideal seria a ligação a um *socket* para este tipo de bateria à placa *RFZigBee*, que possibilitasse a sua instalação sem necessidade de soldadura, o que levaria a uma troca simples, uma vez que o referido *socket* estaria instalado numa placa de circuito impresso, sendo apenas necessário colocar e retirar a bateria.

No entanto, o único modelo encontrado revelou-se fraco em termos mecânicos e com um preço elevado, para além de aumentar consideravelmente o tamanho do encapsulamento do produto no qual seria instalado.

Como tal, desenhou-se uma outra placa de circuito impresso, que contém apenas a bateria, uma ficha para ligação de um conector, que liga a dois fios para alimentação da placa de comunicações, e um *jumper*, para uma ligação simples do dispositivo. Esta placa é apresentada na Figura 96, estando o seu esquemático apresentado na Figura 149 do Anexo II.

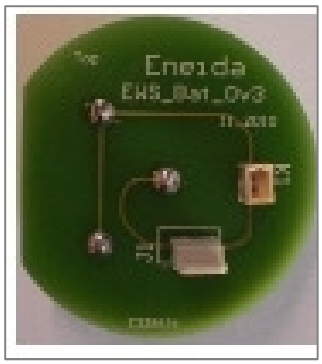


Figura 96 - Placa Bat, para instalação de bateria. As três soldaduras visíveis são dos pinos da bateria TL-5935. É ainda visível o *jumper* (branco, com referência J1) e o *header* para ligação de conector de alimentação (K1).

Esta bateria tem 35 mm de diâmetro, e foi a principal condicionante do diâmetro da caixa para estes sensores, tal como se verá numa das seguintes secções.

5.1.3.Circuito de Interface SPI

O circuito de interface SPI que interliga controlador de comunicações *ZigBee* – configurado como escravo na comunicação SPI – e controlador de aplicação – configurado como mestre na comunicação SPI – contém os seguintes pinos, ordenados pelas suas funções:

- sinalização:
    - SRDY (*Slave Ready*): pino de sinalização controlado pelo controlador de comunicações, para o qual é uma saída, e configurado como pino de entrada com interrupção no controlador de aplicação;
    - MRDY/SS (*Master Ready / Slave Select*): pino de sinalização controlado pelo controlador de aplicação, para o qual é uma saída, e configurado como pino de entrada com interrupção no controlador de comunicações;
    - RST (*Reset*): pino para *reset* por *hardware* do controlador de comunicações, ordenado pelo pino de saída configurado para o efeito do controlador de aplicação;
- Dados:
    - MISO (*Master In Slave Out*): pino de saída de dados do controlador de comunicações, ligado à entrada de dados de interface SPI para o controlador de aplicação;
    - MOSI (*Master Out Slave In*): pino de saída de dados do controlador de aplicação (configurado como saída de dados da interface SPI), e ligado à entrada de dados do controlador de comunicações;
    - CLK (*Clock*): pino de saída de *clock* da interface SPI do dispositivo mestre – o controlador de aplicação – ligado ao pino de entrada de *clock* do dispositivo escravo – o controlador de comunicações;

- Tensão:
    - VCC: tensão de 3,3V, partilhada pelos dois microcontroladores;
    - GND: *ground* do circuito, partilhado pelos dois microcontroladores.

5.1.4.Constituintes da placa *RFZigBee*

A placa de circuito impresso *RFZigBee* foi construída de forma a cumprir com os critérios de modularidade e simplicidade definidos inicialmente, bem como de baixo consumo, estando os seus componentes apresentados na Tabela 44.

Tabela 44 - Componentes da placa *RFZigBee.*

Descrição	Fabricante	Referência	Qtd.
Controlador *ZigBee*	RADIOCRAFTS	RC2400HP-ZNM	**1**
Regulador 3,3V low power (a validar)	TEXAS INSTRUMENTS	TPS78233DDCT	**1**
HEADER, VERTICAL, 1ROW, 5WAY	HARWIN	M52-040023V0545	**3**
Fio vermelho 150 mm	MOLEX	06-66-0012	**1**
Receptacle Housing 2 Way	MOLEX	51021-0200	**1**
Ficha Antena U.FL	HIROSE	U.FL-R-SMT-1(10)	**1**
CAPACITOR 1uF	MURATA	GRM188R60J105KA01D	**1**
CAPACITOR 2.2uF	TAYO YUDEN	JMK107BJ225KA-T	**1**

Deste modo, contém o componente controlador *ZigBee*, bem como um conjunto de componentes de interface, necessários para a sua ligação estável a placas de aplicação, onde está colocado o controlador de aplicação (caso dos *headers* de 5 pinos, 3 para criar uma ligação sólida), um regulador de 5V para 3,3V, que estabelece a tensão proveniente da bateria em 3,3V, bem como os respectivos condensadores de entrada e saída, para além de um receptáculo U.FL, para ligação de um cabo de antena para o exterior do invólucro.

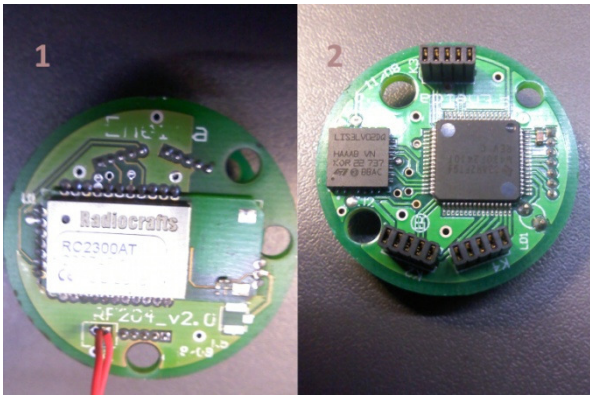


Figura 97 - Fotografia da placa *RFZigBee* (1) e placa Vib (2).

Na Figura 97 é apresentada à esquerda a placa *RFZigBee*, onde está montado o módulo Radiocrafts, e onde são visíveis as ligações das três fichas que fazem o interface físico com a placa do sensor de aceleração e temperatura. São também visíveis, no canto inferior direito da mesma imagem (1), os *pads* para soldadura da ficha UF.L de interface com a antena. Em (1) é visível o módulo de comunicações RF2300-ZNM, precursor do módulo RC2400-ZNM, mas com as mesmas dimensões. Em (2) é visível o sensor de aceleração LIS3LV02DQ, à esquerda, e o microcontrolador MSP430F2417, à direita. As fichas visíveis em (2) são para interface eléctrico (comunicações e alimentação) e suporte mecânico. Os pormenores das ligações entre a placa *RFZigBee* e a placa Vib (que contém o controlador de aplicação) são detalhados no Anexo II, Figura 148 - Esquemático da placa *RFZigBee*.

5.1.5. Encapsulamento

Quaisquer encapsulamentos – ou caixas – para as quais estas plataformas foram desenvolvidas têm como requisito um mínimo de índice de protecção IP65. Uma das caixas, destinada às *Gateways*, é apresentada na Figura 98. A sua constituição é $AlSi_{12}$, uma liga de alumínio conhecida como alumínio marítimo, e que lhe confere boa resistência a corrosão em ambientes húmidos e com altos teores de sal, como são os ambientes de petroquímicas e fábricas de pasta de papel, tipicamente próximas do mar.

Figura 98 - Caixa da unidade G2G4. É visível a antena (em cima, à direita) e o cabo *CANbus* (em baixo, à direita).

A caixa do sensor de aceleração e temperatura foi desenhada à medida, uma vez que qualquer desequilíbrio poderá influenciar as suas medições. Por essa razão, já mencionada, as caixas de acelerómetros são tipicamente cilíndricas, para que a massa seja distribuída em torno do eixo de simetria do cilindro. Também foi essa a filosofia do desenvolvimento da caixa para este sensor, tendo ainda em conta que necessitaria de albergar uma bateria, e que esta teria de ser

substituível. Daí proveio a configuração visível na Figura 99, à direita, onde se vê claramente o alargamento do tamanho da caixa em relação à sua base – um tamanho normalizado, e portanto inalterável – para possibilitar albergar uma bateria como aquela apresentada acima. Esta caixa é fabricada em Al 6082 T6 (83), uma liga de alumínio (95% a 98%) com óptima resistência à corrosão, muito usado em maquinaria.

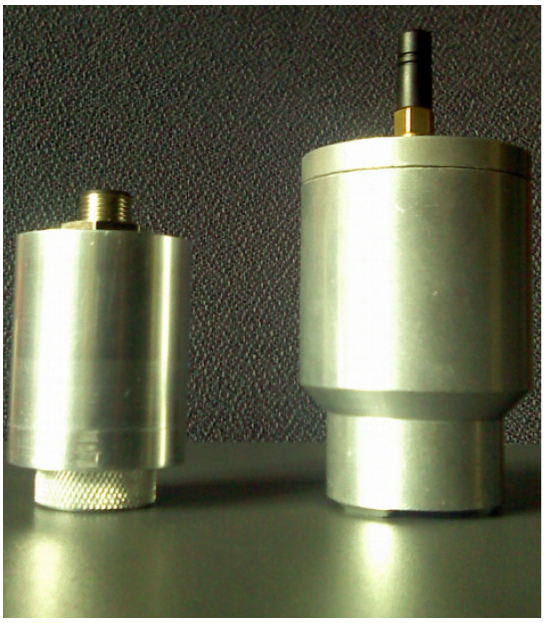


Figura 99 - Caixas dos sensores de aceleração e temperatura: à esquerda, a versão *CANbus* e à direita a versão *ZigBee*.

Na Figura 100 é apresentado o esquema dos diferentes componentes da caixa do sensor de aceleração e temperatura sem fios, sendo a peça central, a negro, aquela onde as diferentes placas de circuito impresso assentam.

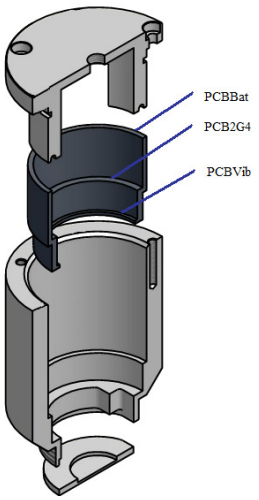


Figura 100 - Representação das várias peças constituintes da caixa do sensor de aceleração e temperatura sem fios. A peça mais abaixo constitui a tampa inferior, a peça acima desta o corpo, a peça a negro a de acomodação de placas e a peça superior a tampa.

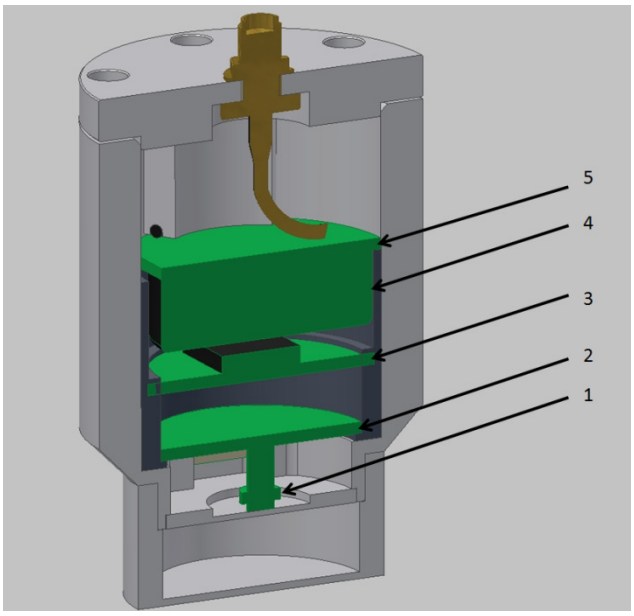


Figura 101 - Corte da caixa do sensor de aceleração e temperatura, com as várias placas colocadas no seu lugar.

Na figura acima, a placa no ponto mais baixo corresponde à do sensor de temperatura (1), sendo que é representada também a verde a ficha de ligação entre esta e a placa que contém o microcontrolador de aplicação e o sensor de vibração (2). Acima destas, encontra-se a placa do módulo de comunicações (3), a bateria (4) e a placa de circuito impresso onde esta se encontra montada (5).

A caixa apresentada na Figura 100 tem 50 mm de largura e 75 mm de altura, ficando com 110 mm de altura quando com a antena colocada. Tem duas aberturas, uma superior e outra inferior, sendo que a superior fecha com a colocação de três parafusos e a inferior com uma rosca, que não é visível na imagem.

Como se pode ver no detalhe da Figura 101, a placa de circuito impresso e a placa do microcontrolador de aplicação encontram-se ligadas por meio de uma ficha, assentando a segunda numa borda definida pela peça de acomodação, apresentada a negro. Esta peça tem uma cor diferente e a referida designação porque a sua função é precisamente acomodar as placas de circuito impresso, uma vez que o processo de fabrico destas implica que tenham sempre irregularidades. Para uma boa acomodação no interior do corpo de alumínio, desenhou-se uma peça de acomodação em plástico, com elevada flexibilidade, que permite que cada placa de circuito impresso assente no local pretendido.

Não visível na mesma figura, existem três fichas de ligação entre as placas de circuito impresso que contêm o microcontrolador de aplicação e o controlador de comunicações, e que proporcionam a transferência de dados e de alimentação entre placas. Também a placa de

circuito impresso que contém o controlador de aplicações assenta num bordo da peça de acomodação.

Acima das referidas PCB, encontra-se uma outra placa de circuito impresso que, como já foi referido, mais não tem do que a bateria para alimentação do sensor, um *jumper*, para facilmente ligar e desligar o dispositivo, e uma ficha de ligação à placa inferior. Para este conjunto alongou-se um pouco o corpo de alumínio, para acomodação da bateria. A referida PCB da bateria é ainda recortada numa das bermas, para passagem do cabo de sinal RF entre a tampa, onde este é montado, e a placa do controlador de comunicações. Este corte é ainda visível na Figura 96.

Adicionalmente, esta placa de circuito impresso necessitava ainda de uma forma de bloqueio, para que todo o conjunto ficasse solidário, sem quaisquer vibrações internas de placas. Para tal efeito, a tampa tem duas protuberâncias inferiores, que na sua base detêm sulcos para colocação de o-rings, e que pressionam a placa da bateria para baixo, mantendo todo o conjunto de placas pressionado, e consequentemente fixado. Estes pormenores, designados de "castelos", são visíveis na Figura 100 e na Figura 101.

No topo da caixa, encontram-se orifícios para introdução de parafusos, e que a fecham. Na figura apresentada, são visíveis três, sendo que a primeira versão da caixa tinha seis deles. A última versão da caixa tem apenas três orifícios, distribuídos sobre a mesma circunferência na borda da tampa.

Esta tampa superior tem ainda um orifício para montagem de uma ficha SMA com índice de protecção IP67 (que está já montada num conjunto que inclui ficha externa, cabo e ficha de ligação U.FL para ligação à placa do controlador de comunicações) na qual se insere uma antena, permitindo as comunicações com o exterior. Todo o conjunto do sensor fechado é apresentado mais adiante nesta dissertação.

5.1.6. Meios de suporte às comunicações

No tópico de secção anterior foram apresentadas as caixas que protegem os dispositivos envolvidos, tendo sido expostos os materiais dos quais são feitas. Para uma boa transmissão do sinal sem fios do módulo de comunicações no seu interior para o exterior, foi selecionado um cabo com fichas U.FL e SMA, instalável num furo na caixa de dimensão da ficha SMA. Este fio tem *o-ring* e contraporca que possibilitam um índice de protecção até IP67, e permite a ligação à estrutura da caixa, que funciona como espelho para a radiação transmitida e incidente. Nas Figura 98, na Figura 99 e na Figura 100 são visíveis os pontos de instalação do cabo U.FL – SMA, sendo que já havia sido mostrado na Figura 97 o ponto de colocação da ficha U.FL na placa de circuito impresso com o módulo de comunicações.

Figura 102 - Cabo SMA-U.FL montado numa placa de comunicações.

Adicionalmente, apresentam-se as antenas seleccionadas, ambas com ficha SMA: uma delas compacta, com um ganho de 0 dB e um comprimento de cerca de 4 cm – para sensores –, e outra de maior dimensão, com um ganho de 2 dB. Ambas têm um revestimento de borracha e são flexíveis, para uma maior resistência a impactos.

Figura 103 - Antena compacta para sensores, nos 2.4 GHz.

5.2. Para a rede 433 MHz

Para a rede 433 MHz mantém-se a estrutura apresentada para a rede *ZigBee*, de uma placa com o controlador de comunicações 433 MHz, constituindo a versão 433 MHz da plataforma de comunicações para redes de sensores sem fios, para além dos outros componentes já apresentados, e que constituem as duas aplicações distintas, de sensor e *gateway*.

O controlador de comunicações CC430F5137, pedra basilar desta plataforma de comunicações, contém na realidade um microcontrolador da família MSP430F5xx, associado no mesmo empacotamento a um transceptor rádio também da *Texas Instruments*, com a referência CC1101. As características do dispositivo rádio foram descritas na secção Camadas Física e de Enlace (Camada MRFI) do Protocolo 433 MHz (capítulo 4). O seu consumo é de cerca de 17 mA em modo de recepção e de 28,8 mA em modo de transmissão, à potência de 10 dBm, implementada, tal como foi referido para o controlador de comunicações de rede 2.4 GHz, para todos os dispositivos.

Na Figura 104 é apresentada uma representação por blocos da placa de circuito impresso que constitui a plataforma para rede 433 MHz, e que contém o controlador da família CC430, sendo ainda constituída por um circuito de alimentação, cristais para geração de sinais, e um circuito com *balun* e filtro para o acondicionamento dos sinais rádio.

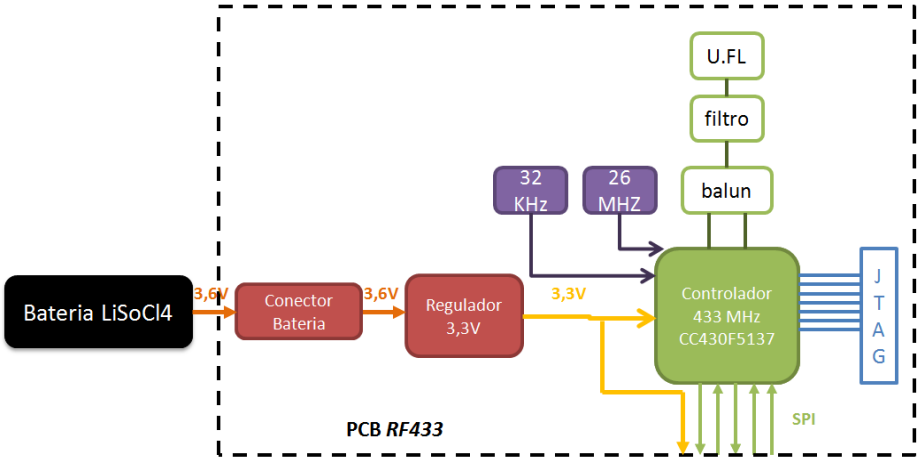


Figura 104 - Representação da placa de circuito impresso para a plataforma de comunicações 433 MHz - RF433.

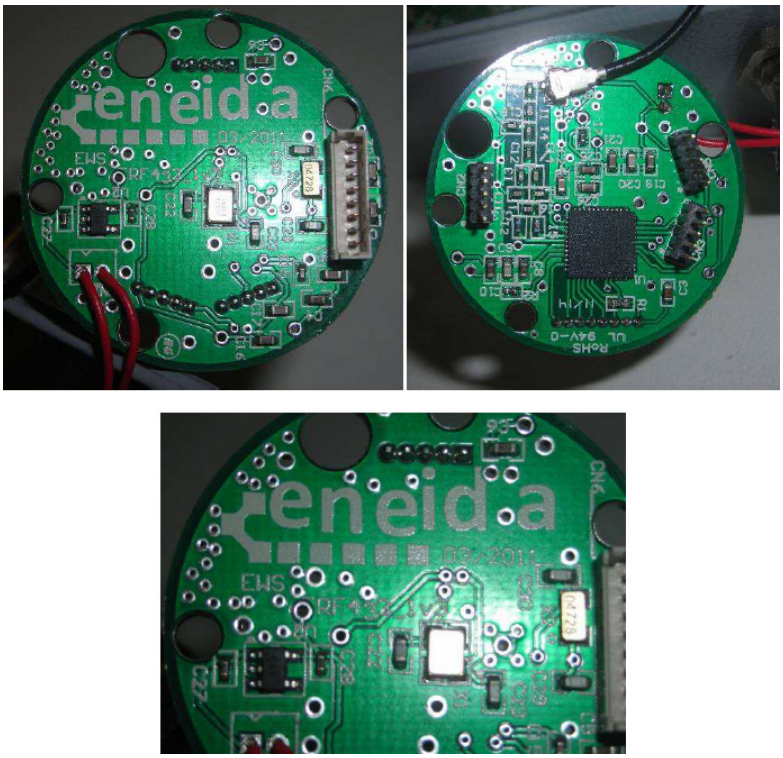


Figura 105 - Camadas superior e inferior da placa RF433.

No que toca à geração de sinais internos fundamentais para o seu correcto funcionamento (apresentados na figura acima), o controlador CC430 necessita de um cristal de 32 KHz para possibilitar consumos de muito baixa potência (ver Testes Laboratoriais), estando aquele ligado

a uma das suas entradas possíveis de cristal (neste caso, a entrada do oscilador XT1)(84). Na outra entrada, dedicada à geração de frequência para o transceptor rádio, foi ligado um cristal de 26 MHz, que serviu de base para a geração do sinal de 433 MHz (84).

A placa de circuito impresso tem o mesmo tipo de interface físico com as placas mãe de aplicação que a previamente apresentada placa *RFZigBee* (da plataforma 2.4 GHz), com três fichas de 5 pinos, e disponibilizando tensão a 3,3V para a electrónica da placa de aplicação do sensor inteligente.

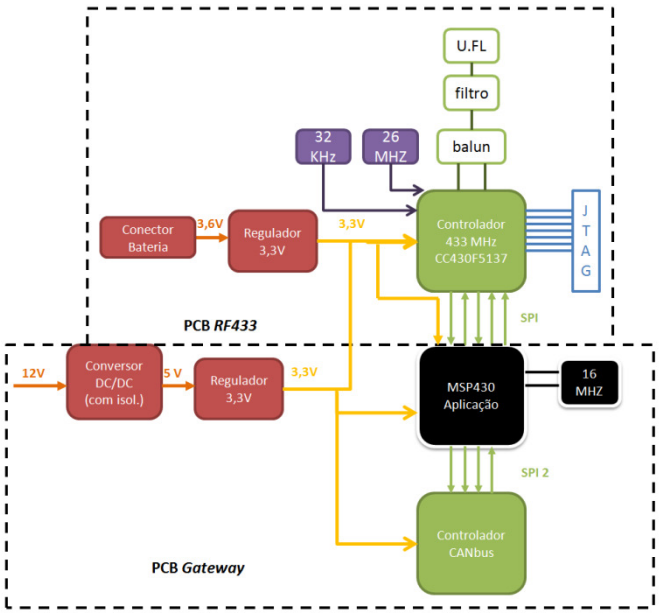


Figura 106 - Representação dos componentes da *gateway CANbus* - 433 MHz.

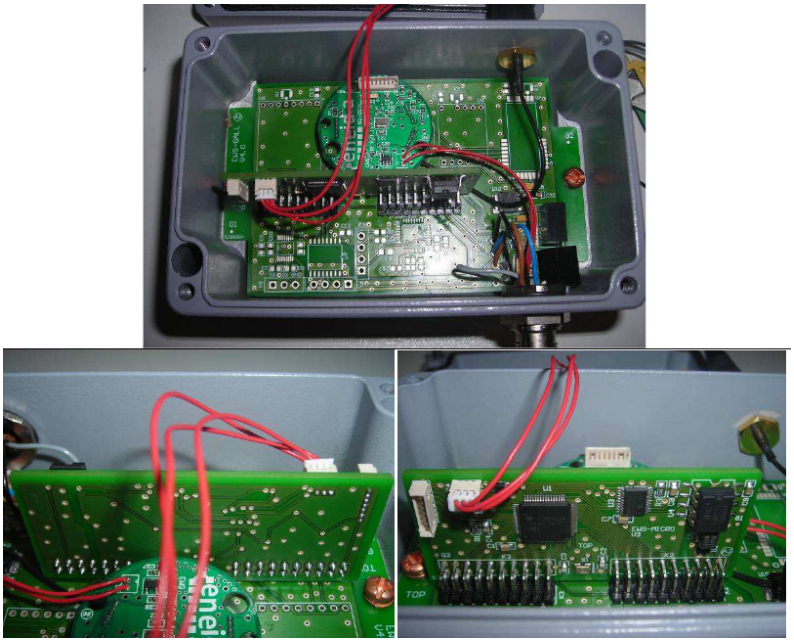


Figura 107 - Fotografia da placa RF433 instalada na *gateway* 433 MHz.

Um dos circuitos mais particulares de desenhar numa solução sem fios é o balun, uma vez que é necessário um equilíbrio completo entre os dois sinais de saída/entrada rádio.

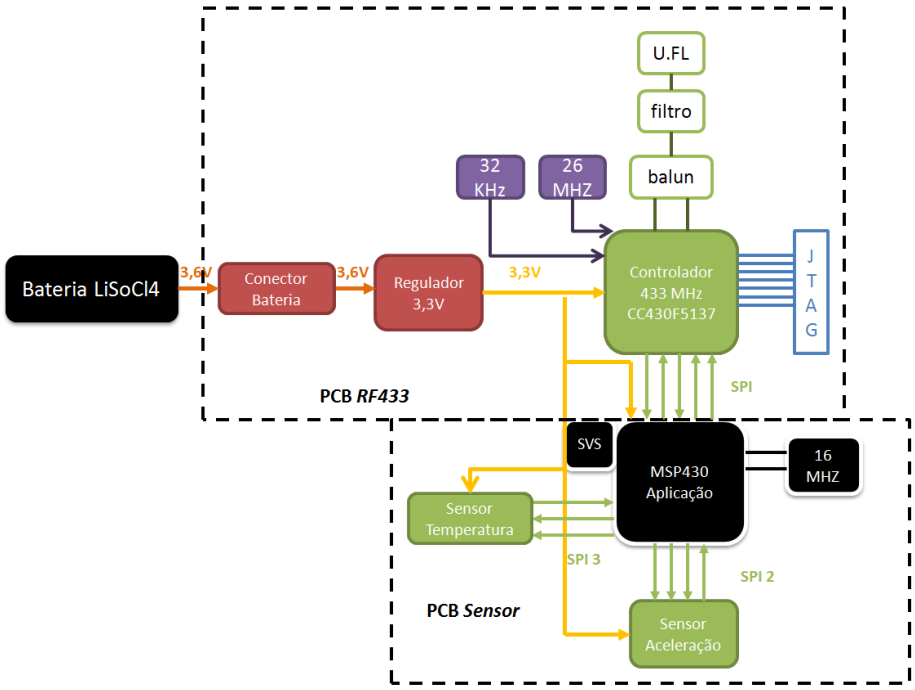


Figura 108 - Representação dos componentes de um sensor de aceleração e temperatura sem fios.

Como se pode ver na Figura 109, onde é apresentada uma imagem de CAD electrónico, existe mesmo um pequeno desfasamento de linhas à saída dos pinos do controlador CC430F5137, mas que não influenciou a performance do sistema, uma vez que a frequência de comunicação em questão é 433 MHz, com um comprimento de onda relativamente baixo, e portanto pouco susceptível a diferenças de mm. O balun necessita de ter afastado qualquer plano de terra, sendo no entanto bastante vantajoso que a placa de circuito impresso seja multi-camada, e que tenha no seu interior uma camada ligada à terra (GND) comum e outra ligada a Vcc (3,3V), para equilíbrio de cargas.

Neste caso, a camada GND ficou imediatamente por baixo da camada superior da placa de circuito impresso, visível na Figura 109.

Outra questão importante e tida em conta foi a da separação da alimentação do controlador de comunicações CC430 da do restante sistema através de ferrites, que impedem a transmissão de sinais acima de 100 MHz através do pino de alimentação dos dispositivos.

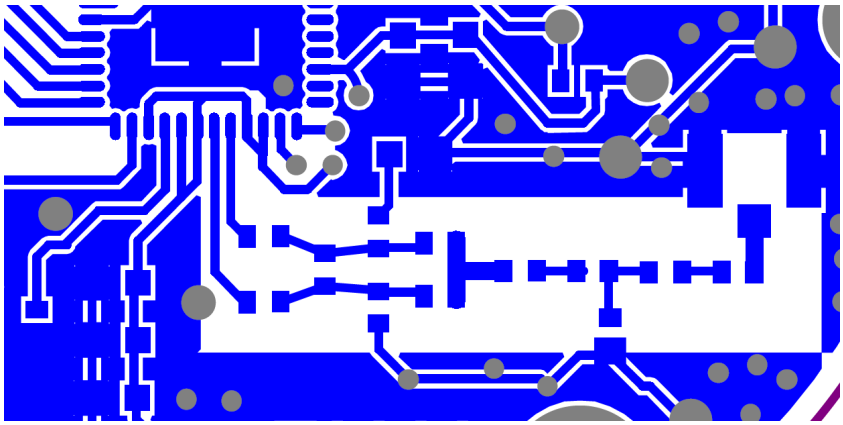


Figura 109 - Pormenor do desenho técnico da placa de circuito impresso RF433, do circuito balun e filtro. A cinzento são representadas as vias que atravessam os diversos planos.

5.2.1. Componentes da placa RF433

Dada a grande quantidade de componentes constituintes desta placa, devido ao conjunto de indutores e condensadores dos circuitos de balun e de filtro para sinal rádio, bem como condensadores associados ao funcionamento do microcontrolador, a tabela de constituintes foi colocada na secção Componentes para plataforma 433 MHz do Anexo II.

Todos os componentes foram selecionados com um critério de preço e de tamanho, uma vez que se pretende que sejam o mais pequenos possível – dada a densidade de componentes numa placa com diâmetro de 33 mm –, mas também que possibilitem soldadura manual (apesar de o processo normal de soldadura ser em máquina, através de posicionamento e cozedura).

Assim, o conjunto de componentes passivos: indutores, resistências e condensadores tem tamanhos de caixa entre 0603 e 0402, para cumprir com os requisitos de espaço na placa.

5.2.2. Circuito de alimentação

O circuito de alimentação associado à plataforma 433 MHz, tal como apresentado na Figura 106 e na Figura 108, é idêntico ao apresentado para a plataforma *ZigBee*.

5.2.3. Encapsulamento

Também o encapsulamento dos dispositivos desenvolvidos – tanto *Routers* como sensores – sobre a plataforma 433 MHz é idêntico ao descrito para a plataforma *ZigBee*.

5.2.4. Meios de suporte às comunicações

Também os meios de suporte às comunicações para a plataforma 433 MHz são equivalentes àqueles apresentados para a plataforma *ZigBee*, alterando-se a frequência das antenas.

Figura 110 - Imagem da caixa da unidade G433M2.

6. Testes Laboratoriais

Os resultados apresentados neste capítulo foram obtidos em testes elaborados em laboratório, para avaliação de características especificas dos dispositivos, como consumo em modo adormecido, alcance de comunicação rádio em linha de vista ou verificação da permanência das ligações entre dispositivos rádio, e também testes de validação feitos em entidades externas, consistindo na bateria de testes de compatibilidade electromagnética efectuados à solução desenvolvida para a monitorização de subestações.

6.1. Testes laboratoriais internos

São apresentados nesta secção alguns dos principais testes efectuados em laboratório às plataformas desenvolvidas.

6.1.1.Consumo

Uma das características mais importantes associadas à performance das plataformas desenvolvidas prende-se com o seu consumo, devido ao facto de serem desenhadas para operar recorrendo a uma fonte de alimentação finita, como uma bateria. Desse modo, efectuou-se a medição de consumos em diferentes configurações e em modo adormecido:

- Sensor inteligente *ZigBee*: Controlador de comunicações *ZigBee*, controlador de aplicação e sensores de aceleração e temperatura;
- Sensor inteligente 433MHz: Controlador de comunicações 433 MHz, controlador de aplicação e sensores de aceleração e temperatura;
- Controlador de comunicações 433 MHz.

Para os testes, foi utilizado um multímetro digital com auto-regulação de escala, podendo funcionar como amperímetro ou microamperímetro sem necessidade de intervenção do utilizador. Quando se encontra em modo de microamperímetro, a sua resolução é de 0,0001 mA (ver Figura 112). O multímetro foi montado em série com a alimentação dos dispositivos sob teste, tal como apresentado na Figura 111, tendo-se evitado usar fontes de alimentação ligadas à rede eléctrica, mais geradoras de ruído e de flutuações na medição.

O consumo dos sensores inteligentes verificou-se sempre bastante alto, tendo-se alcançado um consumo mínimo com o sistema em modo adormecido de cerca de 200 μA tanto com o sensor inteligente *ZigBee* como com o sensor inteligente 433 MHz.

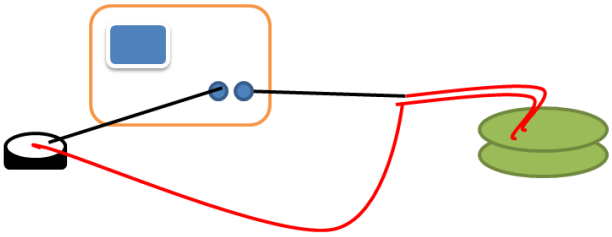


Figura 111 - Esquema de medição de consumos. É apresentada a bateria (à esquerda), ligada ao controlador de comunicações (à direita) através de um microamperímetro.

No entanto, verificou-se que este consumo elevado provinha da placa do controlador de aplicação, uma vez que as medições com as placas de controladores de comunicações revelaram valores bastante inferiores, como se vê na Figura 112. Esta figura apresenta o consumo da plataforma de comunicações 433 MHz, com o controlador de comunicações CC430F5137 em modo adormecido.

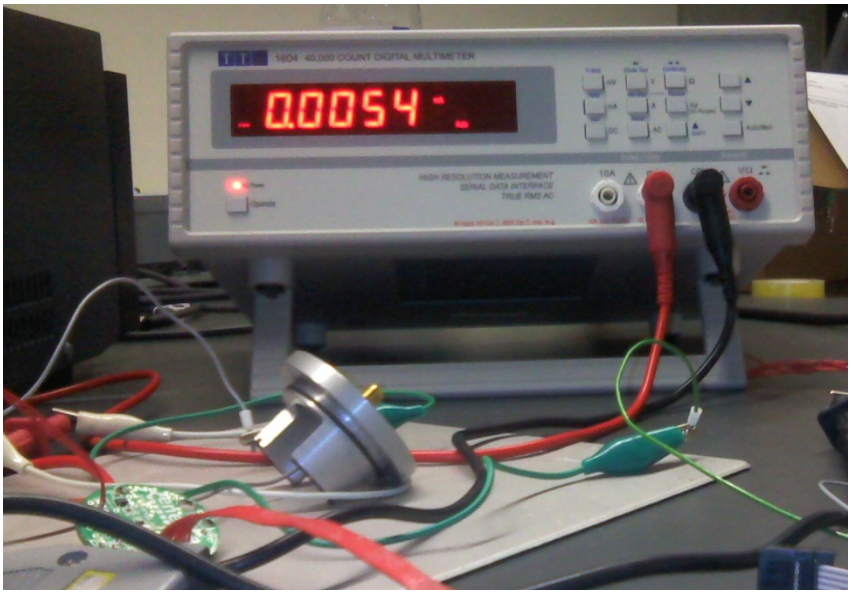


Figura 112 - Fotografia do multímetro digital com o valor do consumo da plataforma de comunicações 433 MHz. O valor encontra-se em miliamperes.

Tendo este consumo sido medido directamente da bateria, e como tal a uma tensão de 3,6V, é de realçar que o consumo real do controlador de comunicações, a 3,3 V, é de 5,9 µA. Um consumo desta ordem permite uma autonomia de anos (mais concretamente, seria de 24 anos, para uma utilização de 90% da bateria). Naturalmente, seria necessário acrescentar-se o consumo do controlador de aplicação, mas para um sensor com um consumo médio de 70 µA, já considerando na média o consumo de modo ligado, teria uma autonomia de quase 3 anos, um valor que já se torna interessante, no que toca à sua manutenção.

Adicionalmente, verificou-se que o sensor de aceleração utilizado para as aplicações de detecção de impacto se mostrou altamente incompatível com soluções de baixa potência, uma vez que, tendo apenas um modo activo e um modo adormecido, não possibilita manter, ao mesmo tempo, um baixo consumo (na casa dos µA ou dezenas de µA) e detectar eventos. O consumo deste sensor em modo ligado leva o consumo total do sensor, em modo adormecido, para os 400 µA. Este tornou-se um dos principais pontos de revisão destes dispositivos, a necessidade da substituição do sensor de aceleração por outro com suporte de programação de *duty cycle*.

6.1.2. Alcance

Os testes de alcance foram feitos em torno do edifício do IPN, em Coimbra, em dias de sol e com baixa humidade. Configuraram-se sensores (de aceleração e temperatura) para transmitirem uma mensagem por segundo, colocou-se uma *gateway* com ligação a PC no exterior do edifício e foi-se afastando progressivamente o sensor, ao longo da Rua Pedro Nunes (a estrada adjacente ao ponto vermelho da Figura 113).

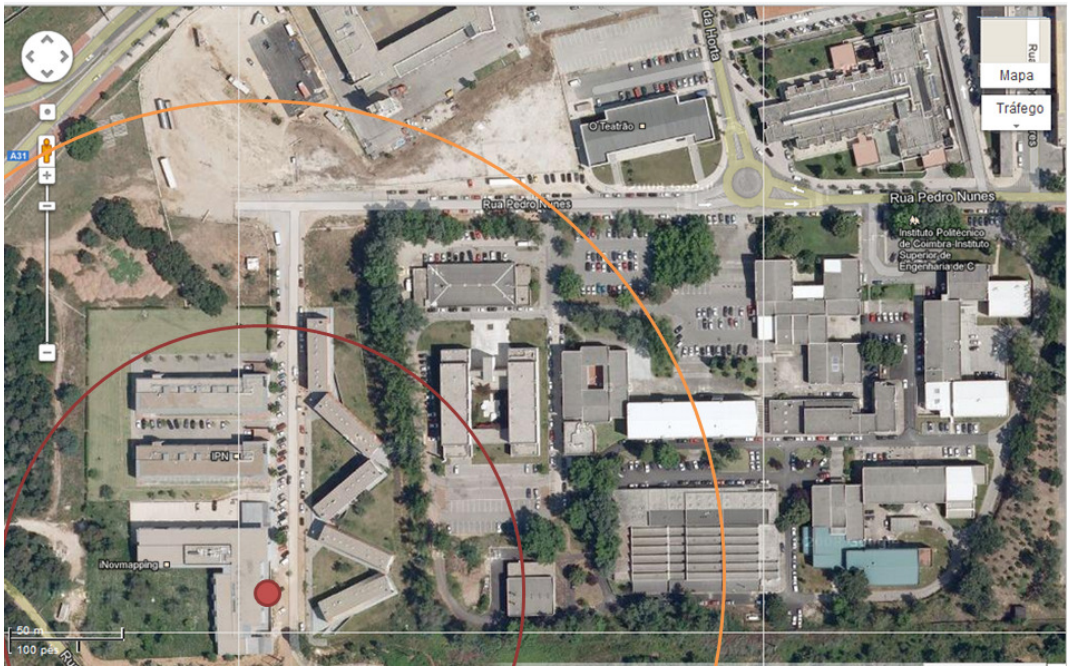


Figura 113 - Testes de alcance com um sensor *ZigBee* (círculo a vermelho) e 433 MHz (círculo a laranja). O círculo central representa a estação de base. A escala encontra-se no canto inferior esquerdo.

Na Figura 113 são apresentados igualmente os pontos nos quais as mensagens transmitidas pelo sensor deixaram de ser recebidas na estação de base. São esses os pontos nos quais a linha correspondente ao alcance do sensor (baseado num dos dois protocolos) cruza a estrada.

Daqui se verifica que se poderá contar com um alcance típico de 100 m em linha de vista para o sensor desenvolvido com base no protocolo *ZigBee* e cerca de 200 m para o sensor

desenvolvido sobre o protocolo 433 MHz. Estas medidas são visíveis através da escala presente no canto inferior esquerdo da Figura 113.São valores que batem certo com as especificações de ambos os dispositivos rádio, mesmo considerando que a estrutura do sensor, apenas com uma base de 50 mm abaixo da antena, permite um alcance considerável, que possibilita criar as soluções de instalação pretendidas.

6.1.3.Permanência das comunicações *ZigBee* ao longo de um período de tempo

Foram feitos vários testes de comunicações ao longo do desenvolvimento, onde se pretendeu testar a repetitividade das comunicações. Tendo em conta que apenas a plataforma baseada em 433 MHz foi alvo de uma instalação piloto de maior dimensão, com uma densidade já considerável de dispositivos e de tráfego de informação (ver Instalações e seus Resultados), apresenta-se aqui o teste à repetitividade nas comunicações de um sensor de temperatura com comunicações baseadas na plataforma *ZigBee* – naturalmente alimentado a bateria –, tendo este sido colocado a medir temperatura e vibração (aceleração, segundo os três eixos cartesianos) durante um período de 12 h, transmitindo dados a cada 30 s para uma *gateway* central, não existindo qualquer outro dispositivo na rede. O dispositivo sensor foi colocado no exterior (razão da descida de temperatura verificada na figura seguinte), a 12 m da *gateway*, existindo duas paredes de *pladur* e uma janela de vidro entre si, e numa zona com uma densidade considerável de redes Wi-Fi (Incubadora de empresas do Instituto Pedro Nunes, onde pelo menos cada empresa terá um *router*). Os módulos de comunicações utilizados foram baseados na primeira versão da plataforma *ZigBee*, que incluía o controlador de comunicações RC2300-ZNM da Radiocrafts (85), baseado no protocolo *ZigBee* (versão anterior ao *ZigBee PRO*), que apenas permitia uma potência máxima de 0 dBm (potência configurável entre -25 e 0 dBm). Na *gateway* foi colocada uma antena com um ganho de 2 dBi, e no sensor uma antena com um ganho de 0 dBi.

Foram assim realizadas 1550 medições e consequentes transmissões, tendo-se verificado demoras na comunicação por 3 vezes, e 34 repetições na transmissão de dados (apenas uma repetição em cada), no entanto, sem qualquer falha, a condição que se prentendia verificar, de forma a validar o código desenvolvido para a comunicação entre sensor e controlador de comunicações e controlador de aplicação. As referidas repetições consistem na existência de dois valores idênticos na base de dados do *software* SCADA, com o mesmo número de série e os mesmos dados adquiridos.

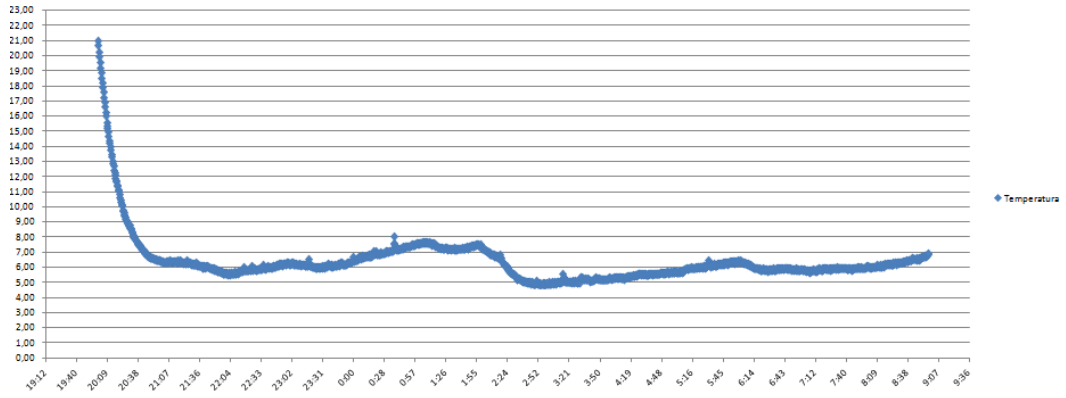


Figura 114 - Dados de temperatura adquiridos entre as 20:00 do dia 15 de Dezembro e as 8:55 do dia 16 de Dezembro de 2009.

Apesar de se ter verificado um grande número de repetições na comunicação, que se verificou em teste posterior serem provenientes da comunicação *ZigBee*, a inexistência de falhas é já um indicador importante do funcionamento adequado do sensor inteligente e sua plataforma de comunicações. No entanto, a taxa de 2% de repetições levanta algumas preocupações do ponto de vista de gastos adicionais com a unidade rádio, bem como uma necessidade de verificação da repetição de dados no *software* SCADA. Apesar de, aquando da ocorrência de repetições, se tratar de apenas uma repetição, é importante ter em conta esta possibilidade na contabilização do tempo de autonomia de cada sensor, tendo em conta que por certo existirão duplicações na transmissão de mensagens. Uma vez que o controlador de comunicações *ZigBee* se trata de um SoC configurável, e portanto passível de *debug* apenas de forma indirecta, não foi possível identificar com certeza a razão da repetição. Caso se tratasse de uma corrupção da mensagem no seu caminho, o receptor descartá-la-ia, após verificação do campo FCS. A razão mais plausível consiste na não recepção de *acknowledgement* no emissor, apesar da sua transmissão por parte do receptor. Esta situação levaria a que o emissor transmitisse novamente a mesma trama, apesar de o receptor ter validado a anterior.

6.2. Testes laboratoriais externos

No âmbito do processo de desenvolvimento de produto, efectuaram-se testes de compatibilidade electromagnética num laboratório certificado, para comprovar de que, por um lado, nenhum dos dispositivos electrónicos desenvolvidos emite radiação acima dos limites permitidos em frequências que não as de comunicação e, por outro, que esses mesmos dispositivos não são influenciados por radiação proveniente de outros dispositivos – o critério de validação neste caso é de que mesmo que o dispositivo cesse a sua comunicação com os seus pares enquanto a fonte de radiação ruidosa está activa, a restabeleça quando esta for desligada.

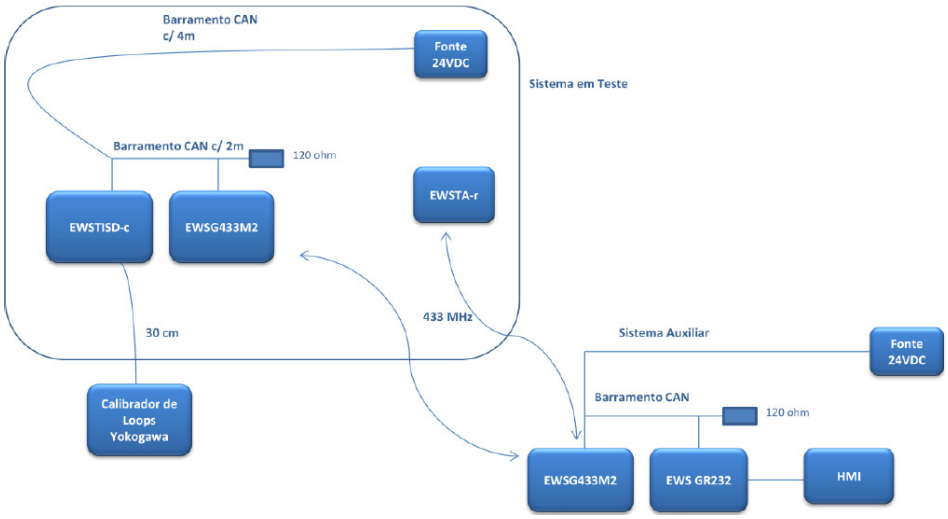


Figura 115 - Representação do sistema submetido a testes CEM.

O sistema que foi submetido a testes de compatibilidade electromagnética (CEM) é apresentado na Figura 115. Os seguintes dispositivos foram submetidos a teste:

- EWSG433M2: referência da *gateway CANbus* para rede 433Mhz, na qual está incluída a plataforma de comunicações 433 MHz;
- EWS TISD-c: referência do sensor de corrente de rede *CANbus*;
- EWS TA-r: referência do sensor de alinhamento para seccionadores, uma derivação da plataforma de comunicações 433 MHz, não apresentada nesta dissertação.

A rede em teste é assim constituída, tal como é apresentado na Figura 115, por um sensor inteligente sem fios EWS TA-r, que transmite dados para uma unidade *Gateway*, que cumpre o papel de Coordenador da rede 433 MHz, e uma ilha *CANbus*, que é constituída por um dispositivo EWS TISD-c, gerador de dados de corrente eléctrica, e por um dispositivo EWSG433M2, que cumpre funções de *Router* na rede 433 MHz, e que por sua vez transmite os dados do dispositivo EWS TISD-c para o Coordenador da rede.

Também fazendo parte da rede de comunicações 433 MHz mas não sob teste encontra-se uma *Gateway*/Coordenador central EWS G433M2, que por sua vez retransmite os dados para uma unidade *gateway CANbus* – RS232 (denominada EWS GR232), estando esta unidade ligada a um PC, onde os dados são visualizados.

A plataforma de comunicações 433 MHz incluída na *gateway CANbus* – 433 MHz (EWS G433M2) permitiu a validação do sensor de aceleração e temperatura 433 MHz, uma vez que este sensor havia sido validado em testes de compatibilidade electromagnética para a sua versão *CANbus*. Como, por outro lado, a unidade EWS G433M2 contém a plataforma de comunicações 433MHz, permite assim a validação de toda a electrónica constituinte daquele dispositivo.

Uma das questões a ter em conta no desenho de dispositivos electrónicos e aferível através dos testes de compatibilidade electromagnética, senão das mais importantes, é a de que qualquer linha eléctrica numa placa de circuito impresso ou um cabo poderá servir de antena, caso não sejam tomadas as precauções devidas no que toca ao desenho das placas de circuito impresso. Modelando este conceito, ter-se-á de considerar as possíveis fontes de radiação, o meio nas quais elas se propagarão e o seu receptor. Uma vez que é imperativa a existência de sinais de alta frequência a percorrer as linhas de uma placa de circuito impresso – sejam elas provenientes de geradores de sinal (*clock*) ou de comunicações série entre componentes – é então importante poder controlar o caminho que estes sinais percorrem, de tal forma que esse mesmo caminho não corresponda a uma antena que permite a emissão sem fios do sinal que o percorre.

Da experiência ganha, as linhas longas ligadas a geradores de sinal são especialmente boas emissoras (principalmente quando o seu comprimento é próximo de um valor múltiplo do comprimento de onda do sinal que a linha transporta) e os cabos especialmente bons receptores, que transportam radiação externa para o interior das placas de circuito impresso. Para colmatar estes problemas é importante um bom planeamento da colocação dos componentes nas PCB, evitando o desenho de linhas longas, bem com um isolamento adequado de cabos provenientes do exterior, promovendo a separação de terras entre linhas de comunicação e alimentação.

Figura 116 - Sistema subestação eléctrica para testes CEM - à esquerda estão as unidades para interface com o computador e visualização de dados e à esquerda a platine com as unidades sob teste.

Os resultados obtidos nos testes de compatibilidade electromagnética foram bastante satisfatórios, tendo todos os produtos desenvolvidos cumprido com os limites exigidos nas normas associadas à Directiva Europeia de CEM. Nas Figura 117 e na Figura 118 são apresentados esses resultados dos testes de emissão (emissão de radiação por parte dos dispositivos), sendo referentes ao sistema como um todo, estando todos os dispositivos em funcionamento.

Os picos que ultrapassam o limite imposto (a verde) situam-se nos 433,92 MHz, frequência de comunicação dos dispositivos no sistema, pelo que não são considerados na avaliação de conformidade.

O limite que não deveria ser ultrapassado é definido pela linha a verde nas figuras seguintes, indicativa do limite permitido para dispositivos a instalar em ambiente industrial.

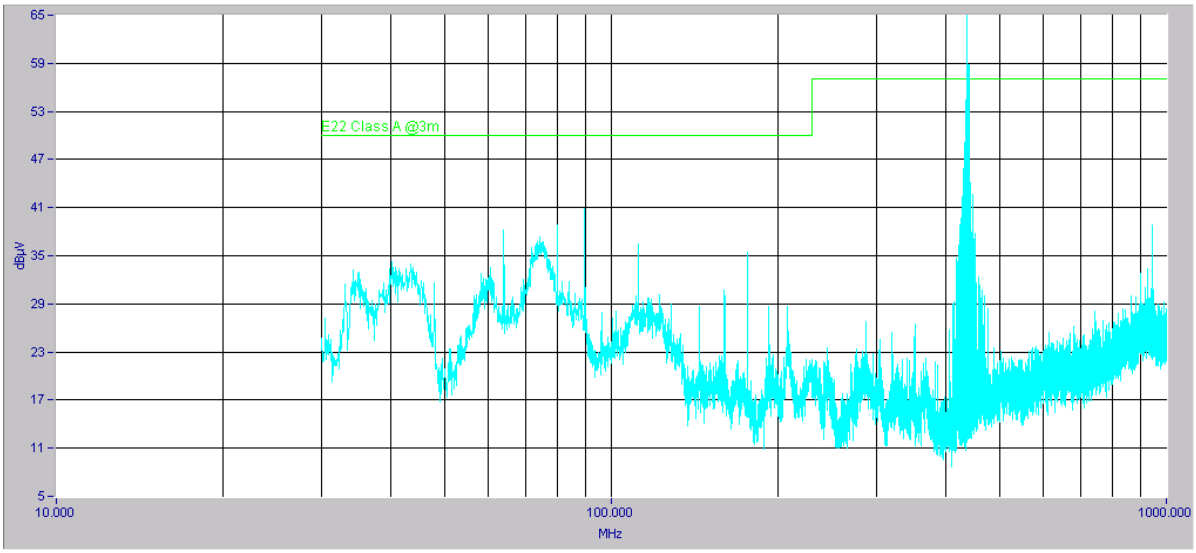


Figura 117 – Testes de CEM – resultados de emissão com polarização horizontal da antena (86).

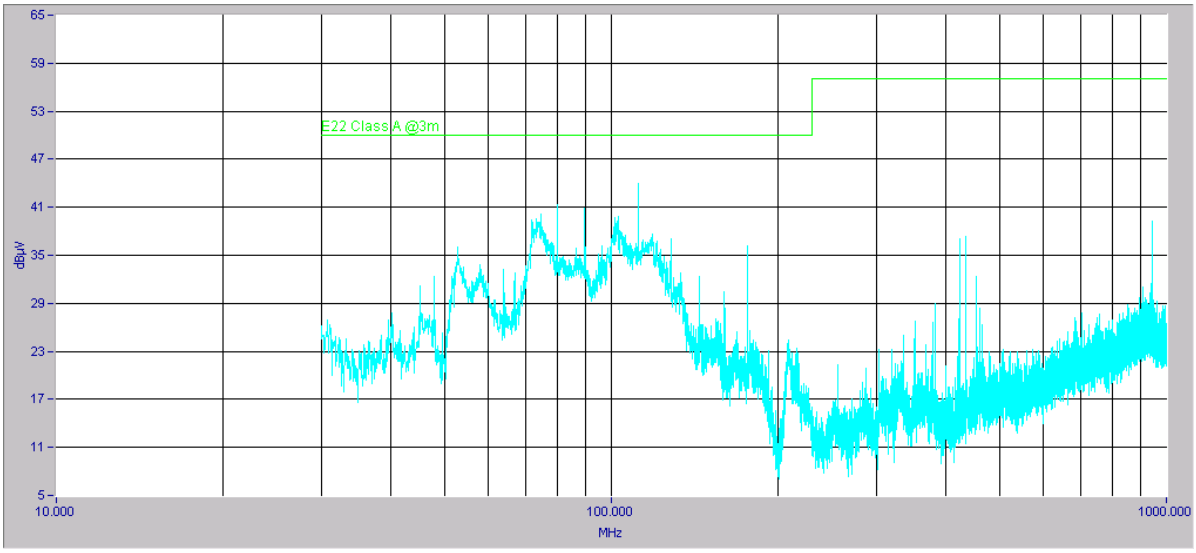


Figura 118 - Testes de CEM – resultados de emissão com polarização vertical da antena (86).

Os resultados dos testes de imunidade a radiação externa são apresentados na tabela seguinte, tendo também sido ultrapassados de forma bem sucedida.

MEIO	FENÓMENO	CRITÉRIO	NÍVEL / FREQ.	RESULT.
= IMUNIDADE =				
Invólucro	Descargas electrostáticas	B	4kV (contacto) / 8kV (ar)	OK
	Imunidade radiada [2]	A	1kHz 80% 10V/m 80MHz – 1GHz 3V/m 1,4 - 2GHz 1V/m 2 – 2,7GHz	OK
	Campo Magnético	A	30A/m	OK
CAN/DC	Transitórios Rápidos	B	1kV (5/50ns; 5KHz)	OK
	Onda choque	B	1kV (com.)	OK
	Tensões RF Conduzidas	A	10V / 1kHz 80% 150kHz – 80MHz	OK
Entradas analógicas	Transitórios Rápidos	B	1kV (5/50ns; 5KHz)	OK
	Onda choque	B	1kV (com.)	OK
	Tensões RF Conduzidas	A	10V / 1kHz 80% 150kHz – 80MHz	OK

Figura 119 - Resultados dos testes de imunidade do sistema 433 MHz (86).

Os critérios A e B referem-se a critérios de validação, sendo:

- Critério A: Durante o ensaio o aparelho deve continuar a funcionar como pretendido, não sendo permitida qualquer degradação perceptível do seu desempenho ou perda de funções para além de um limite que o utilizador possa esperar;
- Critério B: Após o ensaio o aparelho deve continuar a funcionar como pretendido, não sendo permitida qualquer degradação perceptível do seu desempenho ou perda de funções para além de um limite que o utilizador possa esperar.

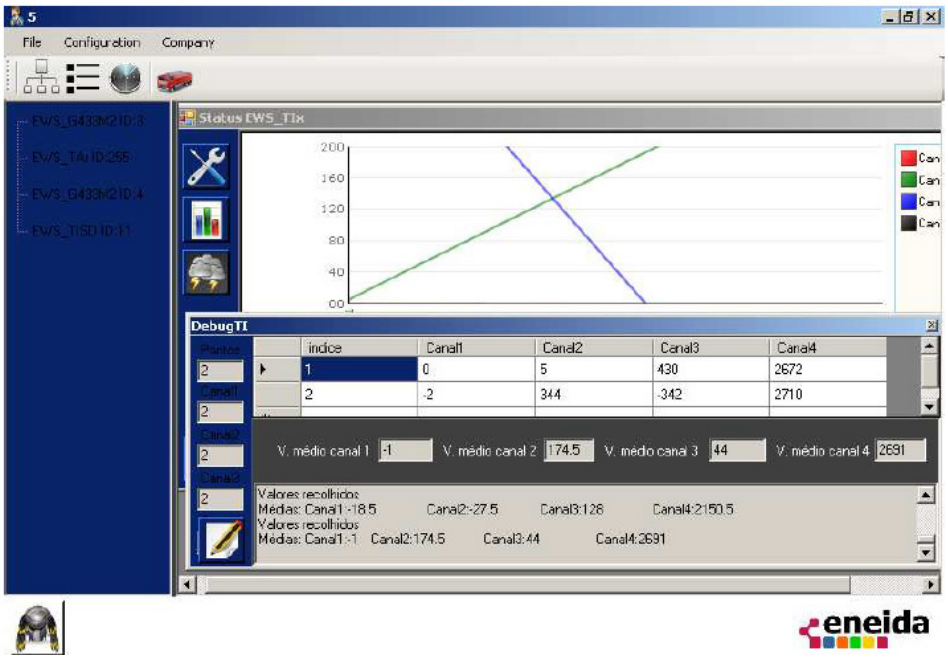


Figura 120 – EWS DS1 - HMI para o sistema desenvolvido. À esquerda, é visível o conjunto de dispositivos sob teste.

A avaliação da performance do sistema foi avaliada através da interface homem-máquina que permite visualização de dados e reconfiguração de dispositivos designada de EWS DS1.

7. Instalações e seus Resultados

7.1. Subestações Eléctricas

O sistema para monitorização de subestações eléctricas foi referido em capítulos anteriores, por isso importa agora apresentá-lo em maior detalhe, relativamente ao número e forma de instalação dos dispositivos desenvolvidos, sendo portanto o foco feito naqueles cuja comunicação se baseia, em algum ponto, sobre o protocolo de comunicações 433 MHz. Assim, os dispositivos instalados foram:

- EWSG433M2: a *gateway CANbus* 433MHz, com capacidade de *routing* na rede sem fios e integração de sensores *CANbus*;
- EWSTA3T-r4: o sensor de aceleração e temperatura, para detecção de eventos de abertura e fecho em disjuntores de alta tensão;
- EWSTA-r4: sensor de alinhamento e temperatura para seccionadores, baseado na plataforma de comunicações 433MHz;
- EWSTIST-c: sensor de corrente para transformadores alta-média tensão, integrado através de uma unidade EWSG433M2;
- EWSTISD-c: sensor de corrente para disjuntores de média tensão não incluído na rede sem fios, para detecção do evento de disparo de disjuntores de média tensão e consequente aquisição do padrão de corte;
- EWSTA3T-c: sensor de aceleração e temperatura para transformadores de alta-média tensão, integrado através de uma unidade EWSG433M2, que transmite uma aquisição por segundo;
- EWSTA3T-c: sensor de aceleração e temperatura para transformadores de alta-média tensão, não incluído na rede sem fios, para detecção do evento de disparo de disjuntores de média tensão e consequente aquisição do padrão de vibração (mesma função que EWS TA3T-r4);
- EWSGR232: *gateway CANbus* – RS232, para ligação ao modem GPRS que transmite dados para o servidor remoto;

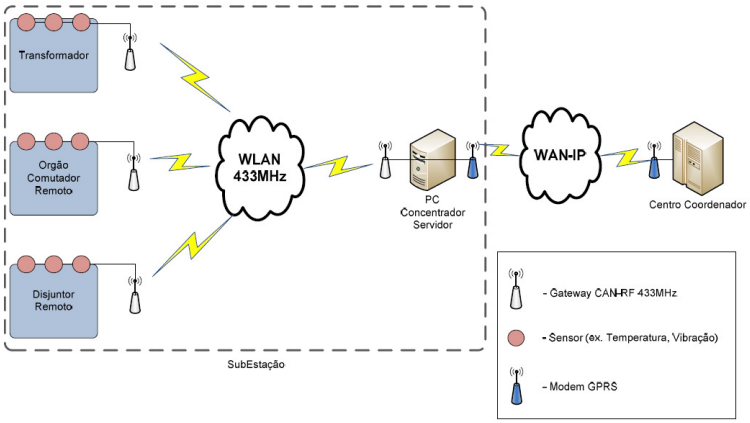


Figura 121 - Esquema representativo da rede a instalar em cada subestação, e da sua ligação a um centro de coordenação remoto (87).

Na Figura 121 é apresentado o esquema de comunicação entre os dispositivos de terreno, a unidade concentradora instalada em cada subestação e o centro coordenador, que acede a uma base de dados residente em servidor, que contém os dados de todas as subestações com instalações. No centro coordenador é possível aceder a dados de monitorização e invocar comandos para controlo das unidades de campo, através de uma interface HMI.

7.1.1. Instalação na Subestação Eléctrica do Alto de S. João, Coimbra

Esta foi a primeira instalação no terreno do sistema de monitorização de subestações eléctricas, tendo os testes até esse momento sido feitos sempre em ambiente laboratorial.

A rede sem fios instalada contém 12 sensores no parque de linhas da subestação, com 3 *gateways* EWS G433M2, uma delas funcionando como AP e unidade concentradora da rede, que por sua vez transmite os dados para a unidade concentradora da rede geral. As outras duas g*ateways* têm as funções de reencaminhamento de dados de sensores sem fios e integração na rede sem fios de dados de sensores cablados, criando assim duas das denominadas "ilhas" *CANbus*. Os sensores de rede *CANbus* que as referidas *gateways* integram na rede sem fios consistem 2 sensores TIST-c e dois sensores TA3T-c, sendo que cada *gateway* EWSG433M2 integra um conjunto de 1 sensor TIST-c e 1 sensor TA3T-c, para monitorização dos dois transformadores de alta-média tensão. O sensor TIST-c permite, através da medição de correntes, a determinação dos tempos de comutação de patamares no transformador de alta tensão. A cada evento detectado, o sensor transmite cerca de 46 KB de dados para a unidade central, que são posteriormente processados através do *software* SCADA. Por sua vez, o sensor TA3T-c monitoriza continuamente, à taxa de uma aquisição por minuto, a velocidade RMS de vibração da carcaça do transformador, segundo os eixos xx', yy' e zz', bem como a temperatura à superfície da carcaça do transformador.

Quanto aos sensores puramente sem fios, estão instalados 5 sensores EWS TA3T-r4, um em cada disjuntor de alta tensão, e 3 sensores EWS TA-r em seccionadores, tal como é representado na Figura 123. Os sensores EWS TA3T-r4 foram instalados nos disjuntores de alta tensão para detecção dos eventos de disparo dos referidos disjuntores. A cada evento de abertura ou de fecho, o sensor transmite, como foi referido em capítulo anterior, 1920B de dados de aceleração por eixo, num total de 5760B, que servirão para a avaliação do padrão de vibração da carcaça do disjuntor aquando da sua abertura ou do seu consequente fecho. Por um lado, esta medida permite o reconhecimento do evento, e por outro lado a sua caracterização.

Existe ainda um outro tipo de sensor sem fios, denominado de EWS TA-r, que por não seguir a mesma plataforma de comunicações não foi detalhadamente descrito no âmbito desta dissertação. Como foi atrás referido consiste numa adaptação da plataforma 433 MHz, de modo a incluir no controlador de comunicações as funções de aquisição de dados de alinhamento, cumprindo o mesmo microcontrolador as funções de aplicação e de comunicações. O sensor EWS TA-r executa periodicamente (uma vez a cada 5 minutos) uma medida. Os valores adquiridos são comparados com limites guardados em memória, sendo que os valores de alinhamento guardados correspondem a uma calibração que ocorre para cada sensor, em laboratório. Caso os valores limite sejam ultrapassados, em qualquer um dos sensores, é transmitida uma mensagem com esses mesmos valores para a unidade central da rede. O sensor repete a transmissão do alerta por um número pré-definido de vezes, sendo que após esse número ser ultrapassado, cessa a transmissão, apenas a retomando passada 1 hora. Esta medida deve-se ao facto de os seccionadores serem dispositivos de difícil intervenção, que apenas pode ocorrer durante paragens de manutenção previamente agendadas. Assim, é natural que o sensor passe vários dias a indicar o desalinhamento do seccionador correspondente, sendo indesejável que o faça a cada medição.

Ligados da rede de comunicações, mais concretamente no mesmo barramento *CANbus* dispositivo de interface CAN/RS232 da unidade central da rede, encontram-se 10 sensores EWS TISD-c e 5 sensores EWS TA3T-c, sendo que cada par (um dispositivo de cada tipo) monitoriza um disjuntor de média tensão, havendo 5 disjuntores sem sensores de vibração e temperatura. Apesar de estes dispositivos não serem contabilizados para as questões relacionadas com a rede sem fios, afectam esta rede de comunicações no sentido em que partilham o acesso à unidade central da rede que, tal como foi detalhado na secção Regulação da transmissão de grandes quantidades de dados na rede do Capítulo 4, regula a transmissão de dados por parte dos sensores.

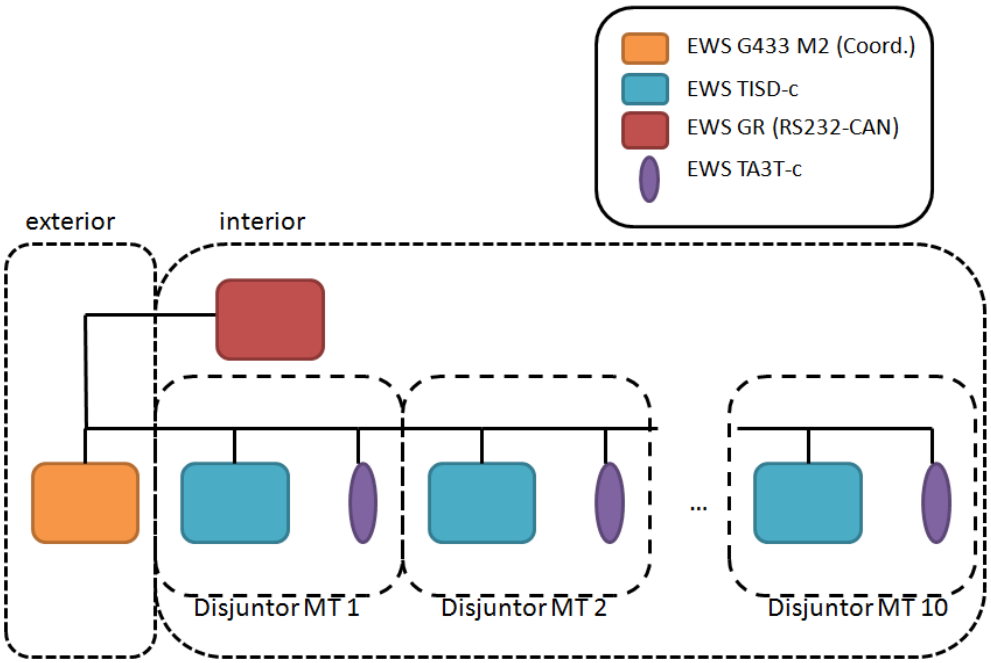


Figura 122 - Esquema representativo do barramento *CANbus* central instalado na subestação do Alto de S. João.

Na figura acima apresenta-se a rede de comunicações instalada no mesmo barramento que o dispositivo de interface à unidade central da rede, fazendo dela parte, como foi mencionado, vários sensores EWS TISD-c, EWS TA3T-c e o Coordenador da rede sem fios 433 MHz, uma unidade *gateway* EWS G433 M2.

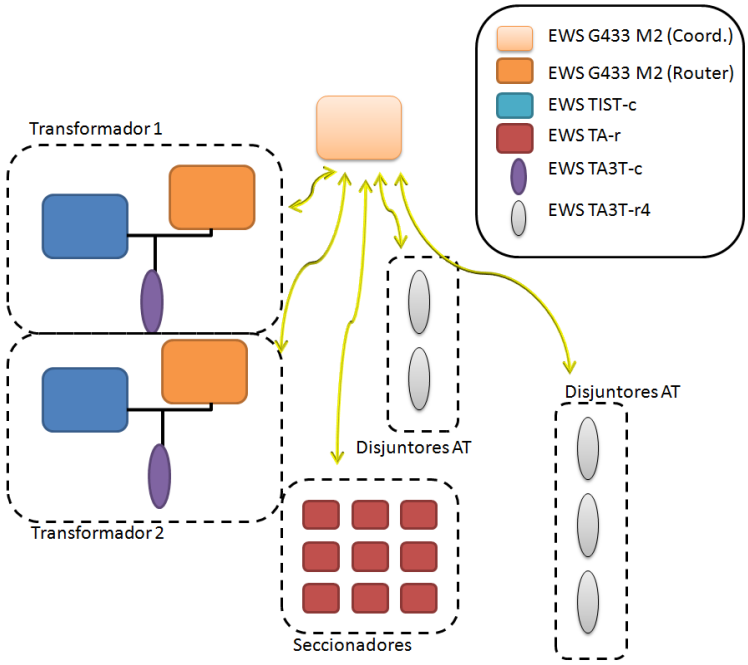


Figura 123 - Esquema representativo da rede sem fios instalada na subestação do Alto de S. João, em Coimbra.

É esta unidade que é representada como Coordenador e ponto central da rede da figura abaixo, onde é apresentada a rede sem fios na sua totalidade. Ainda relativamente à rede da figura acima, todos os dispositivos que a constituem, à excepção da unidade EWS G433 M2, encontram-se no interior de um edifício, no qual estão contidos os disjuntores de média tensão, bem como a unidade EWS GR e a unidade central da rede, que congrega os dados adquiridos por todos os dispositivos da instalação e contém a capacidade de comunicação sobre rede móvel. Naturalmente, a unidade EWS G433 M2 Coordenador foi instalada no exterior deste edifício, para que não se adicione um obstáculo à comunicação com os dispositivos da rede sem fios, instalados no parque de linhas. O edifício em questão é visível na Figura 124, sendo o coordenador a unidade a laranja mais à esquerda. O código de cores desta imagem é o mesmo da Figura 123.

Na figura seguinte é apresentada uma fotografia de satélite da subestação eléctrica do Alto de S. João com a posição efectiva de cada dispositivo, sendo usada o mesmo código de cores da Figura 123 para identificar cada unidade.

Figura 124 - Imagem de satélite com identificação dos dispositivos instalados na subestação eléctrica do Alto de S. João, em Coimbra. Fonte: Google, 2012.

Nesta instalação, foi utilizado um esquema de identificação onde o identificador geral do dispositivo (ver Tabela 45), em formato decimal, indica (apenas visualmente, para o programador) o tipo de dispositivo de que se trata. Lembre-se que cada dispositivo provém de fábrica com o identificador genérico 255 (numeração decimal), sendo acessível via *broadcast*, aceder a todos os dispositivos da rede (como foi mencionado nas secções correspondentes, tanto na rede CAN como nas diferentes redes sem fios 0xFF constitui o endereço de *broadcast*). Apenas no laboratório, antes da instalação, é atribuido a cada dispositivo o seu identificador geral. A seguinte tabela de identificadores apresentada seguidamente foi a utilizada.

Tal como se apresenta na Figura 123, de acordo com os critérios de associação à rede definidos formou-se uma rede em estrela, uma vez que não foram impostas limitações de número de filhos aos dispositivos *Router* e AP, pelo que seria a topologia de rede a esperar para uma instalação em que todos os dispositivos estão dentro de um raio não superior a 40 m do AP (ver escala da Figura 124). Esta conformação de rede será mesmo a mais adequada para este tipo de instalação, uma vez que os dispositivos *Router* necessitam de, em caso de evento, reencaminhar uma grande quantidade de dados, proveniente dos sensores de corrente TIST-c, pelo que o reencaminhamento adicional de dados de sensores sem fios lhes causaria atrasos nessa retransmissão.

Tabela 45 - Identificadores da instalação na subestação do Alto de S. João, em Coimbra.

Dispositivo	Localização	Identificador (de rede geral)
EWSG433M2	Edifício Central	2
	Transformador 1	3
	Transformador 2	4
EWSTISD-c	Transformador 1	30
	Transformador 2	31
EWSTA3T-c	Transformador 1	10
	Transformador 2	11
EWSTA-r	Seccionador AT1	50
	Seccionador AT2	51
	Seccionador AT3	52
	Seccionador AT4	53
	Seccionador AT5	54
	Seccionador AT6	55
	Seccionador AT7	55
	Seccionador AT8	57
	Seccionador AT9	58
EWSTA3T-r4	Disjuntor MT1	20
	Disjuntor MT2	21
	Disjuntor AT1	22
	Disjuntor AT2	23
	Disjuntor AT3	24

Foram registados dados dos sensores ao longo do tempo, reproduzindo-se de seguida algumas das medidas adquiridas no teste à instalação dos diferentes equipamentos e posteriormente à instalação, durante a monitorização dita normal.

Na figura seguinte é visível o gráfico formado pela informação recolhida de um sensor EWS TA3T-r4 desta subestação, aquando do fecho (consequente à abertura) do disjuntor que monitoriza.

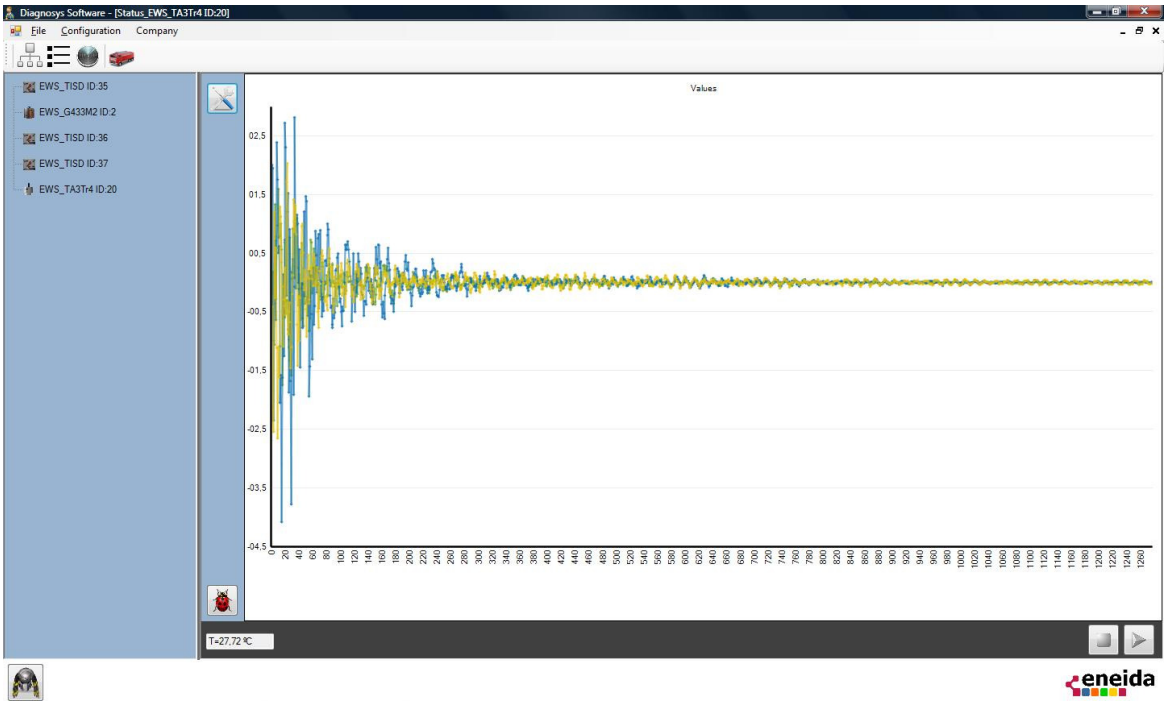


Figura 125- Padrão de vibração da abertura de um disjuntor de alta tensão (eixo dos yy' - intensidade de aceleração, eixo dos xx', amostras - até 1260).

Em primeiro lugar, é necessário referir que o *software* SCADA apenas apresenta os dados referentes a determinado evento caso todo o conjunto de medidas que correspondem àquela medição seja recebido. Para isso, é transmitida pelo sensor em causa uma primeira mensagem onde é identificado o conjunto de dados que será transmitido posteriormente. Assim, a apresentação do gráfico correspondente ao padrão de vibração é já indicativo da transmissão do conjunto de dados adquiridos pelo sensor. Por outro lado, verifica-se um padrão de vibração do tipo de um amortecimento, que está de acordo com o expectável, visto tratar-se da detecção de um impacto numa superfície metálica. Para além dos mecanismos de integridade que incluem o protocolo de comunicações, este resultado permite também fazer uma validação visual do resultado da medição que, não correspondendo naturalmente a uma calibração, é importante que aconteça.

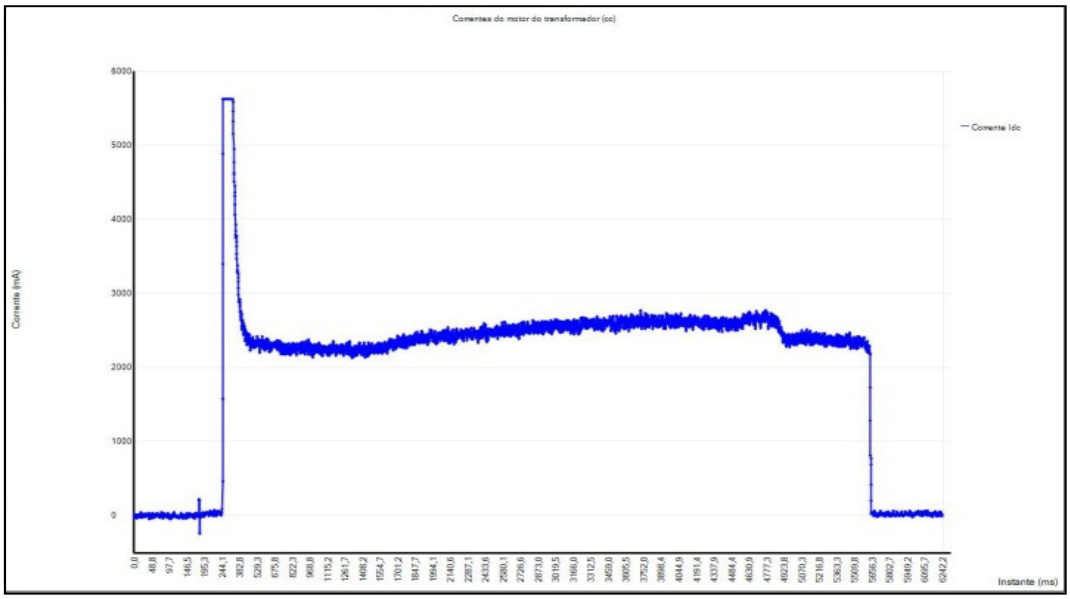


Figura 126 - Padrão de detecção de um pico de corrente (CC) no motor do transformador de alta tensão (mA), com consequente medição do seu tempo de comutação de patamar, obtido a partir do sensor EWS TIST-c.

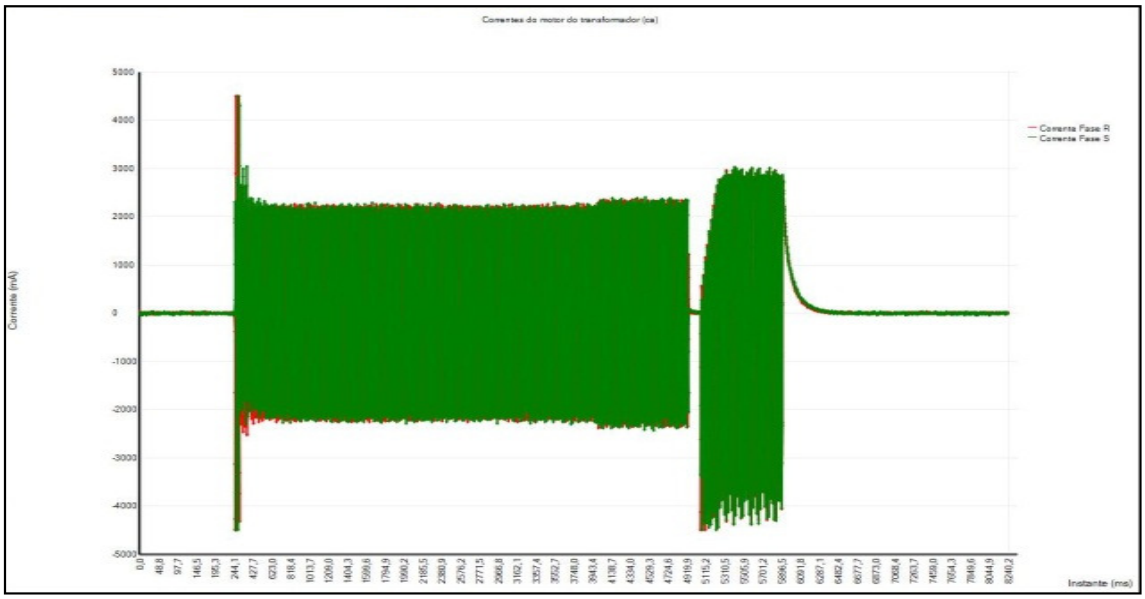


Figura 127 - Padrão de detecção de um pico de corrente (CA) no motor do transformador de alta tensão (mA), com consequente medição do seu tempo de comutação de patamar, obtido a partir do sensor EWS TIST-c.

Nas duas figuras anteriores são visíveis as aquisições de dados (gráficos obtidos através do *software* SCADA) a partir dos sensores EWS TISD-c instalados nos transformadores de alta tensão, que por sua vez tiram proveito da rede sem fios através da ligação a uma *gateway/Router* da rede 433 MHz. Ambos permitem, tal como foi referido para o sensor EWS TA3T-r4, a validação da recepção do conjunto de dados adquiridos pelo sensor. Estes valores foram adquiridos aquando da instalação, precisamente para obter a validação da devida ligação dos diferentes componentes da rede.

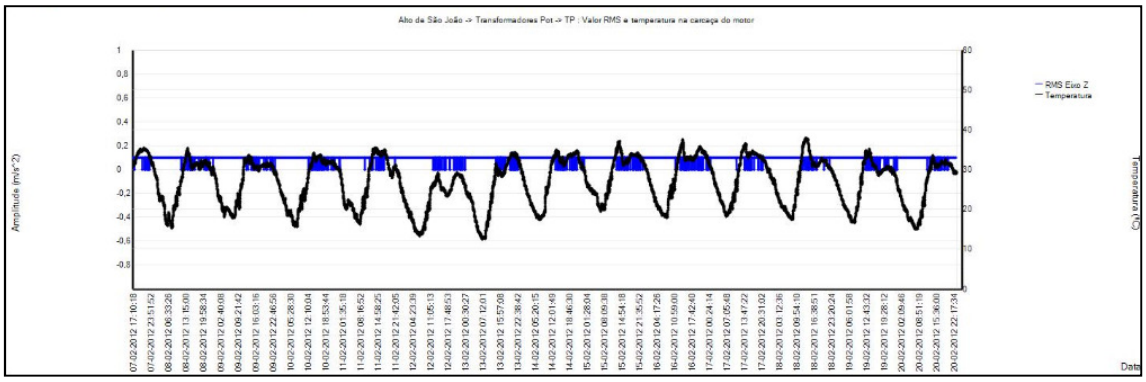


Figura 128 - Dados adquiridos através do sensor EWS TA3T-c instalado na carcaça do motor do transformador de potência.

Na figura acima verifica-se a aquisição de dados do sensor EWS TA3T-c, instalado na carcaça de um dos transformadores de potência da subestação eléctrica do Alto de S. João, para o período entre os dias 7 e 20 de Fevereiro de 2012. O sensor encontra-se a monitorizar a temperatura e a velocidade RMS na carcaça de um transformador.

Neste caso, e tratando-se de uma aquisição contínua ao longo do tempo e não de um evento detectado, como acontece para os sensores EWS TISD-c e EWS TA3T-r4, não existe a necessidade de aceitação da transmissão de dados por parte da unidade central da rede. Assim, e em termos da rede de comunicações, este gráfico valida o correcto funcionamento ao longo do tempo naquele troço da rede.

A presente instalação permitiu ainda testar o sensor inteligente para monitorização do alinhamento de seccionadores, o EWS TA-r, tendo-se verificado uma dificuldade por parte deste na recepção de dados. Tal dificuldade está relacionada com o facto de, apesar de o alcance da unidade EWS TA-r ser semelhante àquele das unidades com plataforma 433 MHz, o mesmo não se passou com a sua sensibilidade, falhando a recepção de comandos por parte da unidade central da rede. Esta fragilidade foi rastreada e foi identificada como falha o facto de não ter sido incluída para este sensor, tal como aconteceu para a plataforma 433 MHz, duas camadas internas à placa de circuito impresso, que permitem um maior equilíbrio da distribuição de carga ao longo da placa, bem como uma maior disponibilidade de corrente.

Apesar desta ocorrência, a instalação das unidades EWS TA-r permitiu a aquisição e validação de dados dos seus sensores, sendo apresentada na Figura 129 várias aquisições de seis dos nove dispositivos instalados na subestação do Alto de S. João.

No Anexo III são apresentadas algumas imagens que permitem uma melhor percepção do espaço constituído pela subestação eléctrica do Alto de S. João, especialmente dos dispositivos sem fios concebidos sobre a plataforma 433 MHz.

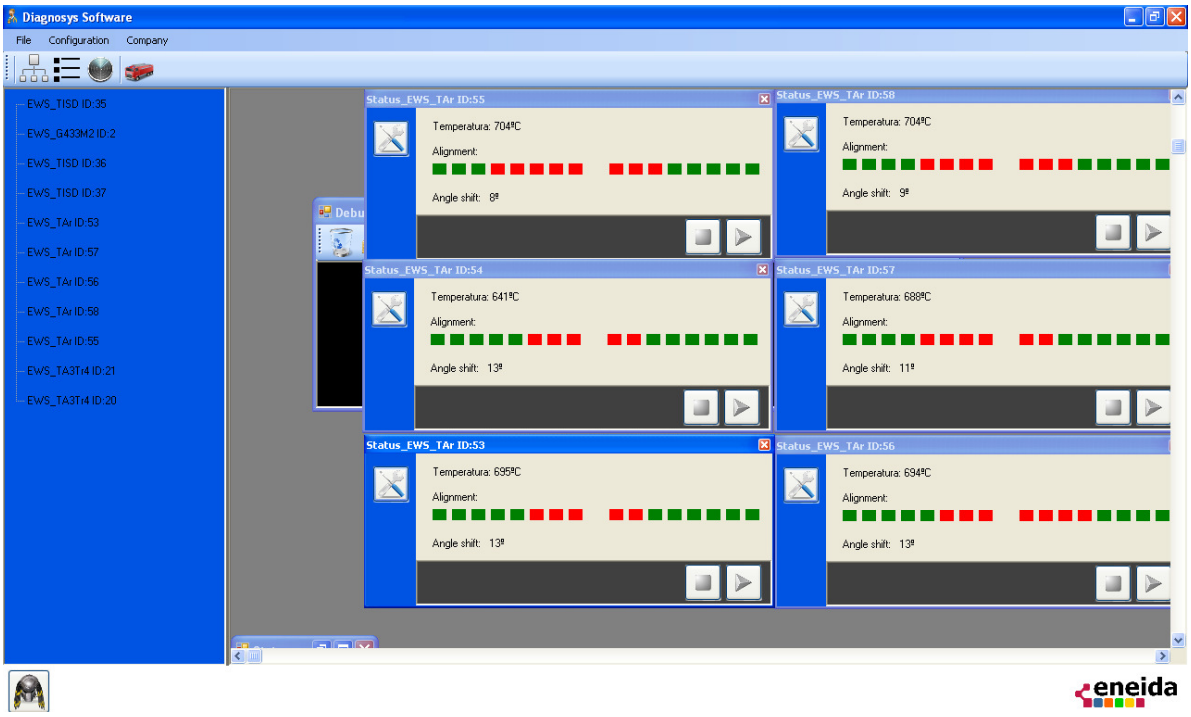


Figura 129 - Apresentação em SCADA dos valores de alinhamento dos 6 sensores EWS TA-r instalados na subestação eleéctrica do Alto de S. João. Os valores de temperatura encontram-se multiplicados por 32.

Esta primeira instalação permitiu a validação no terreno dos testes que vinham a ser executados no laboratório, especialmente do mecanismo criado para o controlo de dados a serem transmitidos na rede, criado para regular a chegada de mensagens à unidade central da rede, neste caso um computador com acesso a uma rede móvel. Apesar de tal teste ser possível em laboratório, apenas a sua validação em terreno permite a obtenção da confiança necessária no sistema desenvolvido. O mecanismo mostrou-se funcional, sem ter ocorrido qualquer "choque" – ou transmissão simultânea – de mensagens a chegar à unidade central.

Por outro lado possibilitou também verificar a programação desenvolvida para os dispositivos que compõem a rede sem fios, que obteve um bom resultado, com a detecção de eventos por parte dos sensores, correcta tentativa de acesso à transmissão para a unidade central da rede por parte dos respectivos controladores de comunicações e, especialmente, a capacidade de manter a transmissão de grandes quantidades de dados por parte dos controladores de comunicações desenvolvidos.

7.1.2. Instalação na Subestação Eléctrica de Corrente, Coimbra

A instalação de um sistema de monitorização de subestações eléctricas em Corrente decorreu imediatamente a seguir à instalação no Alto de S. João. Sendo esta uma subestação mais pequena, o conjunto de dispositivos instalados foi também inferior, tal como se verifica na representação da rede da Figura 131. Aqui, foram instaladas duas unidades EWS G433 M2, uma funcionando como AP e unidade concentradora da rede sem fios, e outra junto aos dispositivos

de monitorização do único transformador da subestação, um sensor de corrente EWS TIST-c e um sensor de aceleração e temperatura EWS TA3T-c.

Figura 130 - Imagem de satélite com identificação dos dispositivos instalados (ver Figura com estrutura da rede instalada em Corrente, em Coimbra). Escala apresentada. Fonte: Google, Inc.

Foram também instalados 4 sensores de aceleração e temperatura sem fios, três deles em disjuntores de alta tensão, no interior do parque de linhas, e outro num disjuntor de média tensão, no interior de um armário que se encontra no exterior, ao invés dos restantes disjuntores de média tensão, que se encontram no interior do edifício (tal situação não se colocou na subestação do Alto de S. João).

Essa foi uma das vitórias em termos de alcance e resistência a reflexões de materiais metálicos, uma vez que, tal como é visível na Figura 132, o armário é completamente fechado e fabricado em alumínio, sendo a única abertura possível para a comunicação através de uma pequena janela existente em uma das portas.

Na Figura 133, é visível a porta da janela aberta, e o sensor instalado, e na Figura 134 apresenta-se a distância que separa sensor e *gateway* concentradora.

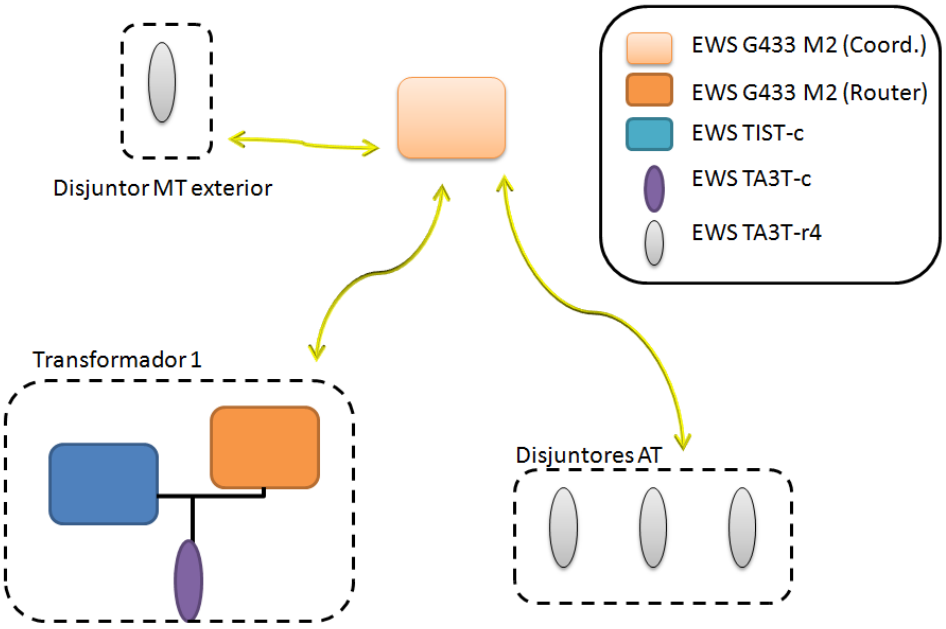


Figura 131 - Esquema representativo da rede instalada na subestação do Alto de S. João, em Coimbra.

Figura 132 - Armário com disjuntor de média tensão.

Figura 133 - Instalação do sensor de aceleração e temperatura sem fios no interior do armário.

Figura 134 - Distância que separa o armário do disjuntor de MT e a unidade concentradora da rede sem fios (a vermelho).

Não foram instalados sensores de alinhamento em seccionadores, pelas razões mencionadas na secção anterior. Em mais uma imagem da instalação, a Figura 135, é visível a forma de colocação do sensor de aceleração e temperatura sem fios EWS TA3T-r4, sobre as barras colocadas acima dos disjuntores, e fixado através de cola colocada na sua base metálica.

Figura 135 - Sensor EWS TA3T-r4 instalado no terreno.

Relativamente a tabelas de identificadores, foi seguido o mesmo formato que para a rede da subestação do Alto de S. João, tal como apresentado na tabela abaixo.

Tabela 46 - Identificadores de rede geral dos dispositivos sem fios ou integrados na rede sem fios na subestação de Corrente.

Dispositivo	Localização	Identificador (de rede geral)
EWSG433M2	Edifício Central	2
	Transformador 1	3
EWSTISD-c	Transformador 1	30
EWSTA3T-c	Transformador 1	10
EWSTA-r	Seccionador AT1	50
	Seccionador AT2	51
	Seccionador AT3	52
EWSTA3T-r4	Disjuntor MT1	20
	Disjuntor AT2	21
	Disjuntor AT2	22
	Disjuntor AT3	23

Tal como seria de esperar, tendo em conta os resultados da subestação do Alto de S. João, também nesta instalação se formou uma rede em estrela, com todos os dispositivos ligados ao AP.

Desse modo, os únicos testes ao processo de reencaminhamento de dados foram efectuados em laboratório, através de condições de aceitação de dispositivos filhos que impunham a ligação ao *Router* devido à não-aceitação de novas associações por parte do AP. A validação desta funcionalidade ficou assim por testar no terreno.

No âmbito do projecto associado a esta dissertação, foram seguidos os resultados das instalações, mais concretamente a recepção – ou não – de dados no servidor central, até três semanas após a instalação. Dentro deste período, verificou-se a recepção de dados provenientes das duas instalações e, apesar de os dispositivos baseados na presente plataforma continuarem em funcionamento, esperava-se que a autonomia dos sensores EWS TA3T-r4 não ultrapassasse os 4 meses, uma vez que o seu consumo médio é de cerca de 1,2 mA, devido ao facto de o sensor de aceleração se encontrar constantemente em modo ligado, para detectar a abertura do disjuntor.

Também na subestação de Corrente foram tiradas medidas para validação do bom funcionamento dos sensores, apresentando-se aqui dados recebidos da abertura e fecho de um disjuntor (sendo que esse evento foi provocado). Os resultados são apresentados nas figuras seguintes.

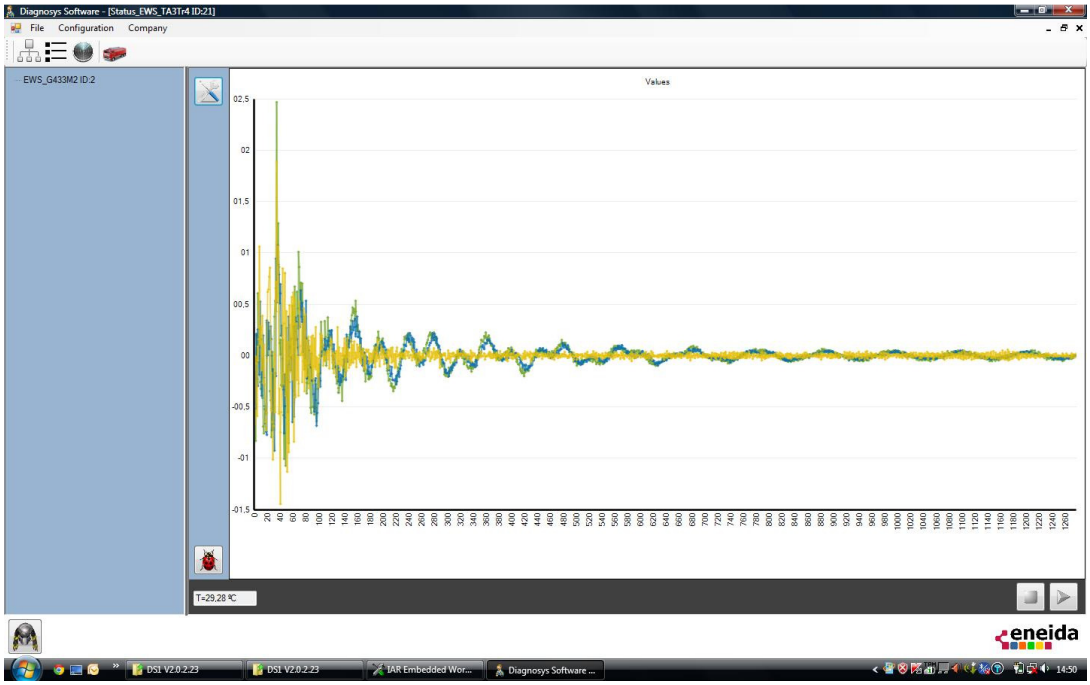


Figura 136 - Padrão de vibração da abertura de um disjuntor de alta tensão (eixo dos yy - intensidade de aceleração, eixo dos xx, amostras – 1260 para cada eixo).

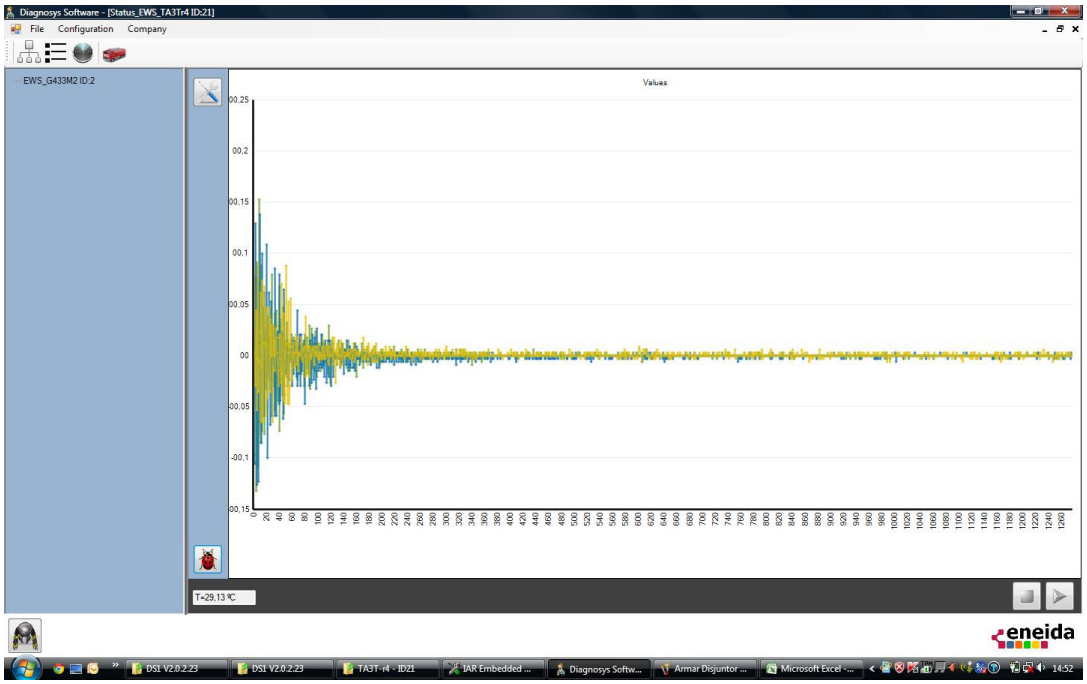


Figura 137 - Padrão de vibração do fecho de um disjuntor de alta tensão (eixo dos yy - intensidade de aceleração, eixo dos xx, amostras – 1260 para cada eixo).

A avaliação dos dispositivos instalados na subestação eléctrica de Corrente obteve resultados equivalentes àqueles da subestação do Alto de S. João, sendo que aqui, por via de se haver detectado uma falha no desenho do dispositivo EWS TA-r – como já foi referido, relacionada com a falta de 2 camadas internas, de massa e Vcc –, estes não foram instalados. O resultado a realçar e que foi possível retirar desta instalação, sendo especialmente importante, está ligado ao facto de plataforma desenvolvida permitir comunicações com dispositivos instalados no interior de um armário, ainda que para curtas distâncias. Este resultado é apenas possível devido à utilização da gama de frequência dos 433 MHz, sendo certo que não o seria sobre 2.4 GHz, de acordo com os resultados obtidos para alcances com a plataforma desenvolvida para essa frequência.

7.2. Pontos quentes em barramentos de alta tensão

A única instalação no terreno efectuada com base na rede *ZigBee* foi feita tendo como objectivo a monitorização de pontos quentes associados a um barramento de alta tensão, através da medição de temperatura na superfície do barramento e do disjuntor associado. Devido a problemas que poderão existir na condução de energia eléctrica, a temperatura destes equipamentos poderá subir até cerca de 80ºC, sendo indicativa de alta dissipação de energia. Por outro lado, e tal como no caso dos órgãos presentes na subestação eléctrica, também aqui não é permitida a instalação de cabos, que causariam curto-circuitos entre o barramento e o exterior, sendo portanto imperativa uma instalação sem fios.

Estes barramentos encontram-se num ambiente fechado, consistindo em salas e galerias de betão, com portas gradeadas em metal. Também por essa razão foi necessário recorrer a dispositivos sem fios, para transmissão de dados da "gaiola" em torno do barramento até à *gateway* (Coordenador), colocada numa sala contígua.

Como tal, foi feita uma instalação piloto, tendo-se utilizado três dispositivos:

- 1 *gateway CANbus – ZigBee*, actuando como unidade Coordenadora;
- 2 sensores de temperatura TT-r2 – sensores em tudo equivalente ao sensor de aceleração e temperatura, mas no qual não foi instalado o sensor de aceleração e onde foi removido o código de controlo referente a esse sensor.

Os sensores recolhem e transmitem periodicamente medições de temperatura (a cada minuto). Para o sensor colocado sobre o barramento foi desenhada uma caixa especial, fabricada em aço (com as mesmas dimensões internas, para colocação das placas de circuito impresso), mas com uma dimensão exterior menor. A caixa tem ainda um revestimento externo em plástico, para isolamento. O conjunto de todos os dispositivos é apresentado na Figura 139.

Com um tão reduzido conjunto de dispositivos, a rede formada foi naturalmente em estrela, com os dois sensores a comunicarem directamente para o dispositivo Coordenador/*gateway*. A tabela de endereços utilizada é apresentada na Tabela 47.

Tabela 47 - Identificadores da rede de monitorização de pontos quentes em barramentos de alta tensão.

Dispositivo	**Localização**	**Identificador**
Sensor de Temperatura	Barramento de alta tensão	5
Sensor de Temperatura	Disjuntor	6
Gateway	Corredor contíguo	2

Os dispositivos sensores e o Coordenador distam entre si de sensivelmente 3 metros, estando a meio dessa distância a referida grade de ferro que impede o acesso à sala do barramento e disjuntor de alternador. Para transmissão de dados do local de monitorização para uma sala distante de monitorização, a cerca de 50 m e através de duas galerias, foi instalada uma outra ligação sem fios, de tecnologia de comunicações na gama dos 433 MHz, com base em dispositivos de uma gama anterior àquela desenvolvida. Esta ligação foi criada porque era expectável, com base em testes de laboratório, que o sinal 2.4 GHz não alcançasse a distância pretendida, e portanto foram utilizados outros dispositivos, baseados na referida gama dos 433 MHz (mais uma vez, cujo desenvolvimento não está no âmbito deste trabalho), para ultrapassar essa distância. Na figura seguinte é apresentada a estrutura da referida rede.

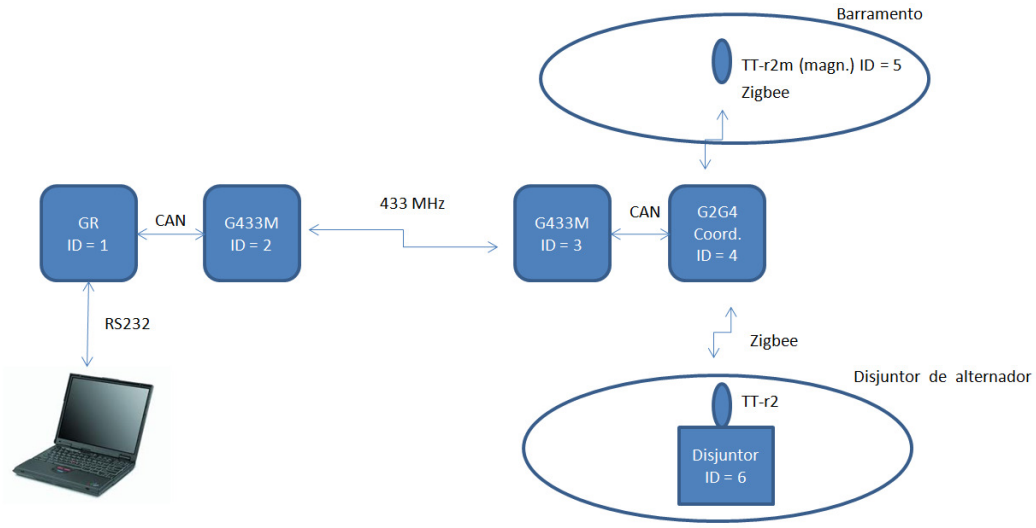


Figura 138 - Estrutura da rede de comunicações referente ao sistema de monitorização de temperatura.

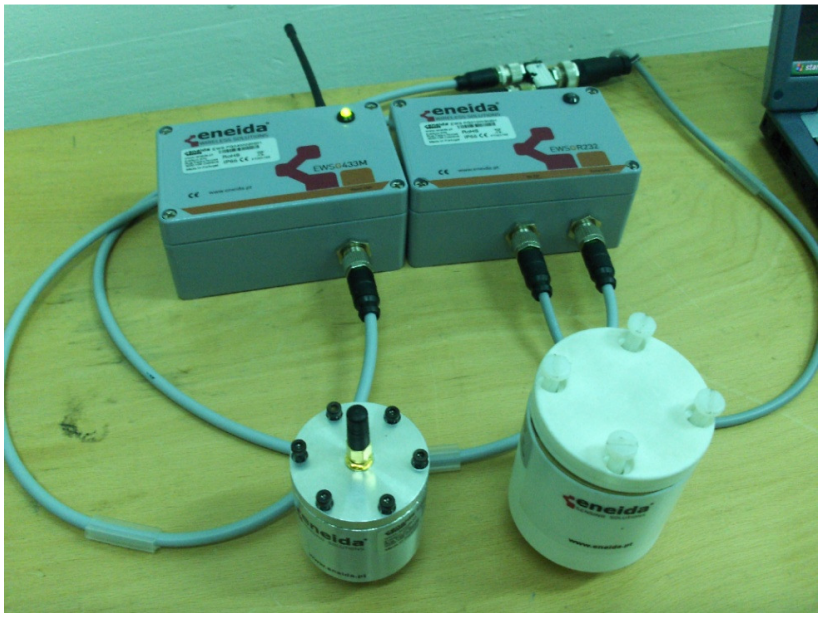


Figura 139 - Sistema de monitorização de pontos quentes em barramentos. Preparação para instalação, o sensor à esquerda tem uma caixa especial, em plástico, para instalação sobre o barramento de alta tensão.

Os sensores instalados têm as características descritas nas secções anteriores para o sensor de aceleração e temperatura, com a diferença de que o seu consumo é consideravelmente mais baixo (por via de não ter um sensor de aceleração instalado), na casa dos 100 µA por hora. No entanto, este sistema piloto esteve instalado apenas para alguns testes do cliente, tendo estado em funcionamento apenas 2 meses, e com os resultados do lado do cliente. No entanto, não

foram detectadas falhas, tendo transmitido continuamente dados de temperatura do barramento, e o *feedback* recebido pelos utilizadores foi positivo.

As figuras seguintes apresentam-se, respectivamente, os sensores instalados nos pontos de monitorização, a sala onde se encontrava a *gateway* e a interface HMI, e a apresentação de dados na referida interface.

Figura 140 - Sensores de temperatura instalados sobre o barramento de alta tensão (esquerda) e disjuntor (direita).

Figura 141 - Sala onde ficou instalada a *gateway*/Coordenador e a interface humana. a sala onde se encontram os pontos de monitorização está à esquerda da porta gradeada.

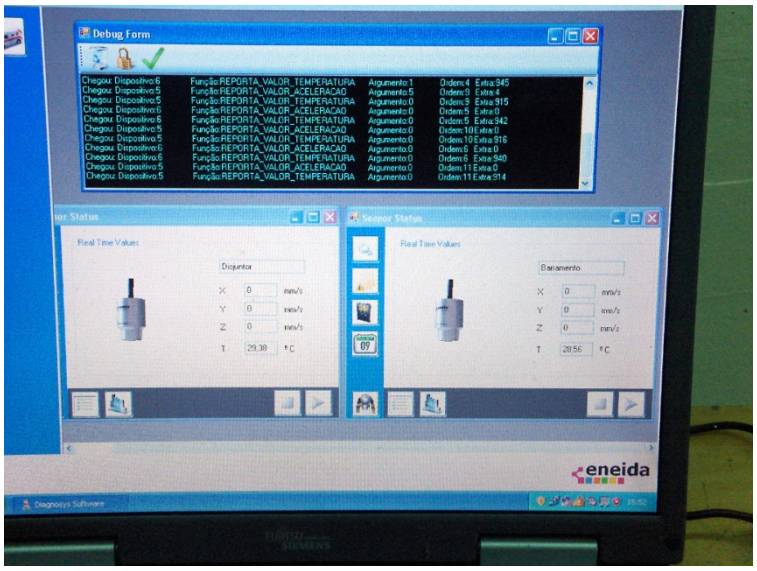


Figura 142 - Interface humana para verificação e registo de valores medidos.

Relativamente aos resultados da instalação, apenas são visíveis através de dois indicadores: os dados adquiridos entre a tarde em que o sistema foi instalado e a manhã seguinte, na qual se verificou o funcionamento adequado dos dispositivos instalados, e o *feedback* do cliente, a empresa EDP Produção, em cujo computador foi instalado o *software* de visualização de dados.

Em relação ao primeiro indicador, foi registado o conjunto de dados recebidos, correspondente aos valores de temperatura dos dois equipamentos monitorizados, no período entre as 18:45 do dia 19 de julho de 2010 e as 9:45 do dia 30 de julho de 2010. Neste período, não foi detectada qualquer falha de comunicação, apresentando-se de seguida o gráfico representativo da medição da temperatura no barramento e no disjuntor do alternador.

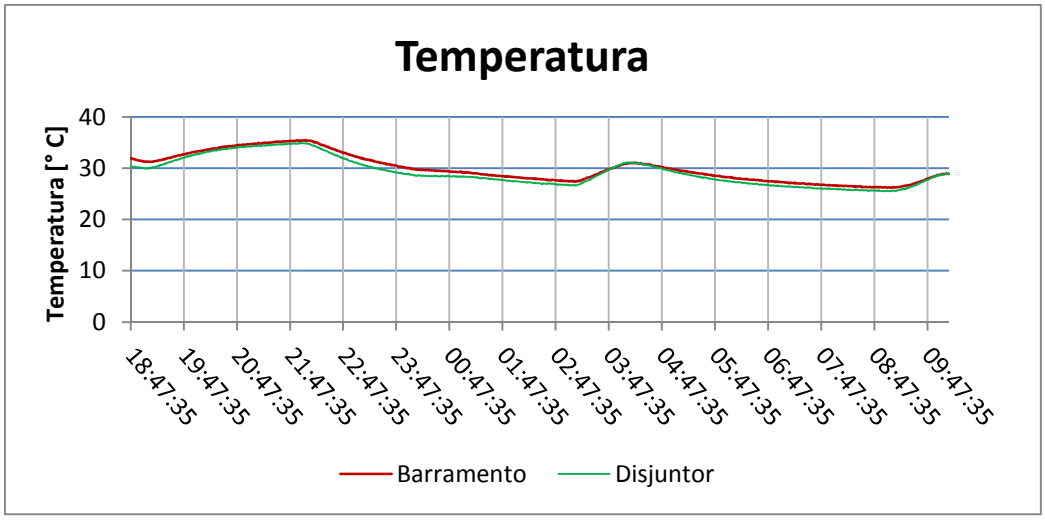


Figura 143 - Variação da temperatura medida sobre o Barramento e a carcaça do Disjuntor de alternador na instalação da Barragem do Alqueva.

Relativamente ao segundo indicador, relacionado com a apreciação por parte do cliente, o *feedback* foi positivo, tendo-se revelado que o sistema se manteve operacional durante o tempo pretendido, permitindo uma monitorização contínua dos dois equipamentos.

Dos resultados existentes, é possível concluir que, apesar dos campos magnéticos gerados pelos equipamentos de alta tensão, os dispositivos desenvolvidos mantêm o seu bom funcionamento, operando ininterruptamente. Este bom funcionamento está relacionado não só com a capacidade da tecnologia de comunicações sem fios sobre 2.4 GHz em operar naquele ambiente, mas também da fiabilidade da electrónica desenvolvida, bem adaptada ao funcionamento nas proximidades de campos magnéticos elevados.

8. Conclusões

O desenvolvimento de qualquer dispositivo ou *software* desde a sua conceptualização até à sua execução e ao seu teste é um longo percurso, onde encontramos vários becos sem saída, sendo necessário regressar atrás e perceber onde estava a falha, e como se pode resolvê-la de forma a progredir. Esta é uma verdade aplicável a muitas áreas do conhecimento e foi sentida por muitas vezes durante todo este trabalho de desenvolvimento, uma vez que a concepção de uma plataforma de comunicações para ambiente industrial não consiste simplesmente na criação de um conjunto de placas de circuito impresso que comuniquem entre si através de dispositivos rádio que nelas estão soldados. É necessário compatibilizar essas pequenas plataformas com as aplicações que delas se pretendem retirar, nas suas mais variadas vertentes, seja um sensor inteligente, uma unidade concentradora ou um *Router/gateway* de informação. Aqui entra a programação do *software* associado ao dispositivo, é certo que é necessário criar um programa que possibilite a comunicação entre dispositivos, mas também a interface para a aplicação, devendo esta ter um conjunto de comandos universais, que possam ser invocados de forma equivalente em qualquer uma das diferentes aplicações.

Nesse ponto em que se trata a interface com as aplicações, é necessário estudar se estas já estão desenvolvidas, ou se é necessário reprogramá-las, para que executem os procedimentos que se pretendem. Esta necessidade foi sentida tanto na criação dos sensores como das *Gateways*, uma vez que os primeiros não tinham quaisquer características de muito baixa potência, e os segundos não estavam preparados para lidar com quantidades de dados tão elevadas quanto aquelas encontradas nas aplicações em questão. Para além da criação de novas funções, é ainda imperativo tratar da interface do lado do microcontrolador da aplicação, para que este reconheça o conjunto de comandos que pode invocar para controlar o dispositivo rádio. Não é uma tarefa trivial, a da compatibilização de interfaces série, quando se programa um dos dispositivos para comunicar com outro que já está desenvolvido e testado (caso da interface com o controlador de comunicações *ZigBee*, vendido como produto final), sendo ainda mais difícil compatibilizar as interfaces série de dois dispositivos programáveis. Apenas foi possível consegui-lo através de ferramentas de monitorização de linhas digitais, para reconhecer se pinos de sinalização e sincronismos de transmissão se encontravam realmente acertados. Essas falhas poderão mesmo advir de problemas na concepção das próprias placas de circuito impresso, como um erro no desenho de uma pista. Essa foi outra das grandes batalhas travadas, desde a aprendizagem com as ferramentas de desenvolvimento de CAD electrónico até à primeira placa de circuito

impresso, e daí ao primeiro protótipo que cumpriu com os requisitos, tanto ao nível das comunicações sem fios como de interface com o respectivo controlador de aplicação.

Neste ponto, estamos ainda ao nível do interior do dispositivo, que na verdade consiste na maior parte daquilo que o define, mas é também necessário idealizar e conceber o seu invólucro, de que forma se colocarão as placas de circuito impresso no seu interior, onde se colocará a bateria (questão especialmente importante no caso do sensor de vibração, que se pretende compacto e incapaz de gerar vibrações secundárias), se será fácil de trocar, de que forma poderá a caixa abrir para que continue a ser estanque após a manutenção ou como se fixará a caixa ao ponto de monitorização no terreno. Também este estudo e trabalho de desenvolvimento necessitou de tempo e tentativas até chegar a um resultado que segue as linhas de orientação definidas na especificação inicial. Depois, verificar se a programação elaborada cumpre com os requisitos iniciais, testar o sistema em condições semelhantes às do terreno, reprogramar algumas funções, e por vezes encontrar problemas que necessitam a alteração de um componente, e consequentemente da placa de circuito impresso – levando ao recomeço do processo.

Comparando agora as características das plataformas desenvolvidas com os objectivos delineados, podemos dizer que grande parte dos objectivos foram cumpridos, foram desenvolvidas duas plataformas que foram integradas com aplicações pré-existentes, e foram desenvolvidas funcionalidades nessas mesmas aplicações de forma a poderem receber as referidas plataformas, cumpriu-se o critério de baixa potência, tendo-se escolhido o conjunto de componentes que permitiu atingi-lo. Adicionalmente, as plataformas são sem dúvida modulares, permitindo criar ainda outros sistemas de monitorização, naturalmente desde que conheçam o conjunto de comandos para o seu controlo e tenham o conjunto de três fichas necessário para a interface física. O reduzido conjunto de funções definidas, especialmente no sistema 433 MHz, (que permitiu maior flexibilidade de programação) são simples de invocar, tendo-se tentado reduzi-las ao indispensável, tal como demonstra a API apresentada no capítulo 4.

Serve este pequeno resumo para suportar o argumento de que o conjunto de objetivos inicialmente elencado pode ser alcançado de diversas formas, sendo que a solução nunca é simplesmente a melhor em termos de performance, mas sim aquela que tem a melhor performance possível, tendo igualmente em conta decisões relacionadas com o preço, a disponibilidade e consequentemente o tempo até um produto atingir o mercado, e também as ferramentas que já temos disponíveis, e que nos permitem conciliar os dois critérios de custo e tempo.

Nos casos em que existe já uma colaboração com um cliente – como foi o caso –, o tempo de desenvolvimento de uma solução deverá também cumprir, tanto quanto possível, com os prazos estabelecidos para entrega da primeira solução.

Assim, é possível argumentar que a solução alcançada é a melhor possível, pois apesar de não seguir uma das mais recentes normas que permitem implementar um algoritmo de *routing* mais sofisticado ou um mecanismo de segurança de dados mais elaborado, esta foi a solução alcançada a tempo, que permitiu criar as soluções pretendidas – através de mecanismos alternativos, por exemplo, ao referido protocolo de *routing* – e o fez dentro de custos estabelecidos, sendo ainda uma plataforma susceptível de vir a ter acrescentos, nomeadamente na convergência com uma das normas enunciadas, como o protocolo *DASH7*.

Uma das soluções desenvolvidas (433 MHz) permite a criação de redes sem fios em ambiente industrial numa área de 500 m de raio – em linha de vista –, possibilitando uma ocupação de uma área de 0,8 km^2, que cumpre com normas técnicas de comercialização de produtos, e que cumpriu com várias instalações em cenário real (casos das subestações eléctricas), integrando uma plataforma inovadora não só pelas suas características de sensorização mas também da rede de comunicações sem fios que ali foi implementada. Por outro lado, e tal como já foi relevado no capítulo dedicado a instalações no terreno, esta mesma plataforma permitiu comunicações a 20 m de distância com um dispositivo que se encontrava encerrado num armário metálico, vantagem que não seria por certo alcançada com um dispositivo baseado nos 2.4 GHz.

A outra plataforma – *ZigBee* – poderá vir a ficar sem um maior desenvolvimento, uma vez que não existindo clientes interessados nas suas soluções, também não conseguirá fazer a sua entrada no mercado. Esta falta de interesse poderá estar relacionada com o avanço de outros protocolos melhor preparados para aquele ambiente, como o protocolo *WirelessHART* ou o protocolo *ISA100.11a.* O protocolo *WirelessHART*, como foi anteriormente argumentado, apresenta-se mesmo na actualidade como o protocolo de comunicações para redes sem fios de baixa potência com melhores características para a operação em ambiente industrial, ao apresentar valências relevantes em relação aos seus competidores em diversas camadas protocolares. Ao nível da camada de Enlace, permite um maior seccionamento da largura de banda disponível em relação aos restantes protocolos, através da combinação dos esquemas de FHSS e de TDMA (provenientes do protocolo de base TSMP). Ao mesmo tempo, ao integrar o mecanismo de acesso múltiplo FHSS, permite também uma melhor tolerância a interferência e distorção multi-caminho, bem típicas do ambiente industrial. Ao nível da camada de Rede, a topologia emalhada associada à capacidade de todos os nós – inclusivamente os Dispositivos Terminais – terem a capacidade de cumprirem funções de associação de outros dispositivos e reencaminhamento de dados é muito interessante do ponto de vista da robustez da rede, pois permite que no caso em que um dispositivo que cumpria funções de reencaminhamento de dados para outros falhe (na nomenclatura do *WirelessHART*, um dispositivo pai), qualquer outro que se encontre nas imediações dos dispositivos filho daquele que falhou se torne o seu novo dispositivo pai, e a rede se adapte. Por outro lado, esta valência permite ainda uma maior

versatilidade no crescimento da rede, visto que a partir de qualquer nó se poderão associar novos elementos. Veja-se que, uma nova instalação é quase sempre faseada, começando-se por monitorizar um conjunto de pontos inferior à totalidade daqueles que se pretende medir. Dado que existe este carácter de crescimento progressivo da rede, é importante que esta esteja preparada para a associação de novos elementos, sendo que o protocolo *WirelessHART*, com a sua rede totalmente emalhada, é indubitavelmente o mais bem preparado para esta situação, dentro da gama dos 2.4 GHz.

Ainda relativamente à plataforma para os 2.4 GHz, desenvolvida sobre o protocolo *ZigBee*, esta ficou num estado intermédio da sua validação, pois seria importante ter conseguido obter um pedido por parte de um cliente que possibilitasse a instalação de uma rede de maiores dimensões – maior área coberta e maior número de dispositivos instalados – que permitisse realmente testar a sua performance. Tendo em conta que tal instalação apenas seria possível existindo essa vontade por parte de um cliente, e que, a existir, representaria intervenção em equipamentos do cliente e seguimento por parte dos seus recursos humanos, não foi realmente possível conseguir um cliente ou mesmo parceiro para testar esta plataforma.

Apesar das óbvias valências do protocolo *WirelessHART*, pretende-se aqui demonstrar que não seria possível ter hoje dois sistemas desenvolvidos sobre qualquer um daqueles protocolos – e este constrangimento temporal é real, uma vez que foram feitas instalações requeridas por clientes, com base nestes sistemas –, pelas razões já apontadas de inacessibilidade a código de base ou de módulos de comunicações preparados para levar a cabo a concepção de um produto.

Apesar disso, acredito que venham a ser esses protocolos a vingar na área industrial, principalmente por virem a ser compatíveis entre si, não obstante acreditar também que a gama dos 433 MHz tem algo a dizer para as comunicações industriais sem fios de baixa potência, por possibilitar alcances (e consequentes consumos) e tolerância a ruído industrial ou proveniente de outros protocolos de comunicação (tipicamente nos 2.4 GHz) impraticáveis para protocolos que assentam em gamas na casa dos 2.4 GHz.

O protocolo *DASH7*, até ao momento o único representante e com uma especificação tornada pública recentemente, que além disso integra o apoio da divisão de investigação do departamento de defesa dos EUA (DARPA), poderá mesmo nos próximos anos vir a implantar-se e a vingar nesta área, onde outros já levam avanço.

De que forma é que os sistemas que se desenvolveram se poderão adaptar a esta realidade onde existem competidores de nível mundial, com um reconhecimento maior? Primeiramente, da mesma forma que até agora, trabalhando directamente com clientes e mostrando de que forma os sistemas se podem adaptar aos seus intentos. No entanto, também a monitorização sem fios e

posteriormente a automação se tornarão do conhecimento comum, existindo sistemas mais simples de instalar, e que os próprios clientes conhecerão e pretenderão.

É então necessário que o protocolo de comunicações 433 MHz siga a linha do protocolo *DASH7*, pois tendo em conta o conhecimento existente hoje, será esse o protocolo forte para o ambiente industrial nos 433 MHz.

Quanto ao protocolo *ZigBee*, à partida não terá perfis desenvolvidos para a área da monitorização ou automação industrial, mantendo-se na área da domótica. Poderá ser um produto interessante na medida em que já é reconhecido, apesar de não possibilitar a compatibilidade com outros sistemas, nesta área.

Adicionalmente, que outros desenvolvimentos poderão ser feitos? Um dos principais prende-se com uma questão que foi pouco debatida nesta dissertação, precisamente porque o cerne do desenvolvimento levado a cabo não se prendeu com ela, que é a renúncia às baterias ou às fontes de alimentação perenes, introduzindo nos nossos dispositivos meios de captação energética do meio ambiente.

É disso exemplo a captação energética a partir de vibrações, no caso do sensor de vibração e temperatura; do campo magnético gerado por um condutor de alta tensão, no caso do sensor de temperatura para pontos quentes em barramentos; ou do sensor de corrente para equipamentos de alta e média tensão, em subestações; ou solar, em quaisquer sensores instalados ao ar livre (caso do sensor de vibração e temperatura instalado no exterior no caso da aplicação para subestações eléctricas).

Apesar de o objectivo não ser o de mencionar marcas ou modelos de produtos comerciais, seguidamente apresenta-se a representação física dos projectos desenvolvidos nesta dissertação de doutoramento, com algumas imagens retiradas das fichas técnicas dos dispositivos concebidos, e que actualmente fazem parte do catálogo de produtos da Eneida, Lda.

Figura 144 - Sensor de temperatura *ZigBee* - TT-r2.

Figura 145 - Sensor de aceleração e temperatura de rede sem fios 433 MHz.

Figura 146 - *Gateway* de comunicações *CANbus* - 433 MHz.

Figura 147 - *Gateway* de comunicações *CANbus* - *ZigBee*.

Bibliografia

1. **CiA.** (2011) Controller Area Network (CAN) in Automation. [Online]. *CAN in Automation.* [Online] Outubro 13, 2011. [Cited: Outubro 13, 2011.] http://www.can-cia.org.

2. **HART Communication Foundation.** HART Communication Foundation. [Online] 2011. http://www.hartcomm.org/.

3. **Bennet, S.** *A history of control engineering 1930-1955.* s.l. : The Institution of Engineering and Technology - IET, 1993.

4. **Kuphaldt, T.** *Lessons in Industrial Instrumentation.* s.l. : Open Book Project, 2011.

5. **Pinto, J.** Brief history of Industrial Instrumentation. *Intech.* 2010, Vol. Janeiro 2010.

6. **Mainwaring, A., et al.** Wireless Sensor Networks for Habitat Monitoring. Atlanta, EUA : ACM, 2002.

7. **Welsh, M. et al.** Monitoring Volcanic Eruptions with a Wireless Sensor Network. [Online] Julho 26, 2004. http://www.eecs.harvard.edu/~werner/projects/volcano/.

8. **União Europeia.** DIRECTIVA 2004/108/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 15 de Dezembro de 2004 relativa à aproximação das legislações dos Estados-Membros respeitantes à compatibilidade electromagnética e que revoga a Directiva 89/336/CEE. [Online] 2004. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:390:0024:0037:PT:PDF.

9. **International Electrotechnical Commission.** Norma IEC 61131-2: Programmable controllers - Part 2: Equipment requirements and tests. [Online] 2007. http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/38182.

10. **União Europeia.** DIRECTIVA 1999/5/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 9 de Março de 1999 relativa aos equipamentos de rádio e equipamentos terminais de telecomunicações e ao reconhecimento mútuo da sua conformidade. [Online] 1999. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1999:091:0010:0028:PT:PDF.

11. **Siva Ram Murthy, S. and Manoj, B.** *Ad Hoc Wireless Networks: Architectures and Protocols.* Nova Deli, Índia : Pearson Education, 2009.

12. **Chien, Charles.** Digital radio systems on a chip: a systems approach. [Online] 2001. http://books.google.pt/books?id=9TtGWdMKBgUC&source=gbs_navlinks_s.

13. **Baronti, P., et al.** Wireless sensor networks: A survey on the state of the artand the 802.15.4 and ZigBee standards. *Computer Communications 30.* 2007, pp. 1655-1695.

14. **Gustafsson, David.** *WirelessHART- Implementation and Evaluation on Wireless Sensors.* Estocolmo, Suécia : KTH Electrical Engineering, 2009.

15. **Nardis, Luca De and Benedetto, Maria-Gabriella Di.** Overview of the IEEE 802.15.4/4a standards for low data rate Wireless Personal Data Networks. *4th WORKSHOP ON POSITIONING, NAVIGATION AND COMMUNICATION 2007 (WPNC'07), HANNOVER, GERMANY.* 2007.

16. **IEEE 802 LMSC.** IEEE 802. *LMSC, LAN/MAN Standards Committee (Project 802).* [Online] Outubro 12, 2011. [Cited: Outubro 14, 2011.] http://ieee802.org/.

17. **IEEE Computer Society.** *IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks Specific requirements - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification...* Nova Iorque, EUA : IEEE, 2007. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).

18. **ANT.** ANT. *This is ANT, the Wireless Sensor Network Solution.* [Online] Outubro 13, 2011. [Cited: Outubro 13, 2011.] www.thisisant.com.

19. **DASH7 Alliance.** DASH7. *dash7.org.* [Online] Outubro 13, 2011. [Cited: Outubro 13, 2011.] http://www.dash7.org/.

20. **IEEE 802.15 TG4.** IEEE 802.15 WPAN Task Group 4 (TG4). *IEEE 802.15 WPAN Task Group 4 (TG4).* [Online] Janeiro 27, 2010. [Cited: Outubro 14, 2011.] http://www.ieee802.org/15/pub/TG4.html.

21. **IEEE 802.15 WG for WPAN.** IEEE 802.15 Working Group for WPAN. *IEEE 802.15 Working Group for WPAN.* [Online] Julho 2011, 2011. [Cited: Outubro 14, 2011.] http://ieee802.org/15/index.html.

22. **IEEE Computer Society.** IEEE Standard Association. *Part 15.4: Wireless Medium Access (...) for Low-Rate WPANs.* [Online] 2006, Setembro 8, 2006. [Cited: Outubro 18, 2011.] http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf.

23. —. IEEE Standard Association. *Part 15.4: Wireless Medium Access (...) for Low-Rate WPANs.* [Online] Outubro 1, 2003. [Cited: Outubro 19, 2011.] http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf.

24. **ZigBee Alliance.** ZigBee FAQ. *ZigBee.* [Online] 2011. [Cited: Outubro 19, 2011.] http://www.ZigBee.org/About/FAQ.aspx.

25. —. *ZigBee Home Automation Public Application Profile.* [Online] 1.1, Fevereiro 8, 2010. [Cited: Outubro 20, 2011.] http://www.ZigBee.org/Standards/ZigBeeHomeAutomation/download.aspx.

26. **ZigBee Standards.** *ZigBee Alliance.* [Online] 2011. [Cited: Outubro 20, 2011.] http://www.ZigBee.org/Standards/Overview.aspx.

27. **Gislaslon, D.** *ZigBee Wireless Networking.* Oxford : Newnes, 2008.

28. **Texas Instruments.** CC2530. [Online] Rev. B, Outubro 5, 2010. [Cited: Outubro 20, 2011.] http://www.ti.com/product/cc2530.

29. **Digi International.** XBee PRO. *ZigBee RF Modules.* [Online] 2011. [Cited: Outubro 20, 2011.] http://www.digi.com/products/wireless-wired-embedded-solutions/ZigBee-rf-modules/ZigBee-mesh-module/xbee-zb-module#overview.

30. **Ember.** EM351 / EM375 SoCs. [Online] Maio 5, 2011. [Cited: Outubro 20, 2011.] http://www.ember.com/products_ZigBee_chips_e300series.html.

31. **Shelby, Zach and Bormann, Carsten.** *6LoWPAN: The Wireless Embedded Internet.* s.l. : Wiley, 2011.

32. **Ee, Gee Keng, Ng, Chee Kyun and Ali, Nor Kamariah Noordin e Borhanuddin Mohd.** A Review of 6LoWPAN Routing Protocols. *Proceedings of the Asia Pacific Advanced Network.* 2011.

33. **SICS.** The uIP TCP/IP stack. *6LoWPAN implementation.* [Online] Outubro 20, 2008. [Cited: Outubro 25, 2011.] http://www.sics.se/~adam/contiki/docs-uipv6/a01109.html/.

34. **Shelby, Zach, Chakrabarti, S. and Nordmark, E.** Neighbor Discovery Optimization for Low Power and Lossy Networks. *draft-ietf-6lowpan-nd-18.* [Online] Outubro 24, 2011. [Cited: Outubro 25, 2011.] http://tools.ietf.org/search/draft-ietf-6lowpan-nd-18#page-6.

35. **Kushalnagar, N., et al.** Transmission of IPv6 Packets over IEEE 802.15.4 Networks. *RFC4944.* [Online] 2007. [Cited: Outubro 25, 2011.] http://www.ietf.org/rfc/rfc4944.txt.

36. **NXP Semiconductors.** JenNet-IP. [Online] 2011. [Cited: Outubro 26, 2011.] http://www.jennic.com/files/product_briefs/JenNet-IP-PBv1.11docx.pdf.

37. **ISA100 Wireless Compliance Institute.** The Technology Behind the ISA100.11a Standard – An Exploration. *ISA100 Wireless Compliance Institute - Education.* [Online] Junho 15, 2010. http://www.isa100wci.org/Documents/PDF/The-Technology-Behind-ISA100-11a-v-3_pptx.aspx.

38. **Verhamme, I.** Wireless control for Process Automation using ISA100.11a. *Industrial Ethernet Book.* 2011, Vol. 64.

39. **Werb, Jay.** *The Technology Behind ISA100.11a.* Yokohama : ISA100 Wireless, 2010.

40. **Dust Networks.** Technical Overview of Time Synchronized Mesh Protocol (TSMP). [Online] http://cds.linear.com/docs/en/white-paper/TSMP_Whitepaper.pdf.

41. **International Society of Automation.** ISA100.11a, Release 1 - An Update on the First Wireless Standard Emerging from the Industry for the Industry. [Online] Outubro 2007. http://www.isa.org/source/ISA100.11a_Release1_Status.ppt.

42. *WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control.* **Song, J., et al.** St. Louis, MO, EUA : Proceedings of the IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), Abril 2008.

43. **ISA100 Wireless Compliance Institute.** Organization. [Online] ISA100, 2011. [Cited: Novembro 2, 2011.] http://www.isa100wci.org/About-Us/Organization.aspx.

44. **HART Foundation.** What is HART? [Online] 2011. [Cited: Novembro 2, 2011.] http://www.hartcomm.org/protocol/about/aboutprotocol_what.html.

45. **ABB Limited.** HART Communications Protocol - What's new in WirelessHART? *Information Bulletin - Instrumentation.* IB/INST–016, Vol. 1.

46. **HART Foundation.** Wireless HART - How it works. [Online] 2011. [Cited: Novembro 3, 2011.] http://www.hartcomm.org/protocol/wihart/wireless_how_it_works.html.

47. **Chen, D., et al.** *WirelessHART: Real-Time Mesh Network for Industrial Automation.* Nova Iorque, EUA : Springer, 2010.

48. *WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control.* **Jianping, S., et al.** s.l. : IEEE, 2008.

49. *Security Considerations for the WirelessHART Protocol.* **Raza, S., et al.** Mallorca, Espanha : s.n., 2009. Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation (ETFA).

50. **Control Global.** WirelessHART vs. ISA100.11a -- What's the Difference? . *Control Global.* [Online] Junho 20, 2012. http://www.controlglobal.com/articles/2012/nixon-wireless-isa.html.

51. **Mokhoff, N.** EE Times - News and Analysis. *EE Times.* [Online] Dezembro 20, 2011. http://www.eetimes.com/electronics-news/4233499/Linear-Technology-acquires-Dust-Networks.

52. **Dust Networks.** Smart Mesh WirelessHART PM2511 Network Manager. [Online] 2010. [Cited: Novembro 3, 2011.] http://www.dustnetworks.com/products/SmartMeshWirelessHART/PM2511.

53. **Nivis.** Industrial Sensing - VersaNode. [Online] 2011. [Cited: Novembro 3, 2011.] http://www.nivis.com/industrial_sensor_networks/VersaNode.php.

54. **RFM (EUA).** XDM2510HC - 2.4 GHz WirelessHART Transceiver Module. [Online] Março 17, 2011. [Cited: Novembro 3, 2011.] http://www.rfm.com/products/spec_sheet.php?wirelesshart2.4 GHz_&record=XDM2510HC.

55. **ISO/IEC.** *ISO/IEC 18000-7: Information technology -- Radio frequency identification for item management -- Part 7: Parameters for active air interface communications at 433 MHz.* s.l. : ISO/IEC, 2009.

56. **Fornazier, H., et al.** Wireless Communication : Wi-Fi, Bluetooth, IEEE 802.15.4, DASH7. 2012.

57. **DASH7 Alliance.** DASH7 Alliance Announces Updated Standard For Wireless Sensor Networks. [Online] Julho 20, 2010. [Cited: Novembro 7, 2011.] http://dash7.org/index.php?option=com_content&view=article&id=159%3Adash7-alliance-announces-updated-standard-for-wireless-sensor-networks&catid=14%3Apress-releases&Itemid=190.

58. —. What is DASH7 Technology? [Online] 2009. [Cited: Novembro 7, 2011.] http://dash7.org/index.php?option=com_content&view=article&id=9&Itemid=11.

59. **Indigresso.** DASH7 Mode 2. *Indigresso Wiki.* [Online] Indigresso, 03 26, 2012. http://www.indigresso.com/wiki/doku.php?id=dash7_mode_2:main.

60. **Norair, J.** *X. ISO 18000-7 Mode 2 An Advanced Communication System for Wide-Area Low Power Wireless Applications and Active RFID.* s.l. : DASH7 Alliance, 2011.

61. **Norair, JP.** *ISO 18000-7 Mode 2 Specification - DRAFT 012.* 2011.

62. **Mode 2 - Dash7 Alliance.** Mode 2 Revision to ISO 18000-7. 2010.

63. **Digi International Inc.** Digi. *XBee-Pro 802.15.4 OEM RF Modules.* [Online] 2011. [Cited: Outubro 19, 2011.] http://www.digi.com/products/wireless-wired-embedded-solutions/ZigBee-rf-modules/point-multipoint-rfmodules/xbee-series1-module#overview.

64. *Accurate Supercapacitor Modeling for Energy-Harvesting Wireless Sensor Nodes.* **Weddell, A., G., Merrett and Kazmierski T., Al-Hashimi B.** s.l. : IEEE Circuits and Systems Society, 2011. IEEE Transactions on Circuits and Systems II: Express Briefs.

65. *Lifetime Prediction for Supercapacitor-powered Energy-Harvesting Wireless Sensor Nodes.* **Renner, C., Jessen, J. and Volker Turau, V.** Hamburgo, Alemanha : s.n., 2009. Proceedings of the 8th GI/ITG KuVS Fachgespräch "Drahtlose Sensornetze".

66. **Varta.** Primary Lithium Cylindrical Cells Lithium-Thionyl-Chloride. *Varta microbattery.* [Online] 2011. [Cited: Novembro 10, 2011.] http://www.varta-microbattery.com/en/mb_data/documents/sales_literature_varta/LEAFLET_Primary_Lithium_Cylindrical_Series_ER_en.pdf.

67. **Tadiran Batteries.** Tadiran iXtra Series. [Online] 2008. http://www.tadiranbat.com/pdf.php?id=TL-5903.

68. **Watterson, C.** Controller Area Network (CAN) Implementation Guide. [Online] 2012. http://www.analog.com/static/imported-files/application_notes/AN-1123.pdf.

69. **Voss, W.** *A Comprehensible Guide to Controller Area Network.* s.l. : Copperhill Media, 2005.

70. **Texas Instruments - CC2530.** CC2530 SoC Datasheet. [Online] Fevereiro 2011. http://www.ti.com/lit/ds/symlink/cc2530.pdf.

71. **Radiocrafts.** *Radiocrafts RC2400HP-ZNM.* [Online] 1.2, 2011. http://www.radiocrafts.com/uploads/rc2400_rc2400hp_data_sheet_1_2.pdf.

72. **IETF.** IPv6 over Low power WPAN (6lowpan). [Online] 2012. https://datatracker.ietf.org/wg/6lowpan/.

73. **DASH7 Alliance.** Opentag. *Files.* [Online] Abril 25, 2011. [Cited:] http://sourceforge.net/projects/opentag/files/.

74. **Texas Instruments - *SimpliciTI*.** *SimpliciTI* Compliant Protocol Stack. [Online] Janeiro 7, 2010. http://www.ti.com/tool/*SimpliciTI*.

75. **Daintree Networks.** Getting started with ZigBee and IEEE 802.15.4. [Online] Fevereiro 2008. http://www.daintree.net/downloads/whitepapers/ZigBee_primer.pdf.

76. **NXP Laboratories.** *ZigBee PRO Stack User Guide.* [Online] Novembro 23, 2010. http://www.jennic.com/files/support_files/JN-UG-3048-ZigBee-PRO.pdf.

77. **Farahani, Shahin.** *ZigBee Wireless Networks and Transceivers.* 22 de Setembro de 2008. s.l. : Newnes, 2008. p. 360.

78. **Texas Instruments SWRA176.** *CC2480 Developer's Guide.* [Online] 2008. http://www.ti.com/lit/an/swra176/swra176.pdf.

79. **Texas Instruments - CC430.** *CC430 - MSP430 Soc with RF Core.* [Online] Dezembro 2011. [Cited:] http://www.ti.com/lit/ds/symlink/cc430f5137.pdf.

80. **Texas Instruments - *SimpliciTI* Specification.** *SimpliciTI Specification, v. 1.09.* 2009.

81. **Texas Instruments - MSP430F2417.** MSP430F2417 Datasheet. [Online] Dezembro 2011. http://www.ti.com/lit/ds/symlink/msp430f2417.pdf.

82. **Tadiran U.S. Battery Division.** Tadiran Lithium Batteries - MODEL TL-5935. *Tadiran Batteries.* [Online] 2012. http://www.tadiranbat.com/index.php/ixtra-high-preformance-lithium-batteries#wafer.

83. **Azom.com.** Aluminum Alloys - Aluminum 6082. [Online] 2012. http://www.azom.com/article.aspx?ArticleID=2813.

84. **Texas Instruments.** MSP430 Ultra-Low Power 16-bit MCUs - RF SoC Series - CC430F5135. *CC430 Family User's Guide.* [Online] http://www.ti.com/lit/ug/slau259e/slau259e.pdf.

85. **Radiocrafts.** RC2300-ZNM - ZigBee® Network Module . *Radiocrafts - Embedded Wireless Solutions.* [Online] 2008. http://www.radiocrafts.com/uploads/rc2300_znm_data_sheet_1_0.pdf.

86. **IEP.** *Relatório de Ensaio - EWS-Sistema Subestação.* 2011.

87. *Redes de Energia Eléctrica Inteligentes: Gestão de activos em subestações, com redes de sensores.* **Cardoso, F., et al.** Maputo, Moçambique : s.n., 2011.

88. **Bormann, C., Sturek, D. and Shelby, Z.** 6LowApp: Problem Statement for 6LoWPAN and LLN Application Protocols. *6LowApp.* [Online] Julho 13, 2009. [Cited: Outubro 26, 2011.] http://tools.ietf.org/html/draft-bormann-6lowpan-6lowapp-problem-01#page-7.

89. **TI e Sensinode.** CC-6LoWPAN Wiki. [Online] 2011. [Cited: Outubro 26, 2011.] http://processors.wiki.ti.com/index.php/CC-6LoWPAN.

90. **Kinney, Sexton.** Seminário Status ISA100.11a. [Online] ISA, 2008. [Cited: Outubro 28, 2011.] http://www.isa.org//Content/Microsites1134/SP100,_Wireless_Systems_for_Automation/Home1034/2008_02_ISASeminar_ISA100.11aStatus_Sexton_Kinney.pdf.

91. **opentag.** opentag. [Online] Opentag Mode 2, DASH7 Alliance, Abril 25, 2011. [Cited: Novembro 7, 2011.] http://sourceforge.net/projects/opentag/.

92. **Indigresso.** DASH7 Mode 2 in a Nutshell (Feature Summary). *The DASH7 Technology Expert.* [Online] Outubro 6, 2011. [Cited: Novembro 7, 2011.] http://www.indigresso.com/wiki/doku.php?id=dash7_mode_2:quickstart:features.

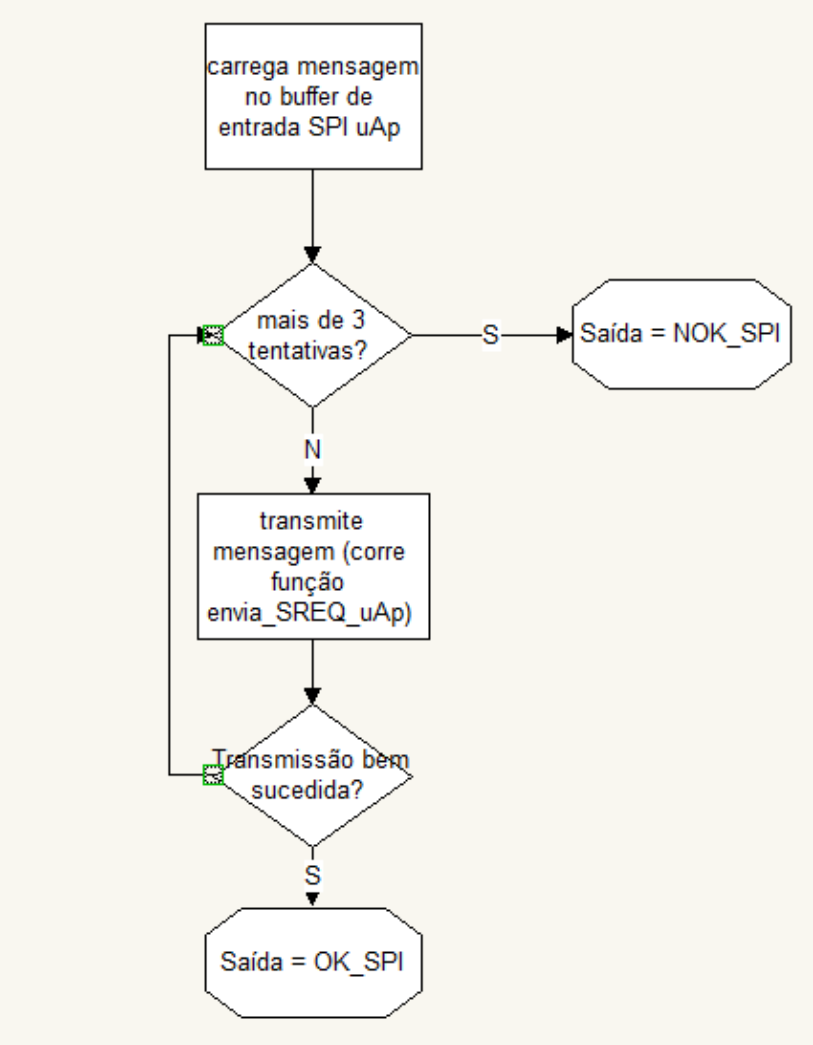
93. **CRP Technology.** Aluminum 6082-T6. [Online] http://www.crptechnology.com/sito/images/PDF/6082.pdf.

94. **Wolf, W.** *Computers as Components: Principles of Embedded Computer System Design.* s.l. : Morgan Kaufmann, 2005.

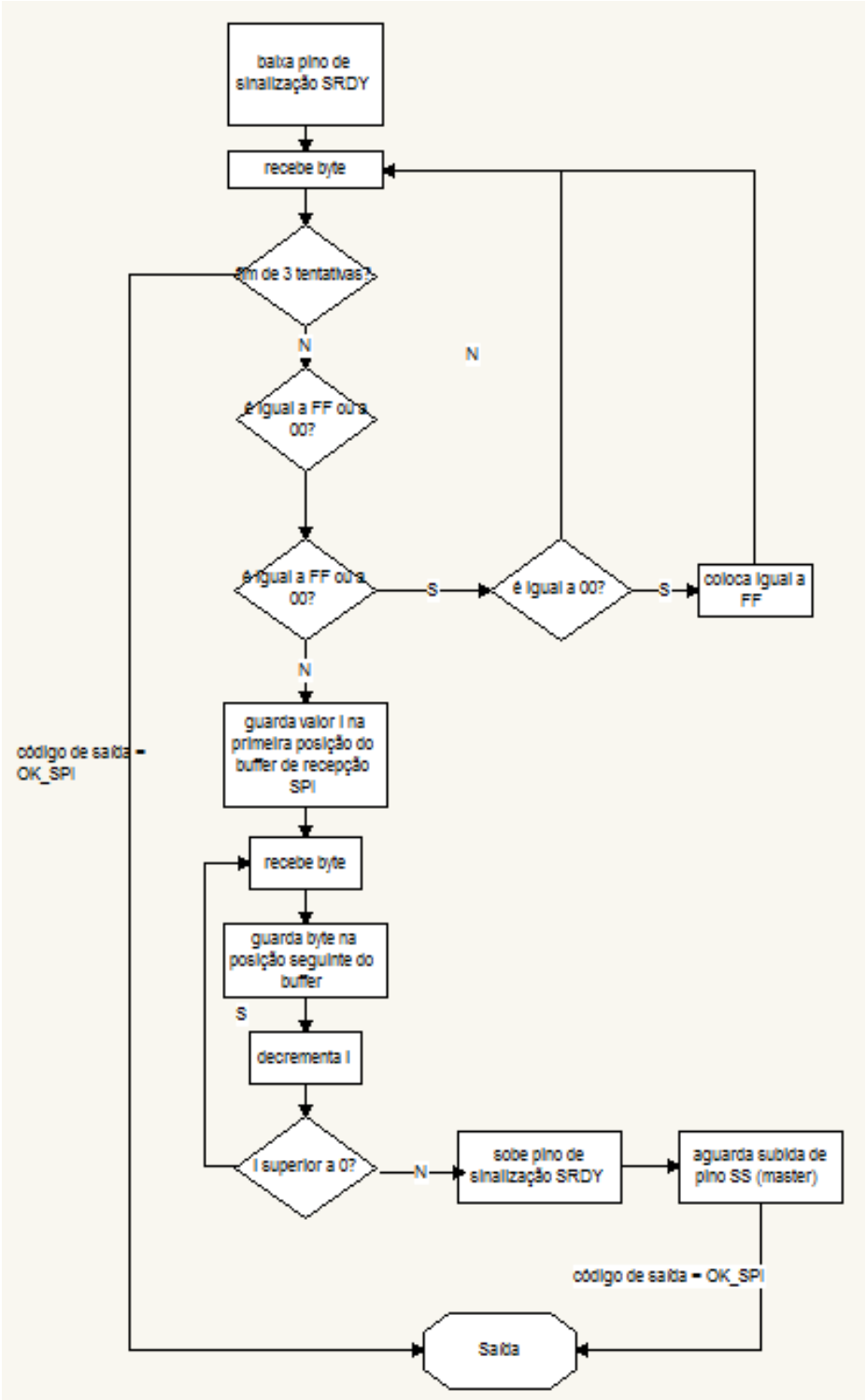
9. Anexo I

9.1. Protocolo 433 MHz

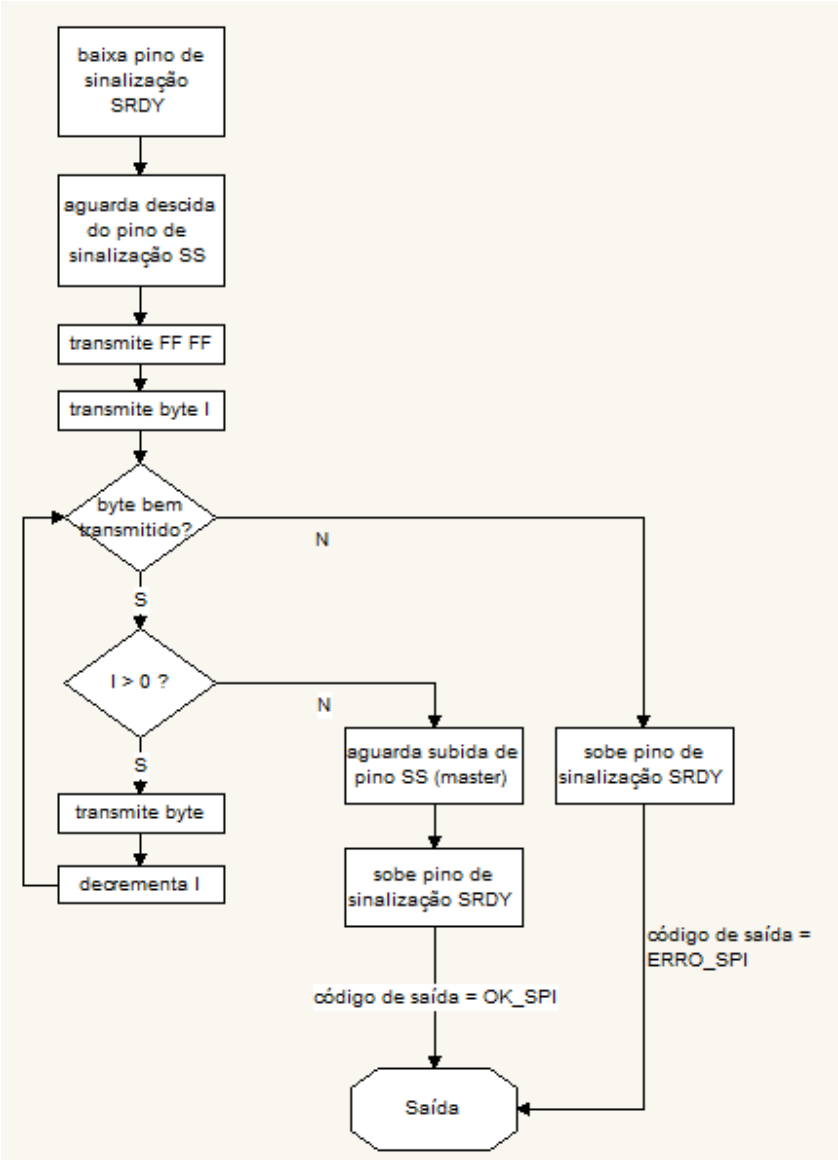
9.1.1. Fluxogramas



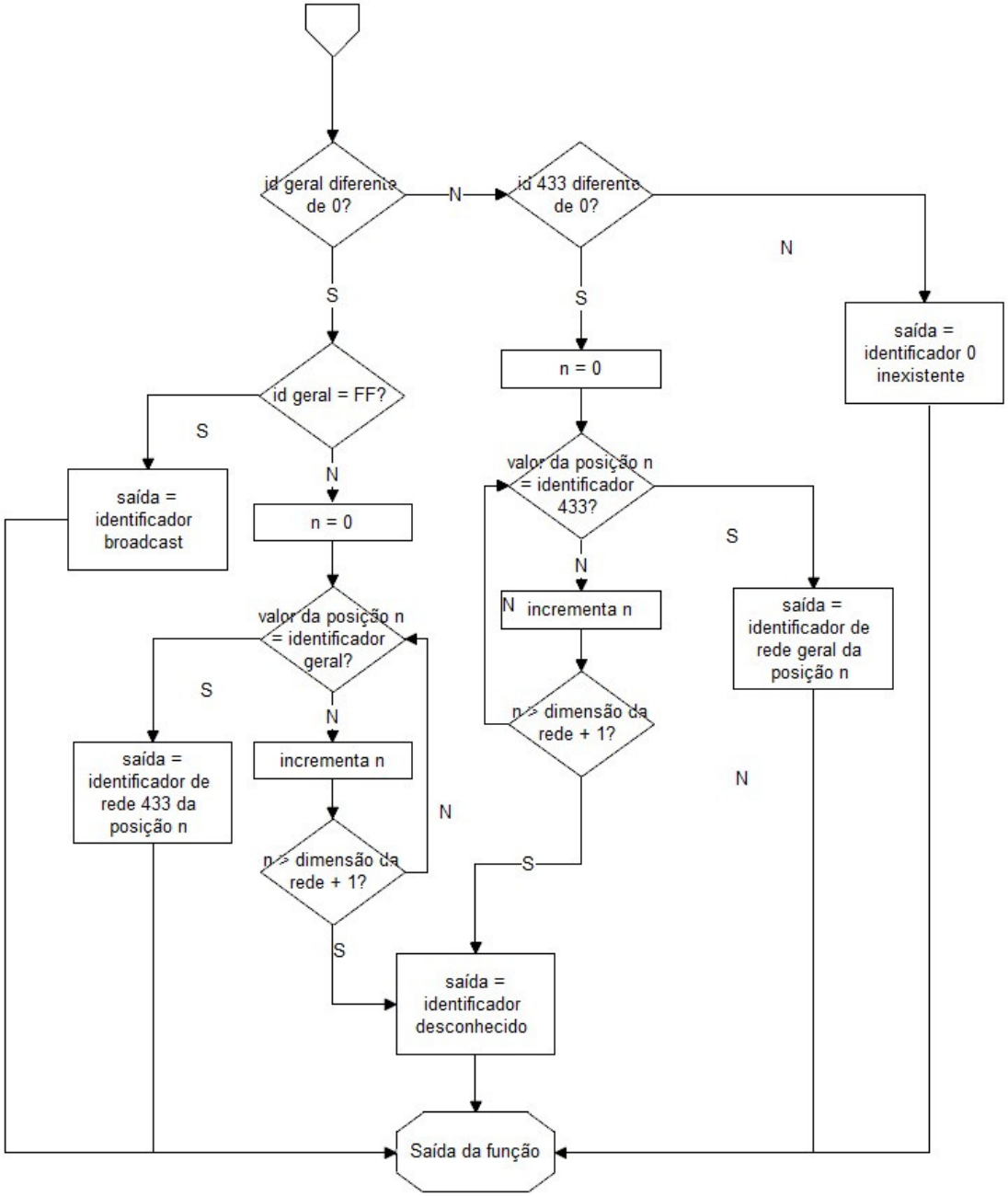
Fluxograma 1 - Representação da função envia_msg_uAp.



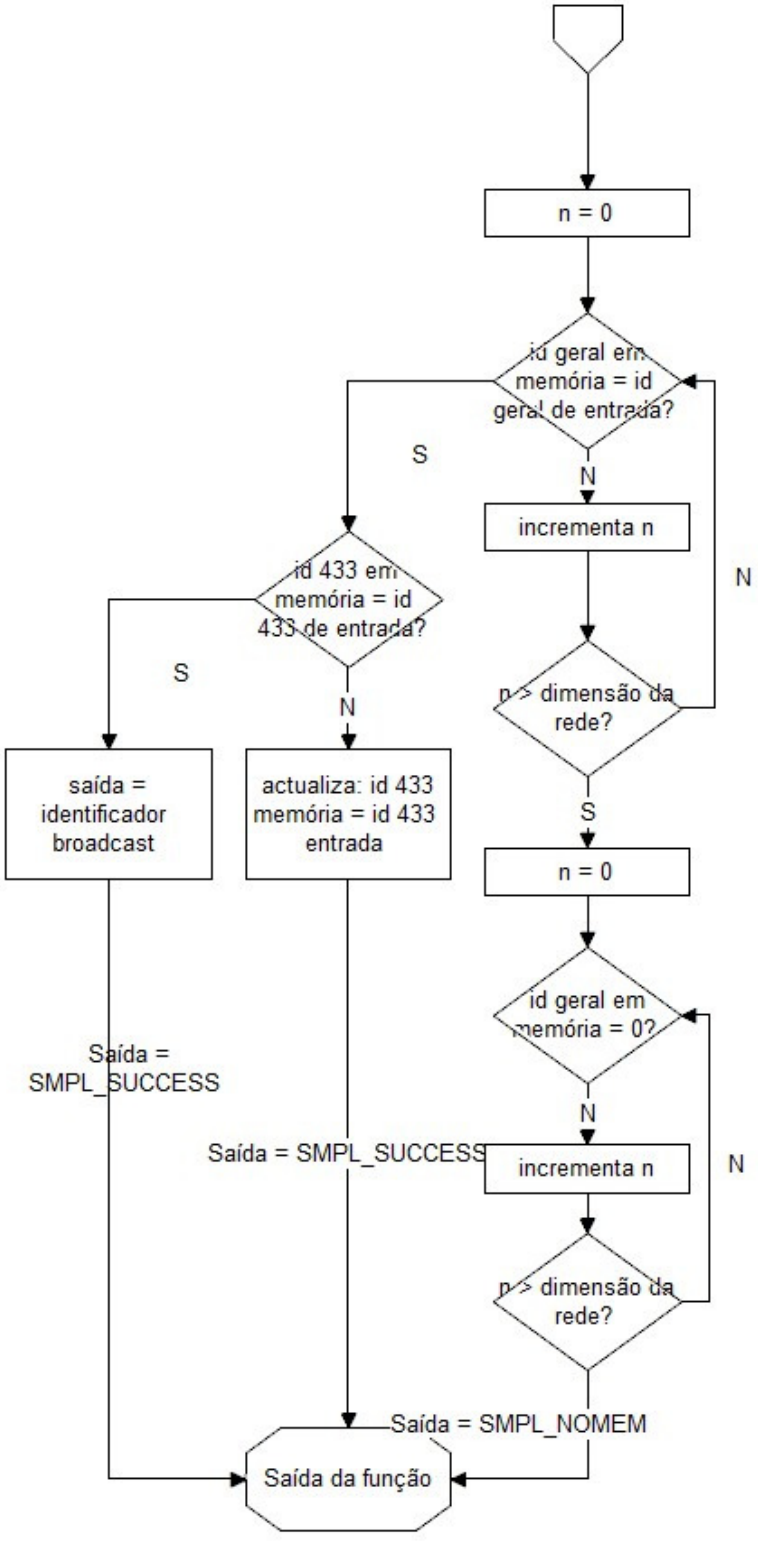
Fluxograma 2 - Processo de recepção de uma mensagem SPI - função recebe_msg_uAp.



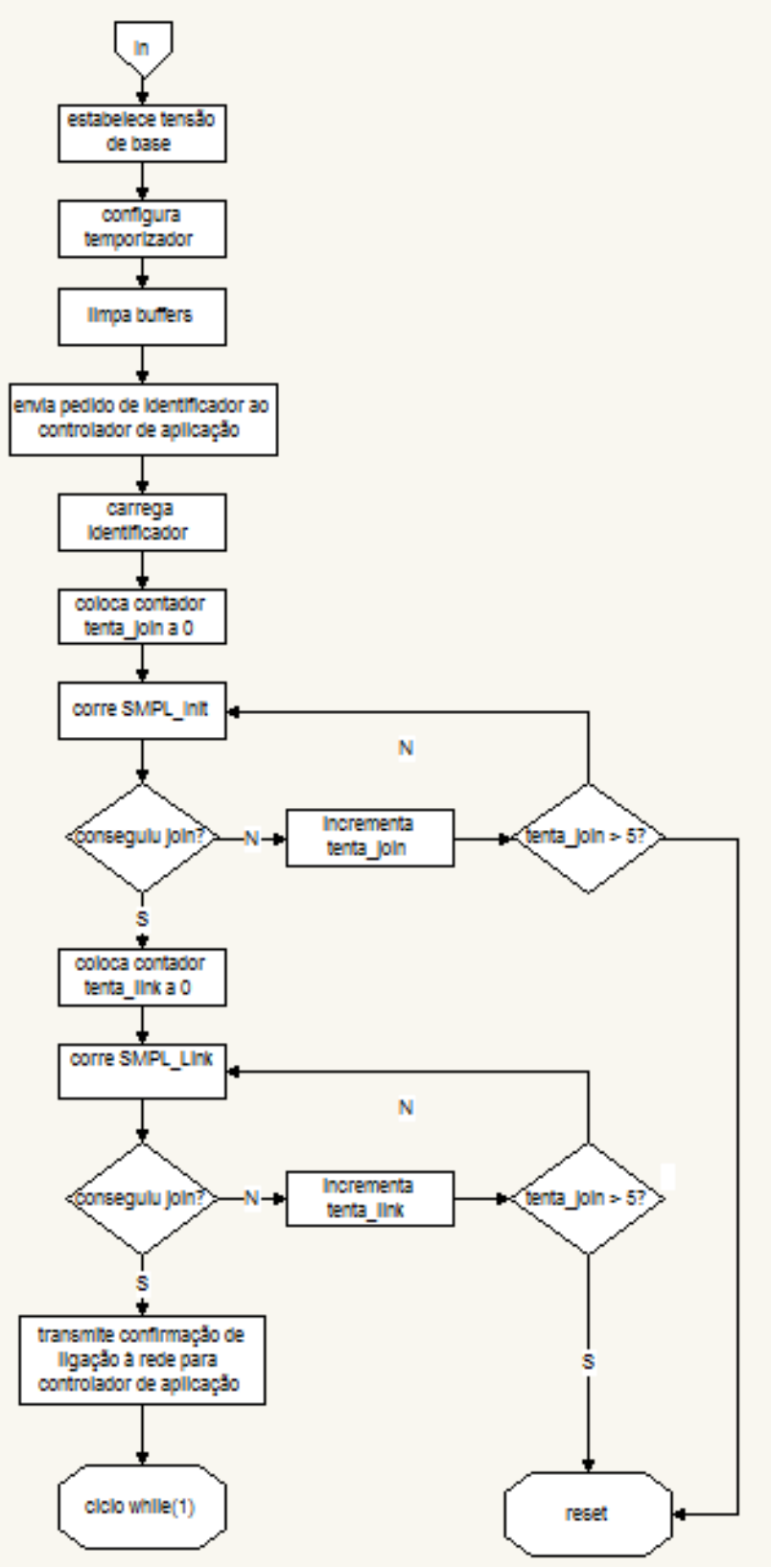
Fluxograma 3 - Processo da função envia_SREQ_uAp.



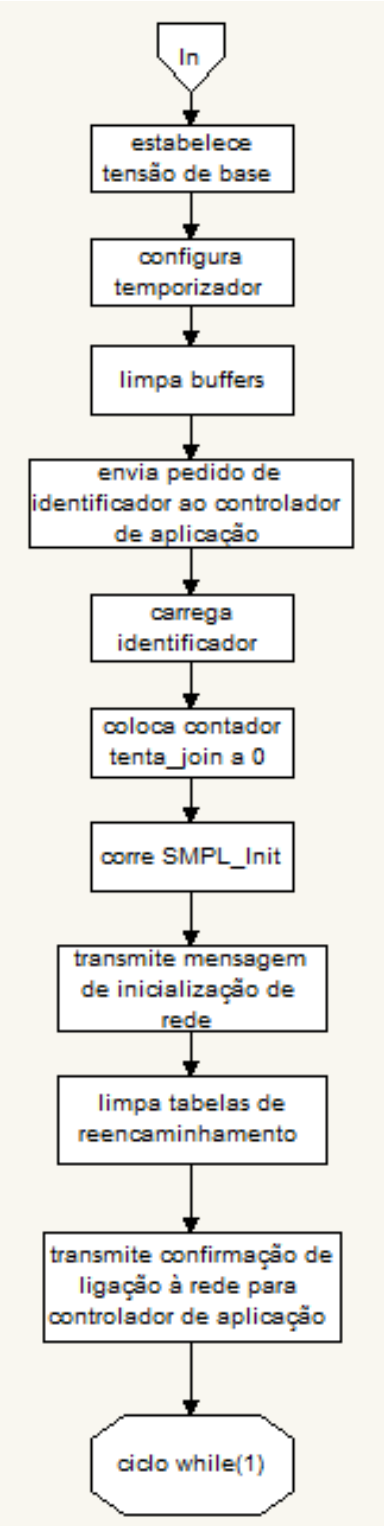
Fluxograma 4 - Processo da função *procura_GW*.



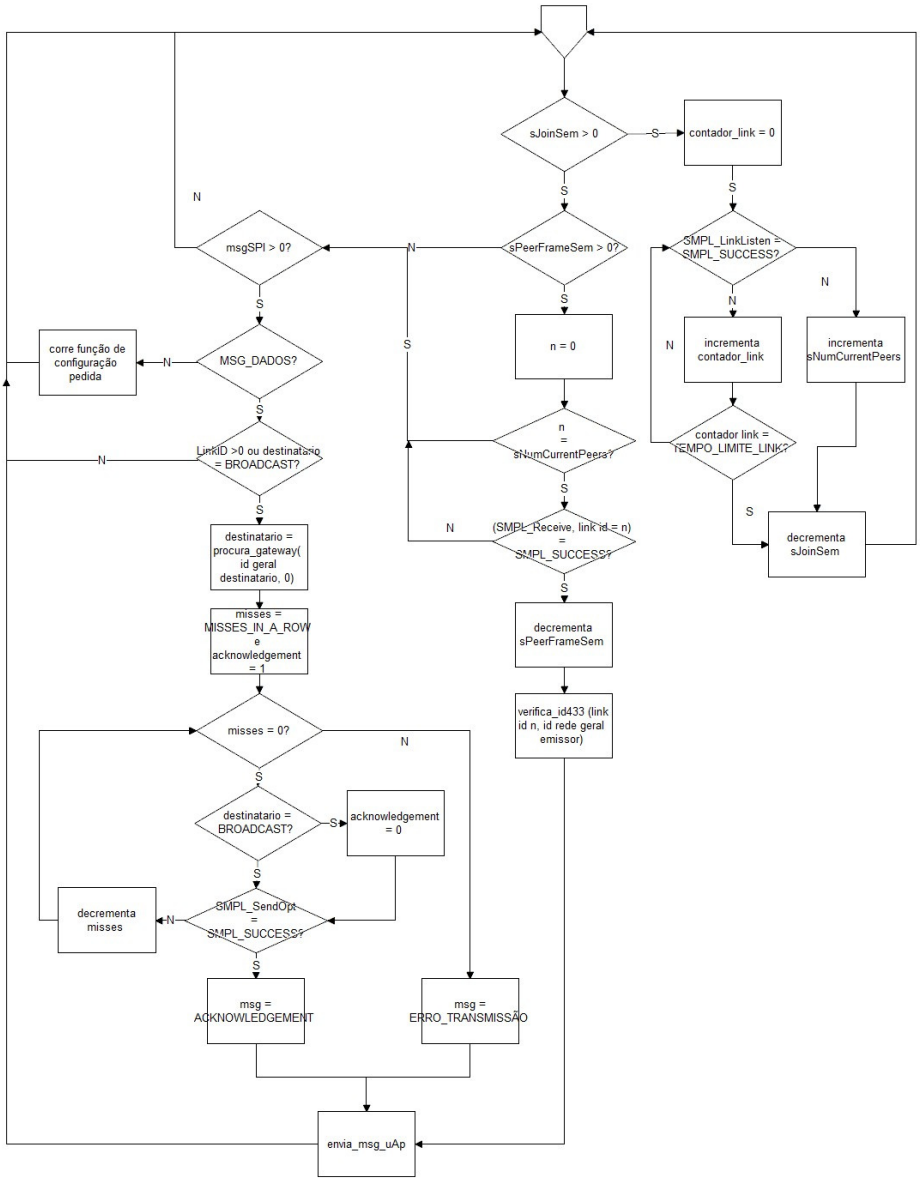
Fluxograma 5 - Processo da função *verifica_433*.



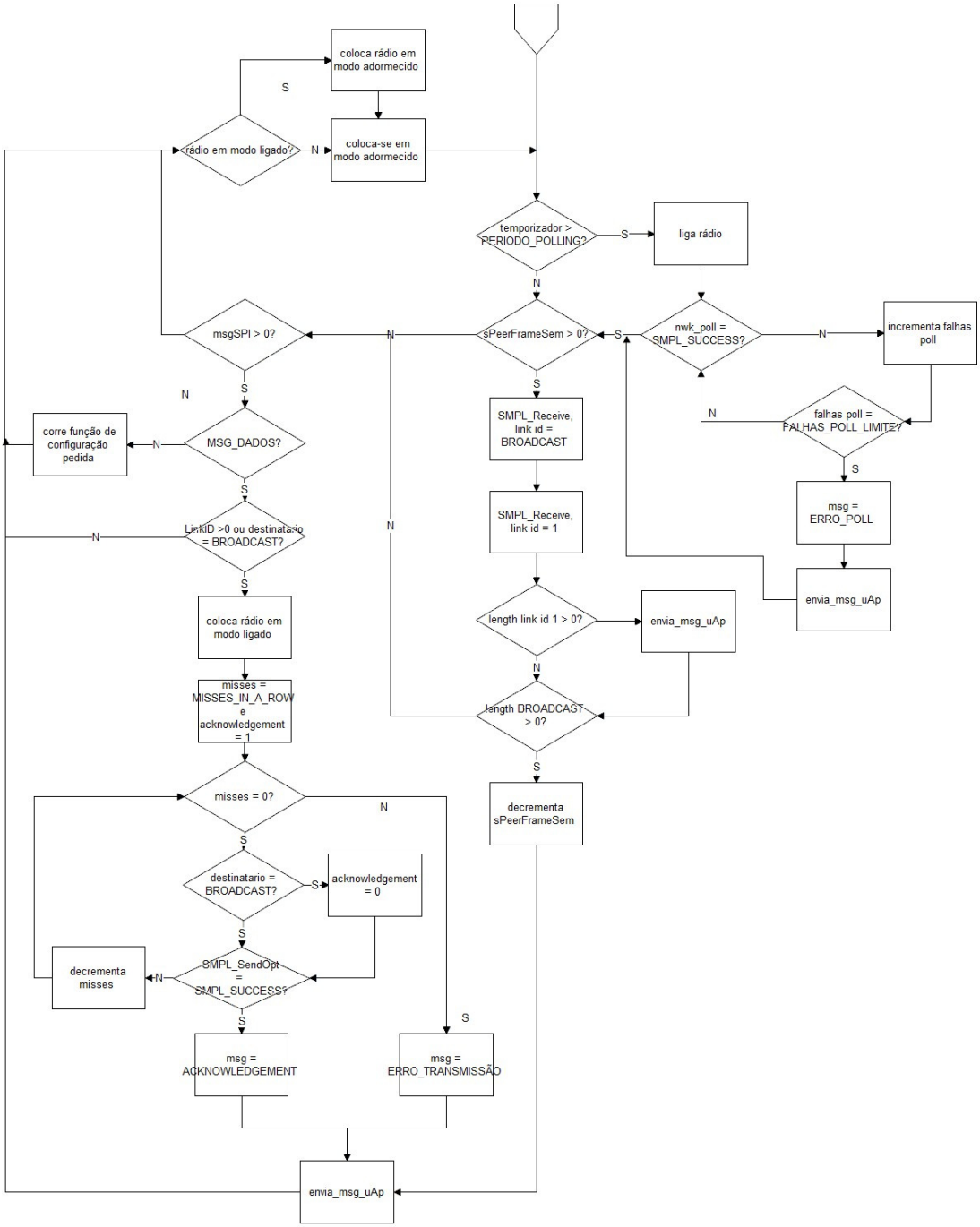
Fluxograma 6 - Processo de inicialização dos dispositivos *Router* e ED.



Fluxograma 7 - Processo de inicialização do dispositivo AP.



Fluxograma 8 - Código de controlo dos dispositivos AP e *Router*.



Fluxograma 9 - Código de controlo de um dispositivo ED.

9.1.2. Valores de configuração inicial

Tabela 48 - Valores de configuração inicial para o protocolo 433 MHz. Fonte: Texas Instruments.

Item	Default value	Description
MAX_HOPS	3	Maximum number of times a frame is resent before frame dropped. Each RE and the AP decrement the hop count and resend the frame.
MAX_HOPS_FROM_AP	1	Maximum distance and ED can be from the AP. Using this hop count significantly reduces the broadcast storm that can result from an ED poll if **MAX_HOPS** is used. Only for AP networks.
NUM_CONNECTIONS	4	Number of links supported as a result of both **SMPL_Link()** and **SMPL_LinkListen()** calls. Should be 0 if the device supports no ED objects (APs or REs).
MAX_APP_PAYLOAD	10	Maximum number of bytes in the application payload.
SIZE_INRAME_Q	2	Number of frames held in the Rx frame queue. Can be 0 for Tx-only devices, or for devices that never receive frames.
SIZE_OUTFRAME_Q	2	Number of frames held in the Tx frame queue. Some **NWK** applications keep Tx frames around to match replies.
DEFAULT_JOIN_TOKEN	0x01020304	Joining a network requires this value to match on all devices. It is sent in the Join message and matched in the receiving Access Point.
DEFAULT_LINK_TOKEN	0x05060708	Obtaining link access to a network device requires this value to match on all devices. It is sent in the Link message and matched in the receiving device.
THIS_DEVICE_ADDRESS	0x12345678	Each device address must be unique. The address assignment should lock out **0xnnnnnn00** and **0xnnnnnnFF** which are broadcast address for the CC1100/CC2500-class radios.
FREQUENCY_AGILITY	Not defined	When defined enabled support for Frequency Agility. Otherwise only the first entry in the channel table is used.
NVOBJECT_SUPPORT	Not defined	Support for saving and restoring connection context.
SMPL_SECURE	Not defined	Enables SimpliciTI security support.
APP_AUTO_ACK	Not defined	Support for application layer acknowledgment support.
EXTENDED_API	Not defined	Support for `SMPL_Ping()`, `SMPL_Unlink()`, and `SMPL_Commission()`.
SW_TIMER	Not defined	If enabled uses software to implement delays.
Access Point Devices		
ACCESS_POINT	Defined	
NUM_STORE_AND_FWD_CLIENTS	10	Number polling End Devices supported by this Access Point
AP_IS_DATA_HUB	Not defined	If this macro is defined the AP will be notified through the callback each time a device joins. The AP should be running an application that listens for a link message on receipt of this notification. The ED joining must link immediately after it receives the Join reply.
Range Extender Devices		
RANGE_EXTENDER	Defined	
End Devices		
END_DEVICE	Defined	Defined unless it is a application hosted on a device tht is

Tabela 49 - Tipos de mensagem controlador de comunicações - controlador de aplicação.

Código	Valor	Descrição
MSG_CONFIGURACAO	1	Mensagem de configuração do controlador de comunicações por SPI
MSG_DADOS	2	Mensagem de dados trocada entre controlador de comunicações e controlador de aplicação por SPI

Tabela 50 - Funções correspondentes à mensagem de configuração.

Código	Valor	Descrição
LIGA_RADIO	1	Função de mensagem de configuração por SPI: colocar a unidade rádio em modo adormecido
DESLIGA_RADIO	2	Função de mensagem de configuração por SPI: colocar a unidade rádio em modo ligado
RESET	3	Função de mensagem de configuração por SPI: fazer *reset* a controlador de comunicações

Tabela 51 - Funções de auxílio a RTC.

Código	Valor	Descrição
SEGS_P_LIGACAO	1	Função de RTC – 1 segundo para comparação com ponteiro *tenta_join*
SEGS_P_NOVA_TENT_LIGACAO	2	Função de RTC – aguarda 2 segundos até tentar nova ligação à rede
MINUTO	60	Função de RTC – hora = 60 segundos
HORA	60	Função de RTC – hora = 60 minutos
PERIODO_POLL	2	Função de RTC – executa *poll* de 2 em 2 minutos

Tabela 52 - Parâmetros de controlo de *polling*.

Código	Valor	Descrição
FALHAS_POLL_LIMITE	2	Tentativas de *poll* até notificação
ERRO_POLL	1	Notificação de erro no *polling* à unidade pai

Tabela 53 - Códigos e parâmetros de controlo de SPI.

Código	Valor	Descrição
ERRO_SPI	1	Código de saída SPI – erro na comunicação
OK_SPI	2	Código de saída SPI – comunicação bem sucedida
TENTATIVAS_SPI	5	Parâmetro de controlo SPI – tentativas para transmitir uma mensagem correctamente
ESPERA_REP_SPI	5000	Parâmetro de controlo SPI – tempo de espera para nova tentativa

Tabela 54 - Parâmetros de funções de programa de controlo.

Código	Valor	Descrição
LIMITE_FALHAS_ACK	1	Parâmetro de controlo – limite para falhas de *acknowledgement* até notificar falha de comunicação ao controlador de aplicação
MISSES_IN_A_ROW	2	Parâmetro de controlo loop – limite para falhas de transmissão
LIMITE_FALHAS_LINK	5	Parâmetro de controlo – limite para tentar *link* com nova unidade pai

9.2. Aplicações

9.2.1. Memória *Flash*

9.2.1.1. Aplicações *ZigBee*

Tabela 55 - Valores do dispositivo TA3T-r2 (*End Device*) guardados em memória *flash*.

Código	Descrição
ID_Familia	Identificador da família de dispositivos dentro da gama de produtos
ID_Modelo	Identificador do modelo do produto, dentro da respectiva família
ID_MSB_serie	MSB do número de série
ID_LSB_serie	LSB do número de série
ID_indice_hardware	Versão *hardware*
ID_indice_software	Versão *software*
Standby	Identificador do estado do dispositivo
Eixos	Identificador dos eixos do sensor de aceleração a monitorizar

Tabela 56 - Valores do dispositivo G2G4 (Coordenador ou *Router*) guardados em memória *flash*.

Código	Descrição
ID_Familia	Identificador da família de dispositivos dentro da gama de produtos
ID_Modelo	Identificador do modelo do produto, dentro da respectiva família
ID_MSB_serie	MSB do número de série
ID_LSB_serie	LSB do número de série
ID_indice_hardware	Versão *hardware*
ID_indice_software	Versão *software*

`

9.2.1.2. Aplicações Protocolo 433MHz

Tabela 57 - Valores do dispositivo TA3T-r4 (*End Device*) guardados em memória *flash*.

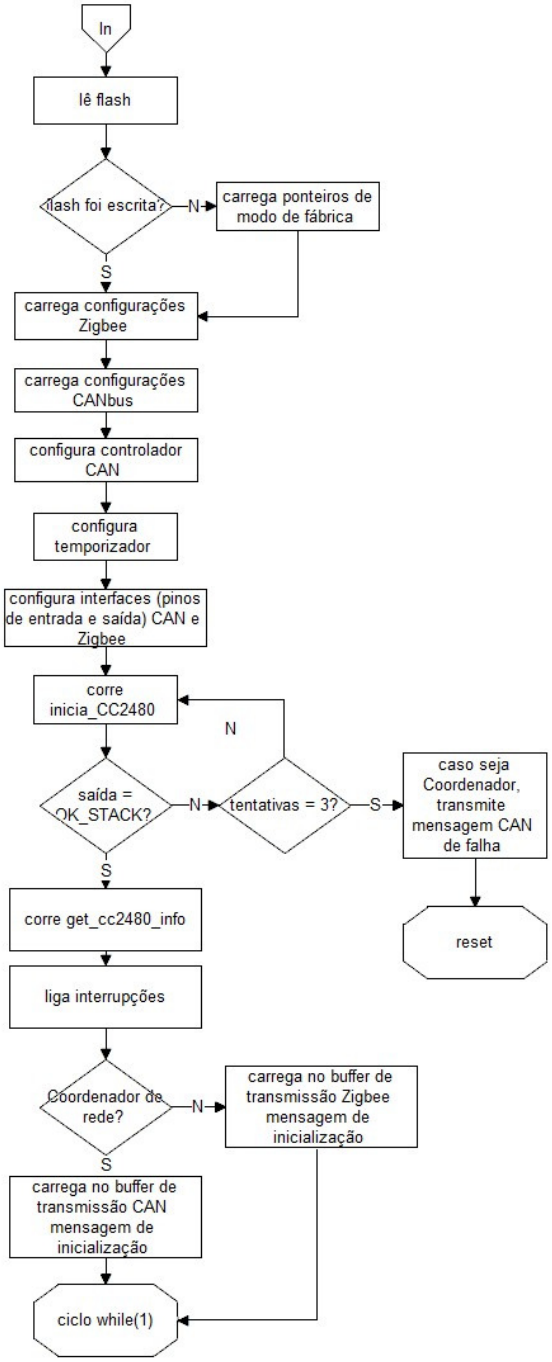
Código	Descrição
ID_Familia	Identificador da família de dispositivos dentro da gama de produtos
ID_Modelo	Identificador do modelo do produto, dentro da respectiva família
ID_MSB_serie	MSB do número de série
ID_LSB_serie	LSB do número de série
ID_indice_hardware	Versão *hardware*
ID_indice_software	Versão *software*
Standby	Identificador do estado do dispositivo
Eixos	Identificador dos eixos do sensor de aceleração a monitorizar

Tabela 58 - Valores do dispositivo G433M (AP ou *Router*) guardados em memória *flash*.

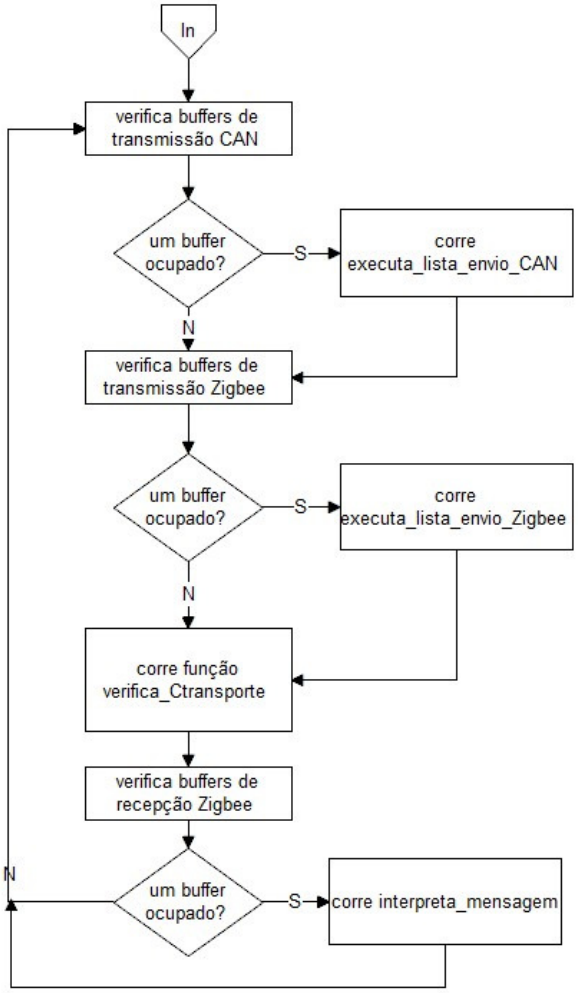
Código	Descrição
ID_Familia	Identificador da família de dispositivos dentro da gama de produtos
ID_Modelo	Identificador do modelo do produto, dentro da respectiva família
ID_MSB_serie	MSB do número de série
ID_LSB_serie	LSB do número de série
ID_indice_hardware	Versão *hardware*
ID_indice_software	Versão *software*

9.2.2. Aplicações sobre protocolo *ZigBee*

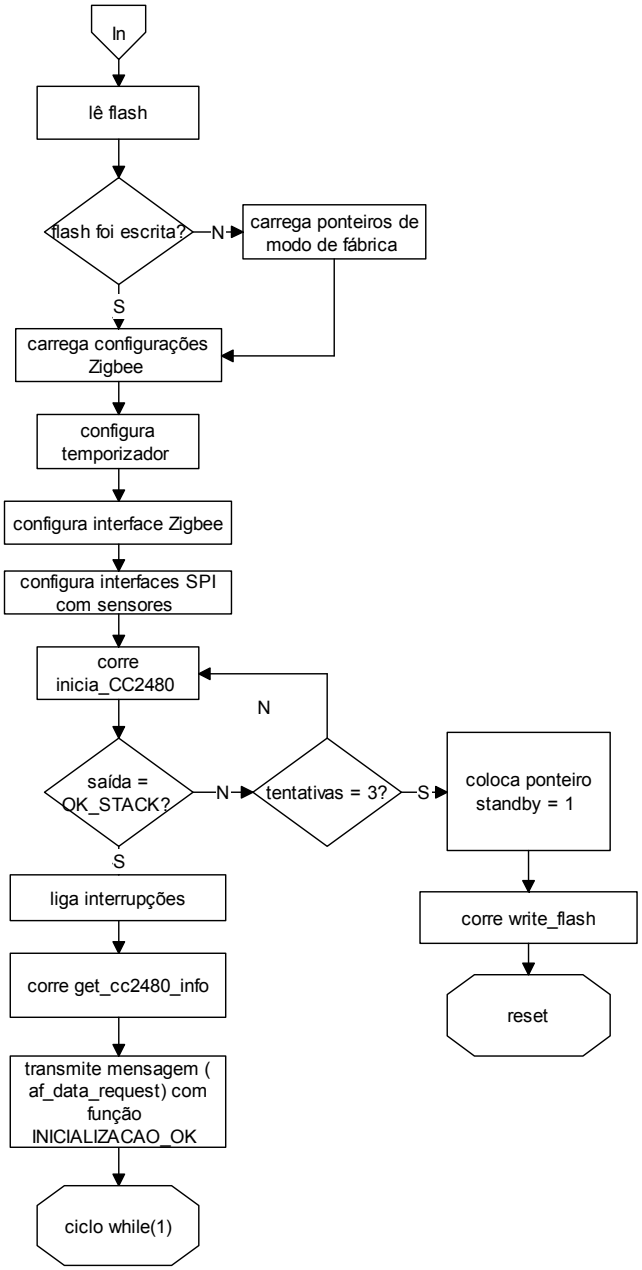
9.2.2.1. Fluxogramas



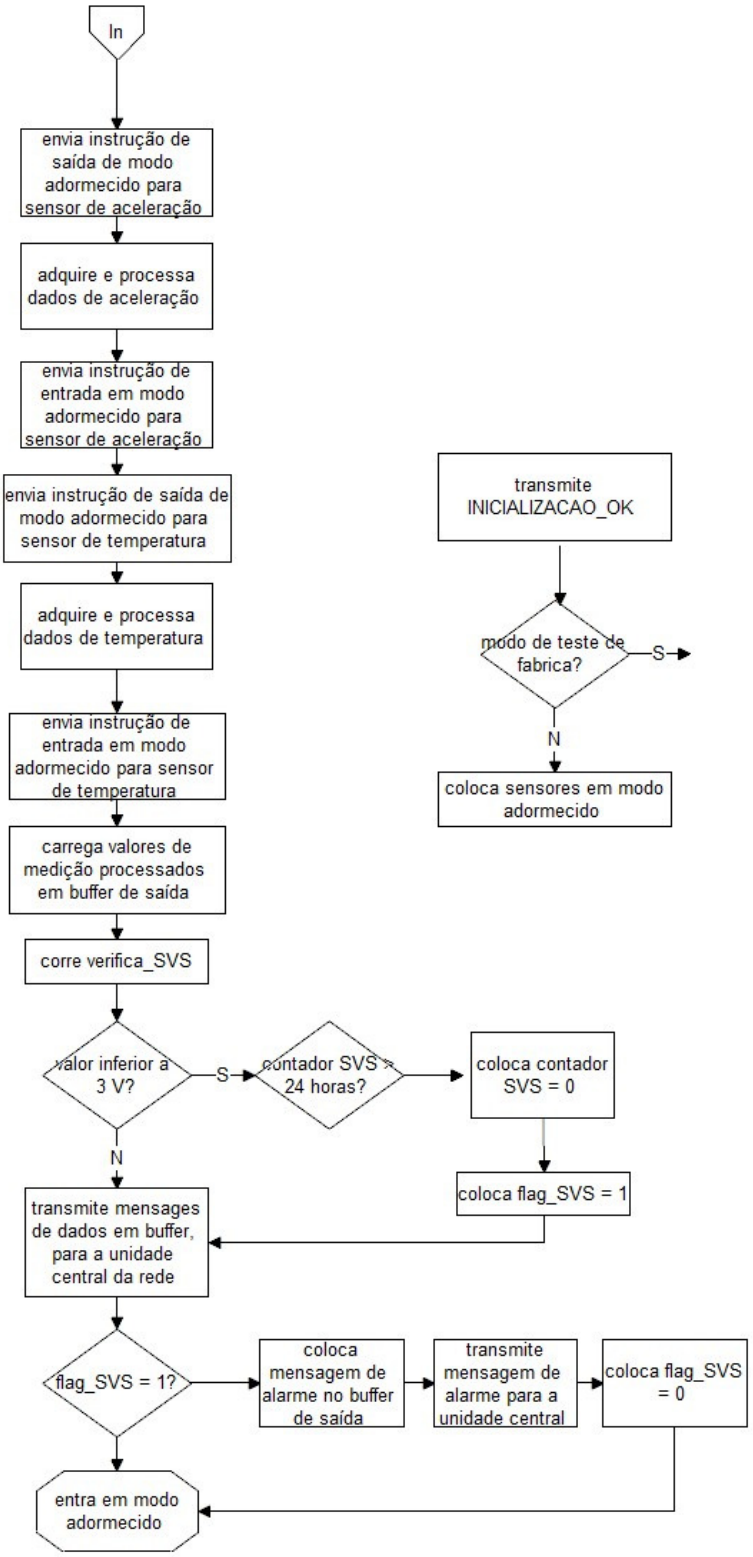
Fluxograma 10 - Processo de inicialização de um controlador de aplicação de uma *gateway ZigBee* – Coordenador ou *Router*.



Fluxograma 11 - Programa de controlo do controlador de aplicação *ZigBee* – Coordenador ou *Router*.



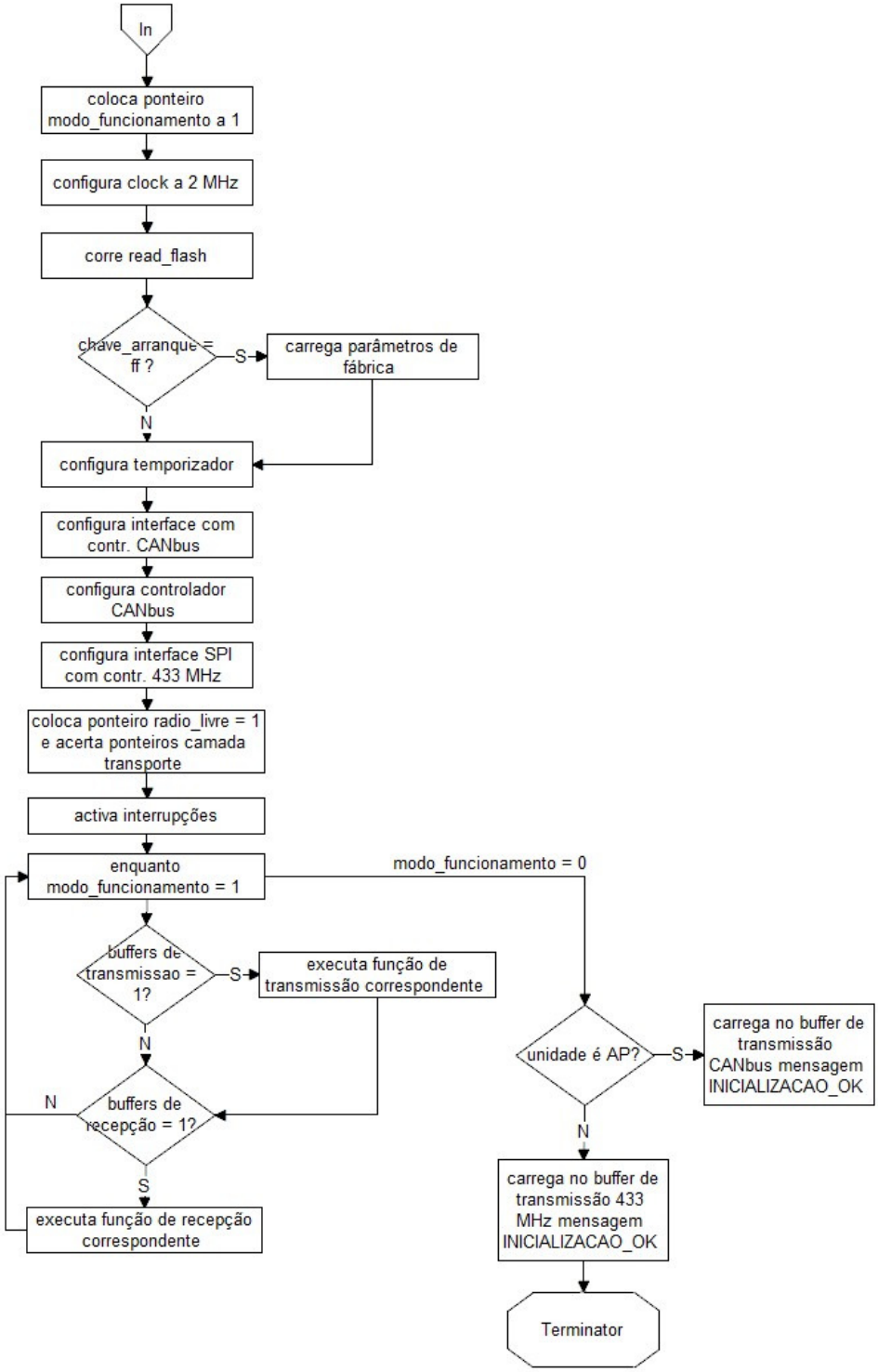
Fluxograma 12 - Processo de inicialização de um controlador de aplicação de um sensor inteligente *ZigBee – End Device.*



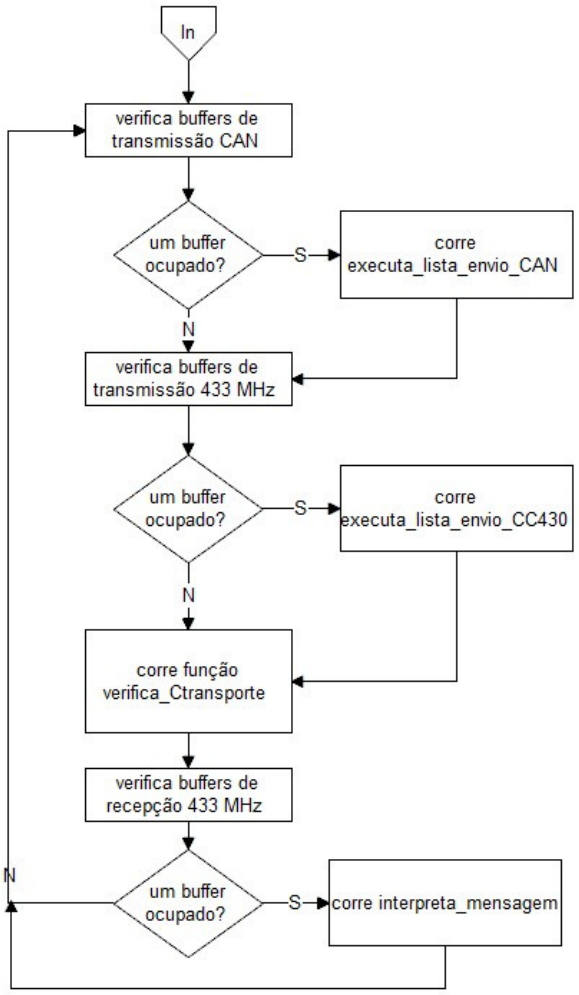
Fluxograma 13 - Programa de controlo do controlador de aplicação *ZigBee - End Device*.

9.2.3.Aplicações sobre protocolo 433 MHz

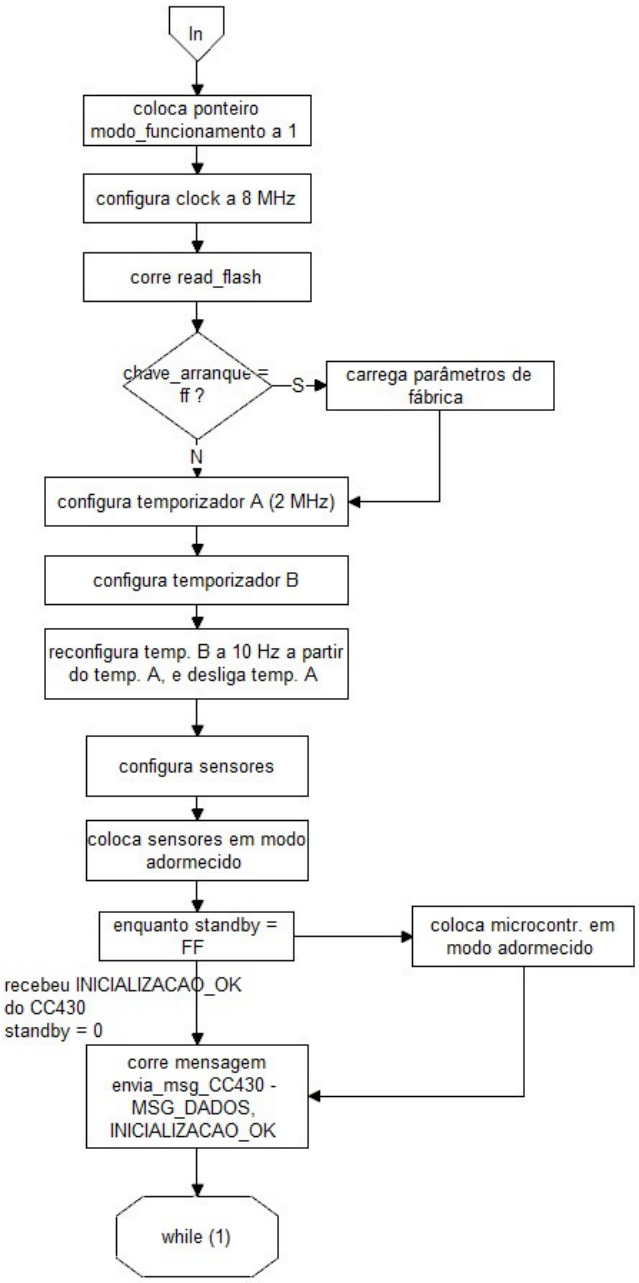
9.2.3.1. Fluxogramas



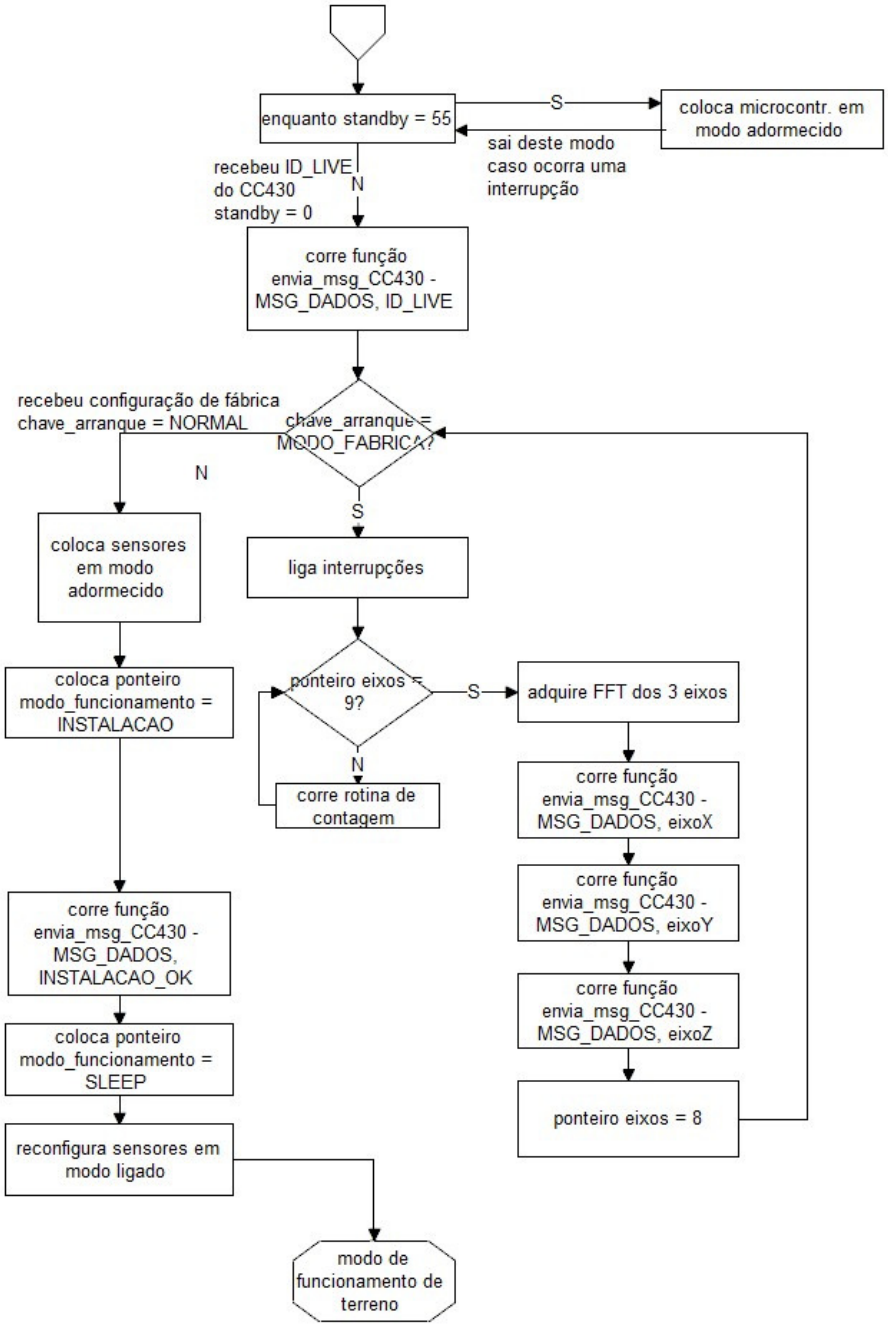
Fluxograma 14 - Programa de inicialização do controlador de aplicação da *gateway* 433 MHz.



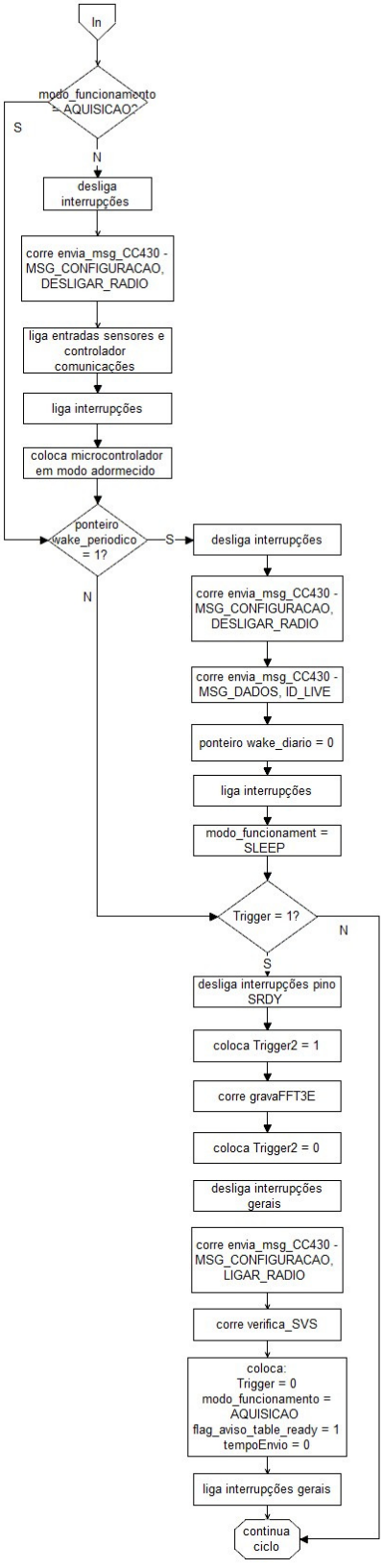
Fluxograma 15 - Programa de controlo do controlador de aplicação 433 MHz – Coordenador ou *Router*.



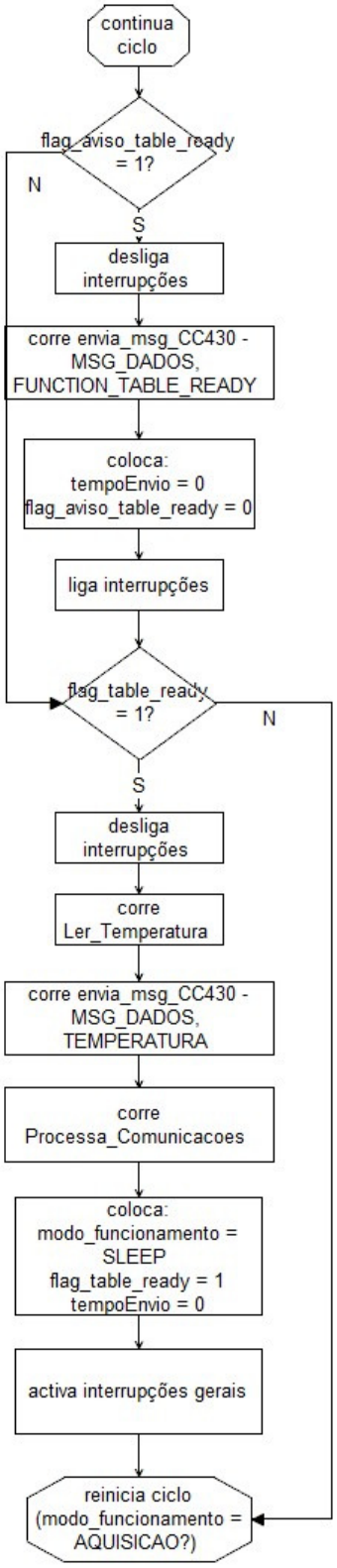
Fluxograma 16 - Programa de inicialização do controlador de aplicação do sensor sem fios (de aceleração e temperatura) 433 MHz.



Fluxograma 17 - Programa de inicialização/configuração do controlador de aplicação do sensor sem fios (de aceleração e temperatura) 433 MHz.



Fluxograma 18 - Programa de controlo do controlador de aplicação de um sensor inteligente (aceleração e temperatura) 433 MHz – *End Device* – parte 1.



Fluxograma 19 - Programa de controlo do controlador de aplicação de um sensor inteligente (aceleração e temperatura) 433 MHz – *End Device* – parte 2.

10. Anexo II

10.1. Circuitos Esquemáticos

10.1.1. Para plataforma *ZigBee*

10.1.1.1. Esquemáticos

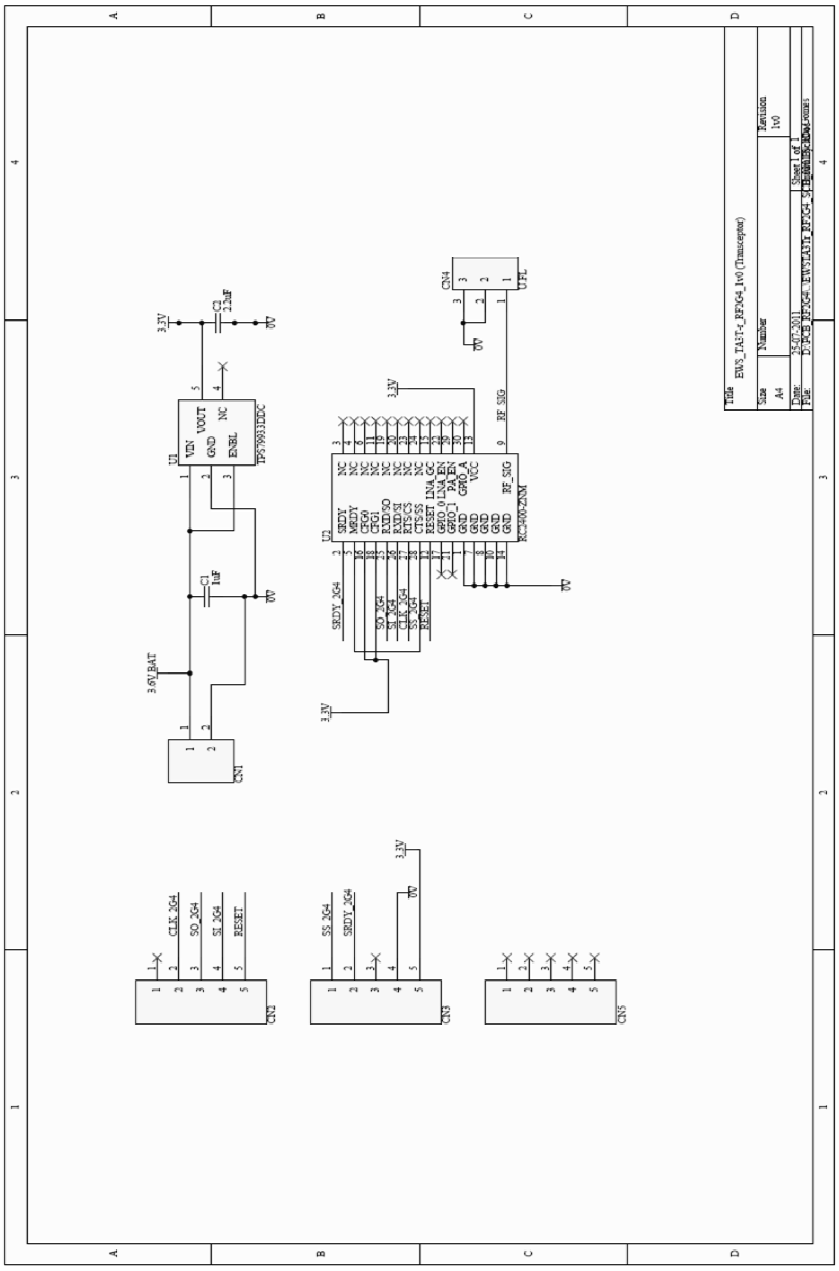


Figura 148 - Esquemático da placa *RFZigBee*.

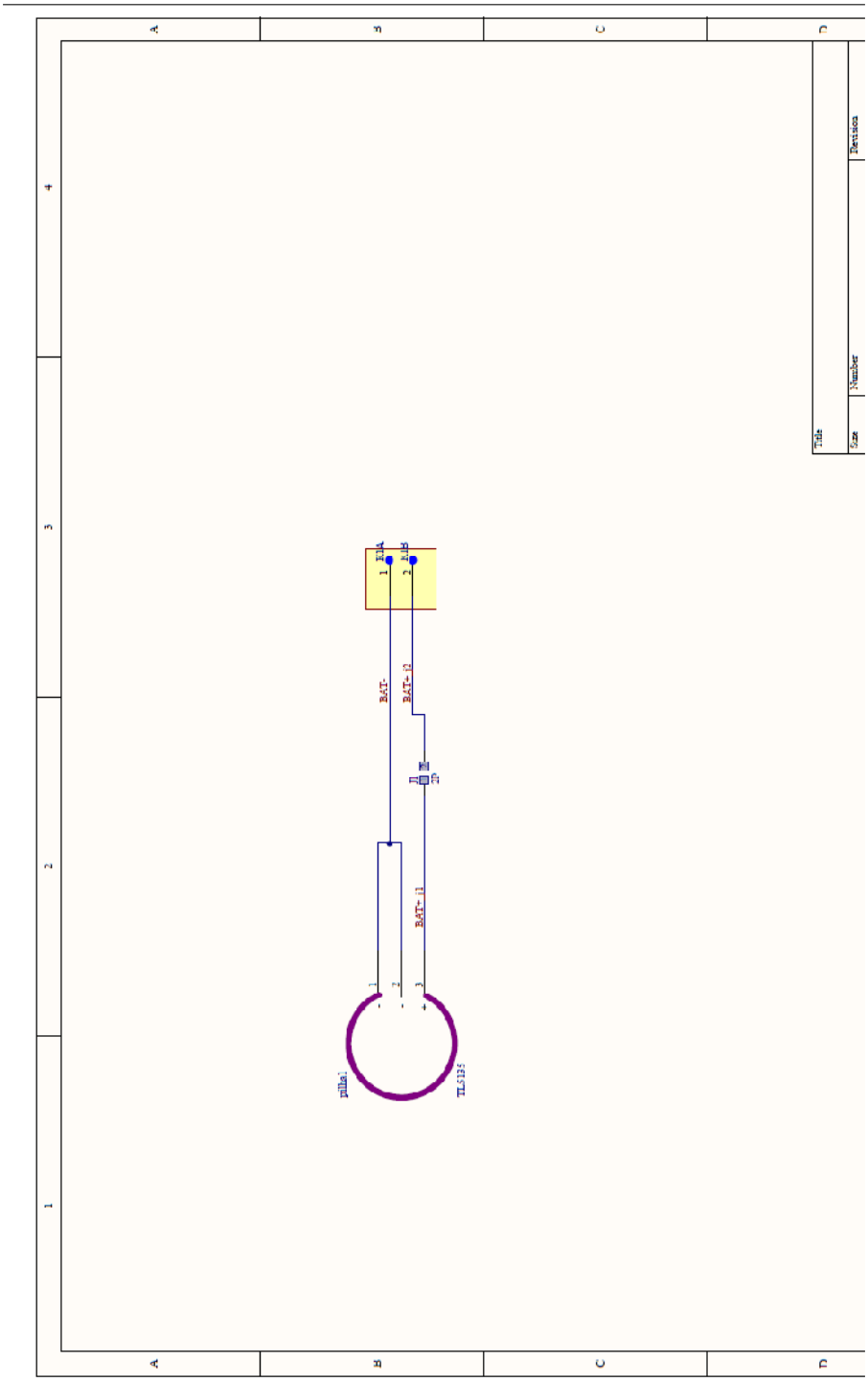


Figura 149 - Placa de circuito impresso Bat.

10.1.2. Para plataforma 433 MHz

10.1.2.1. Esquemáticos

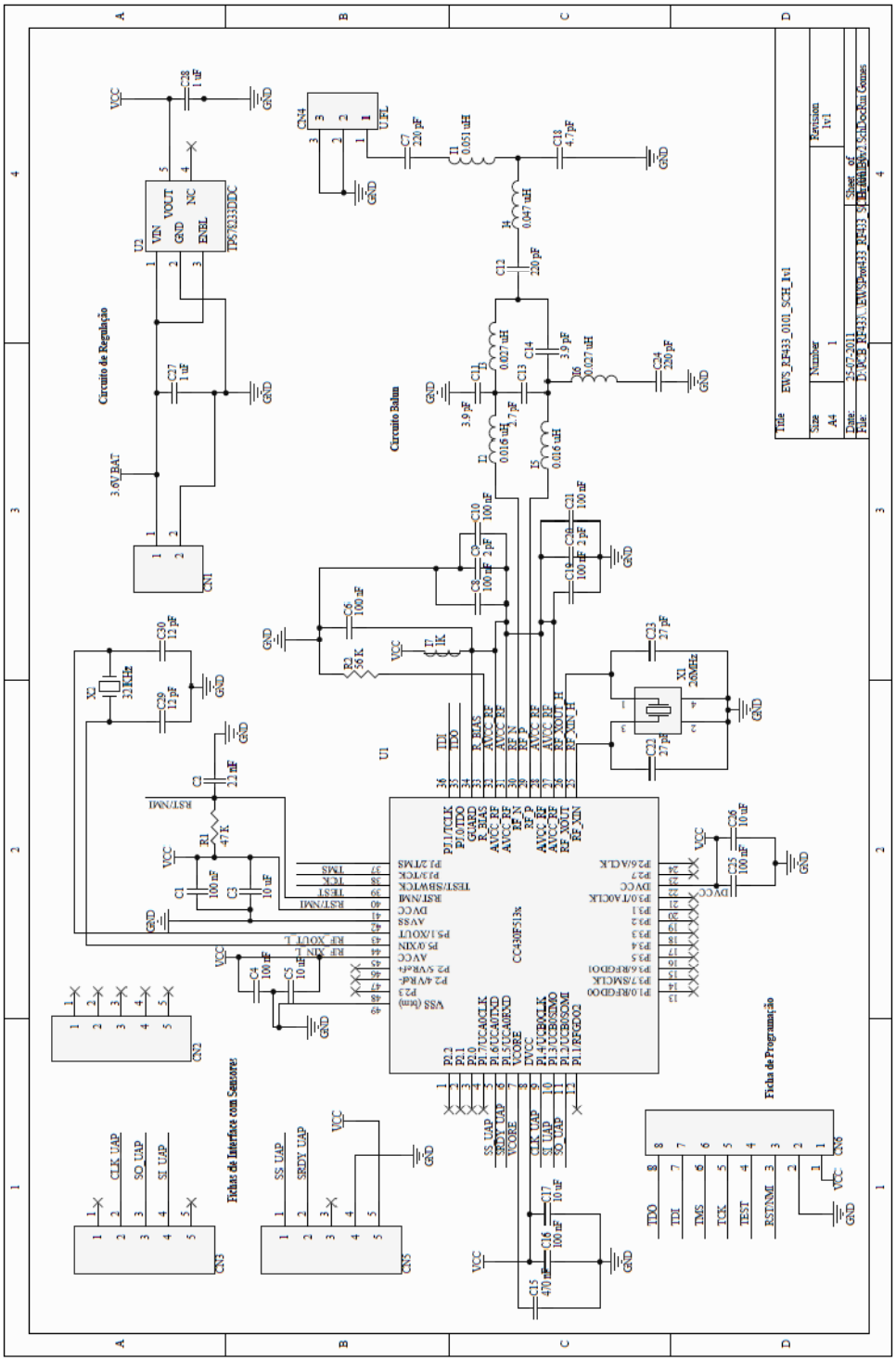


Figura 150 - Esquemático da placa de circuito impresso RF433.

10.1.2.2. Componentes

Tabela 59 - Componentes constituintes da placa RF433.

Descrição	Fabricante	Referência	Qtd.
Header8P	MOLEX	53047-0810	**1**
HEADER, VERTICAL, 1ROW, 5WAY	HARWIN	M52-040023V0545	**3**
Fio vermelho 150 mm	MOLEX	06-66-0012	**1**
Receptacle Housing 2 Way	MOLEX	51021-0200	**1**
Ficha Antena	HIROSE	U.FL-R-SMT-1(10)	**1**
TPS78233DDC	TEXAS INSTRUMENTS	TPS78233DDCT	**1**
CC430F513x	TEXAS INSTRUMENTS	CC430F5135IRGZT	**1**
Cristal 26 MHz	AVX	CX3225SB26000D0FLJZZ	**1**
Cristal 32 KHz	ABRACON	ABS07-32.768KHZ-T	**1**
COND. 100nF	PHYCOMP (YAGEO)	CC0603MRY5V9BB104	**9**
COND. 10uF/10V	TDK	C1608X5R1A106K	**4**
Cond. 2 pF	JOHANSON TECHNOLOGY	251R14S2R0BV4T	**2**
Cond. 470 nF	MURATA	GRM155F51A474ZE01D	**1**
COND. 2.2nF	AVX	06035C222KAT2A	**1**
COND. 27pF	MULTICOMP	MCCA000197	**2**
Resist. 56K	VISHAY DRALORIC	CRCW040256K0FKEAHP	**1**
Resist. 47K	PHYCOMP (YAGEO)	RC0603JR-0747KL	**1**
Bobina 16 nH	TYCO ELECTRONICS	36501E16NJTDG	**2**
Bobina 27 nH	TAIYO YUDEN	HK100527NJ-T	**2**
Bobina 47 nH	TYCO ELECTRONICS	MCFT000034	**1**
Bobina 51 nH	WUERTH ELEKTRONIK	744765151A	**1**
Ferrite 1K	MURATA	BLM15BD102SN1D	**1**
Cond 12 pF	MULTICOMP	MCCA000193	**2**
Cond. 2.7 pF	JOHANSON TECHNOLOGY	500R07S2R7BV4T	**1**
Cond. 220 pF balun	TAIYO YUDEN	UMK105CG221JV-F	**2**
Cond. 220 pF	KEMET	C0603Y221K5RACTU	**1**
Cond. 3.9 pF	JOHANSON TECHNOLOGY	500R07S3R9BV4T	**2**
Cond. 4.7 pF	MURATA	GRM1555C1H4R7CZ01D	**1**
Cond. 1uF	KEMET	C0402C105K9PACTU	**2**

11. Anexo III

11.1. Imagens de dispositivos instalados na subestação eléctrica do Alto de S. João

Figura 151 - Sensor de corrente EWS TIST-c instalado no transformador de alta-média tensão.

Figura 152 - Sensor de vibração e temperatura EWS TA3T-c instalado na carcaça do transformador de alta-média tensão.

Figura 153 - *Router* 433 MHz associado a um dos transformadores de AT-MT.

Figura 154 - Transformadores de alta-média tensão.

Figura 155 - Sensor de vibrações e temperatura 433 MHz instalado sobre o disjuntor de alta tensão.

Figura 156 - Unidade Coordenador EWS G433 M2, instalada numa lateral de uma torre, a cerca de 4 m do chão.

Artigos Publicados

Gomes, R., Oliveira, J., Cardoso, F. "*Integrating ZigBee and CAN Networks in Industrial Applications*". Em: *6th IEEE International Conference on Distributed Computing in Sensor Systems Workshops* (DCOSSW), IEEE, 2010

Gomes, R., Oliveira, J., Cardoso, F., Faria, S., Falcão, P. "*A hybrid sensor network for the real-time condition monitoring of rotating machinery*". Em: *6th IEEE International Conference on Distributed Computing in Sensor Systems Workshops* (DCOSSW), IEEE, 2010

Gomes, R., Oliveira, J., Cardoso, F., Faria, S., Falcão, P., Silva, A. "Redes de Energia Eléctrica Inteligentes: Gestão de Activos em subestações, com redes de sensores". Em: Congresso Luso-Moçambicano de Engenharia 2011 (CLME 2011), 2011