Universidade de Aveiro Departamento de Eletrónica, Telecomunicações e Informática
2018

André David Távora Perdigão

Infraestrutura de Comunicações e Serviços para IoT em ambientes Urbanos

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Eletrónica e Telecomunicações, realizada sob a orientação científica do Doutor Rui Aguiar, Professor Catedrático do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro

o júri

presidente	**Prof. Doutor Mário José Neves de Lima** Professor Auxiliar da Universidade de Aveiro
Vogal Arguente principal	**Doutor(a) Rui Lopes Campos** Investigador do Instituto de Engenharia de Sistemas e Computadores do Porto
Vogal Orientador	**Prof. Doutor Rui Luís Andrade Aguiar** Professor Catedrático da Universidade de Aveiro

agradecimentos

Para começar gostaria de agradecer Prof. Doutor Rui Aguiar, pois, sem ele não conseguiria fazer este trabalho.
Também gostaria de deixar o agradecimento aos vários investigadores, técnicos e professores, que me ajudaram várias vezes durante a execução do trabalho.
Aos meus pais pela ajuda prestada no trabalho.
Aos meus familiares e amigos, por me apoiarem e me fornecerem meios para a execução deste trabalho.
E claro, a todos os investigadores e técnicos que disponibilizaram os documentos e os fóruns de apoio que me ajudaram na realização deste trabalho.

palavras-chave **Laboratório vivo, IoT, watchdog, Wi-Fi, IEEE 802.11p, redes veiculares, redes de sensores**

resumo

Nos últimos anos têm sido criticados os testes das tecnologias apenas em simuladores, por não terem em conta as condicionantes da realidade e suas influências para os utilizadores em ambiente real.

Tais críticas têm levado à realização de testes em ambientes reais, tendo, contudo, um efeito agravante que é a exigência de uma infraestrutura grande e cara, o que torna mais difícil aos investigadores e desenvolvedores o acesso às mesmas.

Por vários motivos, incluindo os custos de desenvolvimento em ambientes reais, tem existido um aumento da diferença entre a tecnologia desenvolvida no momento e a tecnologia disponibilizada para o público em geral, o que gerou um crescente interesse em criar laboratórios em condições reais pelo mundo inteiro, chamados laboratórios vivos.

Estes laboratórios têm por objetivo disponibilizar as tecnologias em desenvolvimento, fornecendo o acesso aos investigadores interessados, assim permitindo que sejam feitos testes e demonstrações nestas plataformas, obtendo resultados realísticos. Tal poderá acelerar a finalização destas tecnologias, ajudando a reduzir a diferença entre as tecnologias disponíveis e as tecnologias a serem desenvolvidas no momento.

Este trabalho apresenta contribuições para o projeto PASMO, que vai fornecer uma plataforma que disponibiliza tecnologias recentes para testes e desenvolvimento.

As contribuições apresentadas neste trabalho para a plataforma estão divididas em três partes, que são: *planeamento*, *eletrónica* e *controlo de rede*.

A parte de *planeamento* consiste em decidir a localização dos equipamentos da plataforma, mas, como a plataforma tem de funcionar em diversas condições temporais, foi necessário a execução de vários testes que servem para verificar os limites das várias tecnologias escolhidas, de forma a garantir o bom funcionamento da plataforma mesmo em condições adversas.

Assim sendo, neste trabalho foram feitos testes de LoRa e Wi-Fi, em que se obteve um alcance superior a 500 metros para o Wi-Fi, e um alcance de 100 metros para os sensores de estacionamento de LoRa testados.

Com base nos resultados obtidos foram selecionadas algumas opções de localização dos dispositivos.

A parte de *eletrónica* resume-se na criação de um sistema heartbeat, que controla se o equipamento da plataforma está a funcionar normalmente, e caso exista algum problema pode remover temporariamente a energia ao equipamento da plataforma de forma a obrigar a um reiniciar. Esse sistema, tem um circuito para controlar a energia fornecida aos equipamentos da plataforma, e além disso, o sistema heartbeat tem um dispositivo de processamento, que monitoriza um desses equipamentos e controla o circuito.

Verificou-se que com a solução desenvolvida se consegue monitorizar um Access Point.

Na parte *controlo de rede* foi feito um programa que consegue comunicar com cada um dos sistemas heartbeat, que consegue controlar cada um deles sem a necessidade da deslocação ao local do equipamento.

keywords **Living Lab, IoT, watchdog, Wi-Fi, IEEE 802.11p, Vehicular network, sensor network, VANET**

abstract

In recent years, it has been criticized to only test technologies at simulators, before being applied for everyone to use.

Due to these critics, it is now necessary to test all technologies in real environment. However, some technologies require a large and expensive infrastructure, making it difficult for researchers to access.

For some reasons, including the reasons above, there has been an increasing difference between the technologies used and the technologies in development. This generates a growing interest in creation of open living labs around the world.

These laboratories are made to provide recent technologies, giving access to researchers interested in its development. Allowing test and demonstrations at these platforms for realistic results. This will help in finalizing the technologies, which will reduce the gap between available technologies and the technologies in development at the moment.

This thesis presents some contributions made for the PASMO project, which will provide a platform where will be possible to test and develop some recent technologies.

These contributions can be divided in three different parts: planning, electronic e network control.

In the planning part it was discussed where the equipment will be deployed. To select the locations, it was necessary to tests the technologies used under different climatic conditions. These tests were made to know the limits of the technologies used, in order to guarantee that the platform works in adverse conditions. The tests were made on Wi-Fi and LoRa, and analysing the results obtained we concluded that the range of Wi-Fi is more than 500 meters and the range of LoRa parking sensors is 100 meters. Based on these results, some options were selected to the places of equipment.

In the electronic part, it is the projection of a heartbeat system. This system will check if the platform equipment is operating normally. In case of problems, this system can temporarily remove the power of the equipment, to make a hard reset on the equipment. For this it was necessary to create a circuit to control the energy and a program to a microcontroller that will check the equipment and control the circuit. With the solution developed it was verified that an access point can be monitored.

For the network control part, a program has been made that can communicate with each heartbeat system. With this program, the user can control and monitor each heartbeat system without having to go to the location of the equipment.

Índice

Siglas e acrónimos

ACK – acknowledgment

AP – access point

BPSK – Binary Phase Shift Keying

BS – base station

BSS – Base Station Subsystem

BT – bandwidth-time

CCK – Complementary code keying

CRC – Cyclic Redundancy Check

CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

CTS – Clear to send

DBPSK – Differential Binary Phase Shift Keying

DCF – Distributed Coordination Function

DFT-s-OFDM – Discrete Fourier Transform Spread orthogonal frequency division multiplexing

DIFS – Distributed Interframe Space

DQPSK – Differential Quadrature Phase Shift Keying

DSSS – Direct sequence spread spectrum

ED – end device

FDD – frequency division duplex

IoT – Internet of Things

IP – Internet Protocol

IT – Instituto de Telecomunicações

LDPC – low-density parity check

LPWAN – low power wide area network

LTE – Long Term Evolution

M2M – machine to machine

MAC – media access control

MIMO – multiple input, multiple output

OBU – onboard unit

OFDM – orthogonal frequency division multiplexing

OFDMA – orthogonal frequency division multiple access

PCF – Point Coordination Function

QAM – Quadrature Amplitude Modulation

QPSK – Quadrature Phase Shift Keying

RSU – roadside unit

RTS – Request to send

SC-FDMA – Single Carrier Frequency Division Multiple Access

SIFS – Short Interframe Space

STBC – space-time block code

V2I/V2R – vehicle-to-infrastructure/vehicle-to-roadside unit

V2V – vehicle-to-vehicle

VANET – vehicular ad-hoc network

VPN – virtual private network

WAVE – wireless access in vehicular environments – Nota: WAVE do IEEE 802.11p é diferente do IEEE 802.11ac Wave1 e IEEE 802.11ac Wave2

WLAN – wireless local area network

1. Introdução

Nos últimos anos a aderência às tecnologias de comunicação e informação tem aumentado, devido à facilidade de acesso e à redução do seu preço. Além disso estas tecnologias oferecem grandes vantagens na sua utilização, como a facilidade de acesso à informação, a facilidade de comunicação a grandes distâncias e permitem executar múltiplas tarefas de maneira fácil, com maior rapidez e mais confortavelmente. Por estes e outros motivos, estas tecnologias passaram a ser uma parte crucial da vida de cada indivíduo.

Pelo facto das tecnologias de informação e comunicação serem uma parte cada vez mais importante da vida atual, os utilizadores também tendem a ser cada vez mais exigentes com a qualidade do serviço fornecido. Para corresponder às expectativas cada vez mais exigentes dos utilizadores é necessário um constante desenvolvimento das tecnologias. Também devido às crescentes exigências dos consumidores para com a tecnologia, são colocados em causa os testes das novas tecnologias apenas com emuladores e simuladores, questionando a autenticidade dos resultados dos mesmos.

Assim, seria desejável a realização dos testes das tecnologias em ambientes reais, antes de serem disponibilizadas para o público em geral. Contudo, tais testes, pela exigência de infraestruturas caras, tornam-se difíceis de realizar, como é o caso das tecnologias aplicadas em smartcities.

Para resolver o problema de acesso a estas tecnologias, os governos e algumas organizações internacionais estão a criar laboratórios vivos espalhados pelo mundo inteiro, passíveis de utilização coletiva. O objetivo destes laboratórios é colocar tecnologias recentemente projetadas em ambientes reais, de forma a investigadores e desenvolvedores terem acesso às mesmas, podendo testar e desenvolver soluções para serem utilizadas pelo público em geral.

Neste documento propõe-se relatar um trabalho enquadrado num esforço de disponibilizar algumas das tecnologias desenvolvidas nos últimos anos num espaço físico urbano, de tal forma que permite que qualquer teste executado sobre a plataforma a ser implementada obtenha resultados realistas. Ao disponibilizar esta plataforma, para além dos resultados mais realistas, também permite que qualquer interessado tenha acesso a estas tecnologias sem ter um grande investimento em infraestrutura, o que irá facilitar o desenvolvimento e implementação das mesmas.

Com esta plataforma será fornecido acesso a tecnologias recentes que apresentam grande interesse de ser implementados em ambiente urbano num futuro próximo. Disponibilizar a plataforma ao público ajudará a que se consiga finalizar o desenvolvimento das tecnologias. Além disso, como esta plataforma é implementada em ambiente urbano, irá aproximar os cidadãos destas tecnologias, o que facilitará a sua aceitação e ajudará na sua implementação em grande escala. Estas tecnologias são as que se pretendem implementar em smartcities, que é um dos assuntos recentes falado frequentemente. Contudo, as principais dificuldades no desenvolvimento de smartcities estão relacionadas com a falta de plataformas onde se possa experimentar e demonstrar as tecnologias necessárias para a sua criação.

Nesta plataforma pretende-se disponibilizar tecnologias de redes veiculares, de redes de sensores e de redes de WLAN, permitindo a qualquer pessoa que esteja interessada, possa desenvolver soluções para estas tecnologias.

1.1 Objetivos

Dentro deste contexto, o trabalho tem o objetivo de contribuir para o desenho e implementação de uma plataforma de redes de comunicação na Barra de Aveiro que terá as seguintes características:

- O protocolo IEEE 802.11p com RSUs que fará a cobertura da A25, desde o início da ponte da barra até á "Friopesca", o que abrange cerca de 5km de via.
- Implementar cobertura de Wi-Fi nas praias da Barra de Aveiro e Costa Nova.
- Colocar sensores de estacionamento na Av. Fernão de Magalhães – Barra
- Colocar sensores de medição atmosférica no porto e na praia da Barra.
- Fazer a cobertura de LoRa em toda a área da Barra.

O contributo para este projeto pode-se repartir-se em três partes:

- O planeamento, onde foram selecionados locais para os equipamentos que dependem do alcance utilizável.
- A eletrónica, em que foi desenvolvida uma solução para monitorizar constantemente se os equipamentos estão a funcionar devidamente.
- A rede de controlo onde foi criado um programa para que um utilizador consiga controlar todo o sistema de monitorização da plataforma.

No planeamento foram feitos estudos do alcance de um AP, para ver até que distância este tem uma boa cobertura e, qual é o alcance máximo de transmissão dos sensores de estacionamento, de forma a garantir o bom funcionamento à maioria das condições atmosféricas.

Nesses testes foi feito o estudo do alcance e da largura de banda do AP a várias condições temporais e, quanto afeta ter múltiplos dispositivos conectados ao mesmo AP. Em relação aos sensores de estacionamento, foi preciso verificar qual o alcance máximo da transmissão dos dados em diferentes condições atmosféricas.

Com os resultados dos estudos feitos foram selecionadas as posições para a colocação dos APs e dos Gateways LoRa.

A eletrónica de controlo consistiu no desenvolvimento de um sistema de heartbeat para a monitorização dos equipamentos da plataforma. Para desenvolver esse sistema foi necessário um circuito que controle a energia dos equipamentos da plataforma, de forma a obrigar o sistema a reiniciar em caso de anomalia.

Também foi preciso escolher um dispositivo com processamento, com um programa que controla o sistema heartbeat e o circuito e monitoriza o equipamento da plataforma.

Além disso, também foi feito um estudo de soluções que aumentem a fiabilidade do sistema heartbeat, selecionando técnicas que protejam os equipamentos de monitorização.

Na rede de controlo foi desenvolvido um programa que consegue conectar todos os dispositivos pertencentes ao sistema de heartbeat para a sua monitorização e controle. Além deste programa, na rede de controlo também foi necessário desenvolver uma solução de uma rede de backup, para, no caso de haver problemas na internet, continuar a ser possível comunicar com o sistema heartbeat.

1.2 Estrutura do documento

Além da introdução (capítulo 1), o documento está repartido em outros cinco capítulos.

No capítulo 2 é feito o levantamento das várias tecnologias mais recentes existentes nas redes de comunicações, mais especificamente nas redes de sensores, redes veiculares, nas WLANs, bem como as tecnologias de controlo e fiabilidade desenvolvidas até ao momento.

No capítulo 3 é apresentado o projeto PASMO, onde é identificada a sua localização geográfica e quais os objetivos inicialmente estabelecidos.

No capítulo 4 é apresentado o trabalho desenvolvido que contribuiu para a criação do projeto PASMO, onde são expostos os testes executados, e onde se indicam as variáveis em estudo e as condições climatéricas em que foram feitos os testes. Além disso, averigua-se que técnicas foram estudadas para os sistemas de controlo e monitorização e é feita uma explicação inicial da forma da rede de controlo.

Ao longo do capítulo 5 é apresentado o planeamento feito, como o sistema de controlo foi projetado e como é o programa de monitorização e controlo desenvolvido para correr nos sistemas de heartbeat.

Por fim, no capítulo 6 são indicadas as conclusões obtidas ao realizar este trabalho e algumas alterações ou melhorias possíveis que podiam ser feitas em caso do aprofundamento do mesmo.

2. Tecnologias de comunicação, controlo e fiabilidade

Nesta secção vai ser apresentado o estado da arte: de comunicações com sensores; das comunicações veiculares; das tecnologias de comunicação WLAN; e das técnicas de controlo e fiabilidade desenvolvidas até ao momento e usadas nos sistemas mais recentes.

Das várias tecnologias de comunicação disponíveis, são apresentadas algumas mais apropriadas, e de seguida, dessas, é feita uma escolha das que se enquadram no objetivo da plataforma, sendo então exposta a tecnologia selecionada para usar e uma tecnologia alternativa.

No ponto das tecnologias de controlo e fiabilidade será feita uma explicação do que é "controlo e fiabilidade", e depois são apresentadas duas tecnologias utilizadas.

2.1 Redes sensores (IoT)

As redes de sensores estão muito associadas ao conceito de IoT, por ser uma área essencial do IoT. Por isso, em primeiro lugar será explicado o conceito de IoT e posteriormente apresentadas as situações onde é aplicado.

IoT é a conexão dos dispositivos físicos com a internet, dando-lhes a capacidade de receber e transmitir dados, assim possibilitando acesso às informações que se necessita em qualquer lugar e a qualquer momento, e, dependendo da aplicação, permite que a informação obtida seja a que está a acontecer no momento, a que aconteceu nos últimos minutos, ou apenas um envio de informação esporádica de poucas dezenas de mensagens por dia.

Podem-se conectar sensores atmosféricos, possibilitando saber os vários valores de medidas atmosféricas recolhidas no local do sensor, como se podem conectar sensores de estacionamento, permitindo que os condutores possam saber os locais de estacionamento disponíveis no momento. Além de sensores, também se podem conectar vários eletrodomésticos, o que permite a criação das casas inteligentes, permitindo a comunicação entre eletrodomésticos e outros dispositivos eletrónicos.

Damos o seguinte exemplo da comunicação em casas inteligentes. Se conectar o despertador a uma torradeira e a uma máquina de café, é possível que no momento que o despertador tocar, a máquina de café e a torradeira sejam acionadas e comecem a preparar o pequeno-almoço.

Apesar do conceito de IoT já existir há alguns anos, até ao momento existem poucas aplicações generalizadas, devido às exigências tecnológicas. A sua aplicação seria muito cara, o que fez com que se adiasse a sua aplicação em grande escala. Contudo, com a redução dos custos das tecnologias, a maior facilidade de conexão com a internet e a redução do custo do tráfego, a aplicação do conceito está mais acessível. Por isso, é esperado que este tipo de tecnologia seja uma das que mais altere as nossas vidas num futuro próximo [2].

Na figura 1 podem-se ver algumas das muitas aplicações em que é possível aplicar IoT.

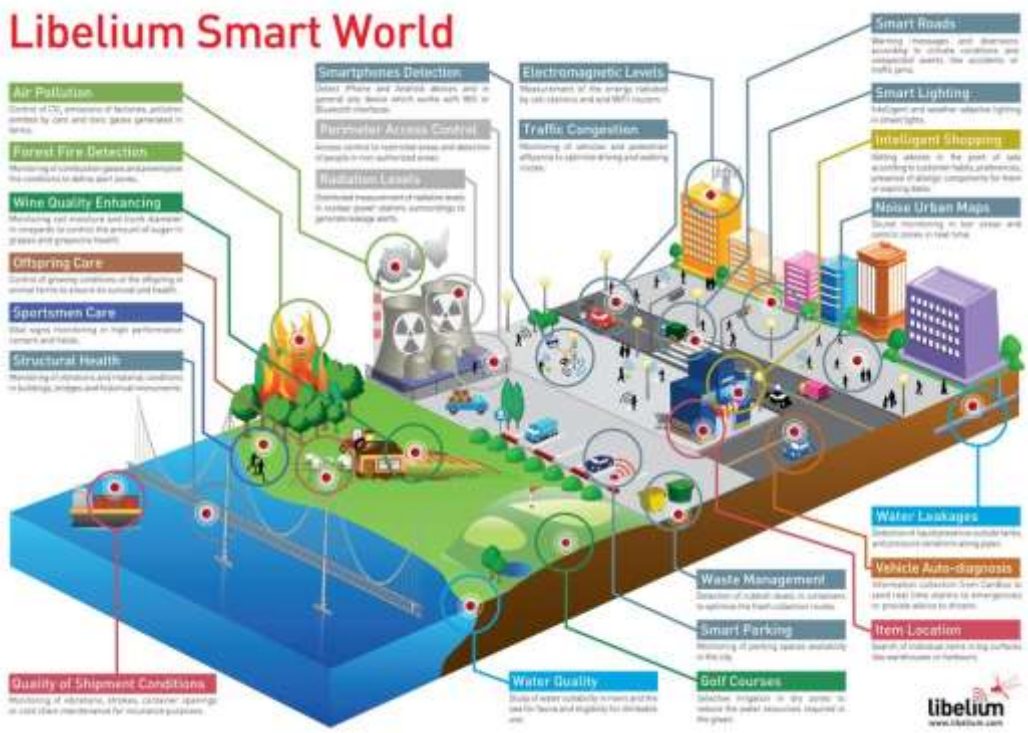


Figura 1 - Áreas onde se pode aplicar tecnologia IoT [1]

Pelo facto da IoT estar muito associado a redes de sensores, quando se procuram tecnologias wireless para essas redes, temos de ver as principais tecnologias de comunicação usadas em IoT. Assim, na tabela a seguir apresentada estão algumas das tecnologias de comunicação possíveis de usar para IoT.

Tecnologia	Pros	Contras
Bluetooth	– Não precisa de licença para o uso da banda – Baixo consumo energético(0.003W) – A segurança é feita pela troca de chaves de encriptação – Baixa latência – Média taxa de transmissão de dados máxima	– Pouco alcance (20 metros) – Bom apenas para redes pessoais
Wi-Fi	– Não precisa de licença para o uso da banda – Bom funcionamento na área abrangida – Baixa latência e alta taxa de transmissão de dados máxima	– Pouco alcance (50 metros em espaço fechado podendo atingir algumas centenas em espaços abertos) – Médio consumo energético (0.1W) não aconselhado para aparelhos que funcionam a bateria – A segurança do Wi-Fi sofre pelo grande uso
GSM	– Bom alcance (até 35 km) – Baixa latência e alta taxa de transmissão de dados máxima	– Necessita de um contrato com um fornecedor de serviço de telemóvel – Alto consumo energético (2W) – Segurança sofre pelo grande uso devido a ser uma tecnologia antiga
LoRa	– Bom alcance (5-10 km típico podendo chegar a mais de 20 km com linha de vista) – Não precisa de licença para o uso da banda – Baixo consumo energético (0.025W) – Segurança feita por autentificação e mantida por todo o tempo de comunicação – Baixo custo, depois de haver cobertura	– Alta latência e baixa taxa de transmissão de dados máxima
Sigfox	– Bom alcance (24 km) – Baixo consumo energético (0.025W) – Segurança pode ser aplicada ao nível da aplicação com encriptação de ponta a ponta	– Alta latência e muito baixa taxa de transmissão de dados máxima – Não podes colocar a tua própria Base Station – Custo de subscrição por cada sensor – Não aconselhado para redes que precisem de transmitir para o sensor
NB-IoT	– Bom alcance (10-15km) – Boa segurança – Baixa latência e alta taxa de transmissão de dados máxima	– Médio consumo energético (0.2W) – Necessita de subscrição com fornecedor de serviço de telemóvel
LTE	– Médio alcance (2km) – Boa segurança – Baixa latência e alta taxa de transmissão de dados máxima	– Médio consumo energético (0.2W) – Necessita de subscrição com fornecedor de serviço de telemóvel
LTE Cat-M	– Bom alcance (10-15km) – Baixa latência	– Médio consumo energético (0.2W Max) deve ter consumos inferiores a LTE – Baixa taxa de transmissão de dados máxima – Necessita de subscrição com fornecedor de serviço de telemóvel
Satélite	– Excelente alcance (abrange o globo totalmente ou quase todo) – Média taxa de transmissão de dados máxima	– Alto consumo energético – Alta latência – Necessita de subscrição para transmissão satélite (muito cara) – Má segurança

Tabela 1 - tecnologias wireless usadas em IoT

Na Tabela 1 estão apresentadas as tecnologias de IoT que são mais usadas, mas ainda existem outras tecnologias, tais como: RPMA [47], Weightless [48], NB-FI [49]. Estas tecnologias são pouco conhecidas ou de difícil acesso neste momento.

Algumas das tecnologias apresentadas na tabela são pouco usadas, mas apesar disso podem vir a ser muito importantes num futuro próximo. Além disso, algumas delas ainda estão em desenvolvimento. Para este trabalho estamos mais interessados em tecnologias de longo alcance (alguns quilómetros) e que tenham um consumo de energia muito reduzido (assim permitindo que ao aplicar os sensores, eles funcionem com apenas

uma carga de bateria durante vários anos, sem nenhuma manutenção). Para isso, as duas melhores tecnologias presentes na Tabela 1 são LoRa e sigfox, que nos seguintes subtópicos vão ser melhor apresentadas.

Também vai ser apresentada uma tecnologia celular, prevista no projeto, que é o GSM, por ter menos restrições na sua aplicação que outras usadas, mas, por ser uma tecnologia antiga, explicamos o protocolo mais recente das redes celulares que é o LTE.

2.1.1 Sigfox

A sigfox [3] [4] é uma operadora de telecomunicações multinacional fundada na França. O seu principal objetivo é desenvolver redes sem fios para aparelhos com um reduzido consumo energético, em que tanto podem ser conectados à internet ou conectados entre si, dependendo da aplicação.

A multinacional desenvolveu um protocolo a que chamou de sigfox. Este protocolo faz o uso de uma tecnologia chamada Ultra Narrow Band modulation, que consiste em enviar mensagens num espaço de frequência reduzido de apenas 100Hz. A transmissão é feita na banda livre situada nos 868MHz na Europa e nos 915 MHz nos EUA, assim permitindo fazer a transmissão com uma potência elevada sem grande consumo energético e que, ao ter uma transmissão com potências elevadas, consegue um maior alcance de transmissão.

Ao criarem o referido protocolo fizeram com que os dispositivos não necessitassem de criar ou manter uma conexão com a internet, o que faz com que não precisem de enviar em cada pacote transmitido bits de sinalização na camada MAC (controle de acesso ao meio), levando a que o protocolo fique mais leve. Também limitaram a informação transmitida por cada frame e a frequência com que se pode transmitir mensagens, reduzindo assim o número de bits transmitidos, levando a um menor consumo energético. Além disso, criaram uma rede de BS (base stations) em vários países ao redor do globo, de forma a que nesses locais qualquer sensor que seja colocado terá em média 3 BS ao seu alcance. Por não haver sinalização na camada MAC os ED (end devices) podem comunicar com qualquer BS ao seu alcance o que faz com que a transmissão apresente alguma redundância, assim aumentando a probabilidade de qualquer transmissão ser feita com sucesso.

Os aspetos apresentados acima, e outros não referidos, fizeram desta tecnologia uma das mais usadas em aplicações IoT, por ter uma longa duração das baterias, um longo alcance, um baixo custo de implementação e apresentar uma boa escalabilidade.

Ao conseguir uma grande escalabilidade, uma grande cobertura e uma boa eficiência energética o protocolo sigfox foi denominada como uma das tecnologias LPWAN (low power wide area network) de referência.

2.1.2 LoRa

LoRa [5] [6] é também uma tecnologia LPWAN, por conseguir cumprir os requisitos de escalabilidade, cobertura e eficiência energética para grandes áreas.

Para cumprir os requisitos, LoRa faz uso de diferentes técnicas. Usa as bandas livres de sub-GHz (868-870MHz na Europa), que em conjunto com as baixas transmissões de dados impostas e a utilização de spread spectrum, faz com que melhore a sensibilidade nos recetores, o que permite que LoRa atinja alcances elevados. A técnica

de transmissão que LoRa usa é a modulação com chirp spread spectrum, que utiliza pulsos lineares modulados em frequência em que faz o espalhamento do sinal numa grande largura de banda. Durante a transmissão de cada pulso, a frequência vai aumentado ou diminuindo, dependendo da informação codificada no pulso. Esta técnica fornece alguma tolerância ao erro na frequência (apresentado entre o recetor e o transmissor). O spread spectrum, em conjunto com o uso de sinais com o produto largura de banda tempo (BT) maior que 1 (duração da transmissão superior ao necessário para transmitir um período do sinal, exemplo: para um sinal com 2 Hz de frequência é preciso 0.5 segundo para transmitir 1 período com BT>1 esse bit será transmitido por mais tempo do que o necessário para 1 período), resulta numa maior resistência contra o efeito de doppler (o que melhora o desempenho da comunicação para objetos em movimento) e interferências na banda e fora da banda de transmissão.

Incluíram também na modulação um esquema de correção de erros usando um código cíclico, ficando com a comunicação mais robusta, adicionando alguma redundância.

Ao configurar a transmissão, dá para programar a largura de banda (que na Europa pode ser 125 ou 250 kHz) e o spreading factor (que pode tomar os valores de 7 a 12). Para cada valor de spreading factor existe uma modulação diferente que é ortogonal às modulações dos outros valores de spreading factor, gerando assim uma maior capacidade da rede e uma melhor eficiência espetral. Ao haver seis valores diferentes a gerar modulações ortogonais, é possível transmitir no mesmo momento e na mesma frequência vários sinais com valores de spreading factor diferentes sem haver nenhuma interferência. O valor escolhido irá afetar o alcance e o tempo de transmissão, sendo que o valor 12 é o que apresenta um maior alcance e maior tempo de transmissão.

LoRa usa um protocolo designado por LoRaWAN, que está projetado de forma a otimizar o consumo energético dos EDs. LoRa normalmente é utilizada em redes com topologia do tipo estrela onde as BS simplesmente fazem o encaminhamento dos dados transmitidos pelos ED com LoRa para o servidor por uma ligação IP. O mecanismo de acesso ao meio usado pelo LoRaWAN consiste em que cada ED tem um limite de dados que pode transmitir por ciclo em cada canal. Atingindo esse limite, ou transmite noutro canal ou espera até um novo ciclo começar. O tempo por ciclo e os dados transmitidos por ciclo têm de cumprir as restrições impostas pela regulação das frequências. Sempre que um ED precisa de transmitir, tem de selecionar qual é o canal que vai usar e, para o escolher, usa um algoritmo pseudoaleatório que vai selecionar um dos canais disponíveis no momento.

A camada MAC da LoRa suporta 3 classes diferentes de EDs, que são a A, a B e a C. No entanto os EDs apenas precisam de suportar as funcionalidades da classe A.

Cada classe tem funcionalidades diferentes:

- Na classe A, o ED tem de abrir 2 espaços de tempo para receção a seguir a uma transmissão. Esses dois espaços podem ser usados para receber informação ou para informar que a transmissão foi bem-sucedida, não recebendo dados em nenhum outro momento.
- Na classe B, o ED, além dos 2 espaços de tempo para receção depois de cada transmissão, tem também uma janela de tempo para receção em momentos programados. Para manter a sincronização do momento da janela de receção entre o ED e a BS, a BS transmite um Beacon periodicamente.

- Na classe C, os EDs estão no modo de receção todo o tempo, exceto no momento em que transmitem.

2.1.3 LTE

Neste segmento vai ser explicado a tecnologia LTE e não uma tecnologia celular feita para redes de sensores, porque a extensão usada no projeto faz uso da rede celular normal e não de uma das adaptações para redes de sensores.

Atualmente, em Portugal, o LTE (Long Term Evolution) [12] está a operar nas bandas de frequência dos 1800MHz, 2600MHz e 800MHz. No entanto existem múltiplas bandas de frequência usadas em diferentes países pelo mundo inteiro compreendido entre os 600MHz e os 2600MHz.

A existência de várias bandas de frequência para LTE advém da forma como a tecnologia foi projetada, pois esta tecnologia foi feita de forma a que o downlink e o uplink fossem diferentes. Essa diferença é devido a que no downlink temos uma antena alimentada pela rede elétrica, assim permitindo usar mais potência e contêm muito espaço para colocar a eletrónica necessária para técnicas de transmissão mais exigentes. Enquanto que no uplink temos um ED com limitações de espaço, de forma a ser portátil e alimentado por bateria. Por esta razão o uplink e o dowlink usam tecnologias e frequências diferentes de forma a obter um melhor desempenho. Assim sendo a seguir vai ser explicado resumidamente como o uplink e o downlink funcionam e que tecnologias usam. [13]

No downlink é usado OFDMA (ortogonal frequency division multiple access) na camada física. Esta técnica divide um canal grande de frequência em canais mais pequenos, utilizando frequências ortogonais, o que permite obter uma melhor eficiência e assim conseguir que se obtenham melhores data rates. Além disso, como os canais são mais pequenos, podem reagir melhor ao ruído em cada canal, assim permitindo um maior alcance. Ao usar OFDMA também permite que cada canal seja controlado e manipulado de forma distinta dos canais adjacentes, assim podendo usar canais diferentes para transmitir para EDs diferentes ao mesmo tempo, o que não se consegue alcançar com OFDM (ortogonal frequency division multiple).

Aproveitando as características do OFDMA, que reparte a frequência em blocos com FDD (frequency division duplex), como representado na Figura 2 e repartindo o tempo em espaços de 1 milissegundos com TDD (time division duplex), faz-se o agendamento de quando cada ED vai receber dados, e as decisões de agendamento podem ser alteradas a cada espaço de tempo de 1 ms. Para tomar cada decisão de agendamento, existem vários parâmetros que são tomados em consideração, como a qualidade de serviço exigida, a prioridade de cada serviço, a qualidade do link radio de cada ED, entre outros.

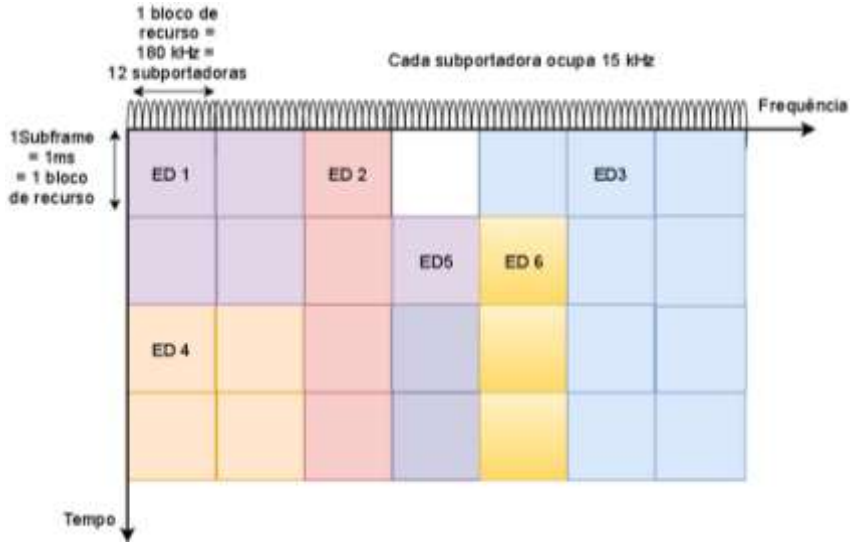


Figura 2 – OFDMA divisão do tempo e da frequência

Além dos canais normais de transmissão, existem canais de controlo que são usados para transmitir as informações de agendamento do uplink e do downlink, entre outras informações necessárias. As informações de controlo são transmitidas nos primeiros símbolos de uma subframe. Como o número de símbolos usados para controlo pode variar, existe um símbolo transmitido no início de cada subframe a informar quantos símbolos serão usados para o canal de controlo.

Assim sendo, para a transmissão do downlink de LTE, foi definida a estrutura de transmissão presente na Figura 3, que usa o modo TDD (time division duplex). Foram estabelecidas frames de 10ms e repartiram-se as frames em dez subframes com 1 ms cada uma, com o objetivo de cada ED poder transmitir durante uma subframe sem interrupção.

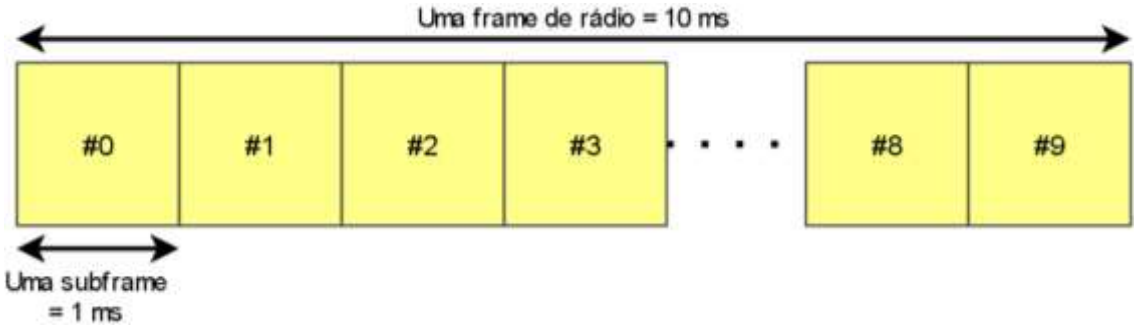


Figura 3 - estrutura de transmissão de LTE

Além de todas as características referidas, também está definido para LTE um sinal de referência que é bastante importante na procura de célula, e no estabelecimento da conexão da célula com o ED. Este sinal contém informação que permite diferenciar entre os vários eNodeB's (célula que conecta o core da rede com a parte wireless), com este sinal e o PBCH (Physical Broadcast Channel) (que é transmitido durante o estabelecimento da conexão) o ED consegue obter as informações necessárias para a conexão, como o tempo de símbolo e de rádio, a frequência, identificar a célula, a largura de banda.

Para o uplink, como havia restrições de espaço e por a alimentação provir de uma bateria, teve de se escolher outra tecnologia sem ser o OFDMA. A tecnologia selecionada foi SC-FDMA (Single Carrier Frequency Division Multiple Access), por apresentar uma boa relação entre a potência pico e a potência média. Para a transmissão SC-FDMA, usa-se DFT-s-OFDM (Discrete Fourier Transform Spread Ortogonal Frequency Division Multiplexing), em que, utilizando a transformada de Fourier, une vários canais pequenos num canal maior, mas reduz o tempo que vai estar a transmitir cada símbolo. A tecnologia divide o tempo usado em OFDMA pelo número de canais usados como representado na Figura 4, ou seja, cada símbolo vai utilizar mais largura de banda, mas vai ser transmitido por uma menor quantidade de tempo.

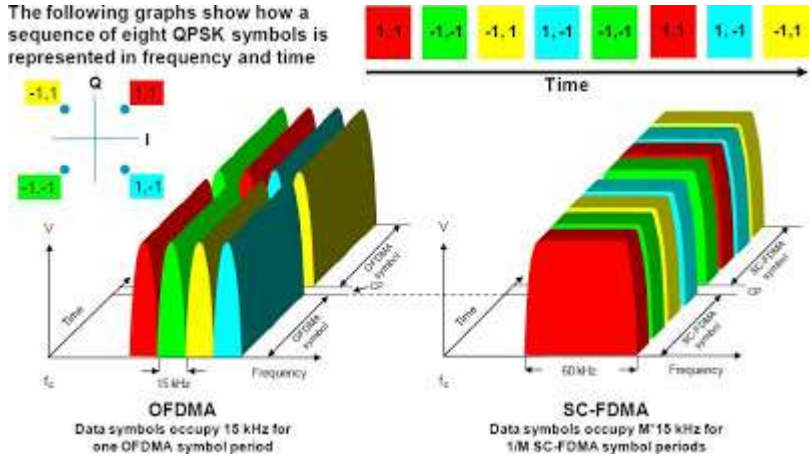


Figura 4 - comparação entre OFDMA e SC-FDMA [14]

Devido a existirem algumas semelhanças entre SC-FDMA e OFDMA, é possível usar as mesmas estruturas de transmissão no uplink e no downlink. Além disso, o agendamento de cada transmissão também é feito pelo eNodeB, que deverá informar cada ED pelo canal de controlo do downlink, indicando o momento e a frequência em que poderá transmitir. No canal de controlo de uplink são enviados os ACK dos pacotes recebidos pelo downlink, a informação da qualidade do canal, as informações da matriz de pré codificação, as informações do MIMO e requerimentos de agendamento. São reservados alguns canais em ambos os limites de frequência da largura de banda do uplink apenas para o canal de controlo e a reserva do canal de controlo é controlada por outra camada sem ser a camada física. Por outro lado, estes canais apenas são usados quando o ED não está a transmitir nada pelos canais de uplink, caso contrário o ED enviará a informação do canal de controlo junto com a informação transmitida pelo canal de uplink.

Além do mais existem alguns canais com períodos de tempo definidos, em que o ED se pode comunicar no caso de se querer associar ao eNodeB ou, no caso de querer requisitar um handover (o momento em que um ED se quer associar a um novo eNodeB com melhor sinal). As informações relativas a estes canais devem ser transmitidas em conjunto com o sinal de referência para o ED se poder associar. Nos canais de tempo definido qualquer ED pode transmitir a qualquer altura, não existindo nenhuma exigência quanto ao momento em que o início ou o fim da transmissão deverá acontecer, mas existem pacotes específicos para este tipo de comunicação.

Ao enviar o primeiro pacote de pedido de associação, o ED receberá uma resposta que lhe fornecerá uma subframe e um identificador temporário que será usado para solicitar um pedido de associação. Se as informações transmitidas na subframe forem aceites, o ED irá receber uma resposta do eNodeB, que irá indicar as últimas informações necessárias e que a associação foi bem-sucedida.

Finalmente, para cumprir os requisitos de bit rate impostos ao LTE, foi implementado o conceito de MIMO, que permite a um dispositivo usar várias antenas para transmitir informações diferentes ao mesmo tempo e na mesma frequência, e o recetor tem a capacidade de descodificar essa informação. Devido a esta tecnologia é possível multiplicar as taxas de transmissão obtidas, em que com duas antenas a transmitir ao mesmo tempo se consegue duplicar a taxa de transmissão.

2.2 WLAN

WLAN (wireless local area network) é um tipo de rede sem fios. Normalmente a WLAN tem um alcance por dispositivo de poucas centenas de metros em espaços abertos, que consiste na conexão sem fios de um access point a um ou mais dispositivos, como por exemplo computador, telemóvel, tablet, etc. Para a conexão, faz uso de ondas eletromagnéticas, de forma a permitir a conetividade de dois dispositivos usando redes sem fios.

A WLAN mais usada e mais conhecida atualmente é o Wi-Fi, que faz o uso de um ou vários dos protocolos IEEE 802.11. Além do Wi-Fi, existem a HyperLAN e outros menos conhecidos e que já não são usados.

IEEE 802.11 atua na camada física e na camada MAC. Para isso criaram vários padrões de transmissão e formas de codificação para redes sem fios. O motivo do IEEE 802.11 ter um sucesso tão grande nas redes wireless locais é porque não interessa quantas redes de Wi-Fi já existam no local; sabemos que se instalarmos uma nova rede Wi-Fi ela vai funcionar.

Os protocolos IEEE 802.11 mais usados atualmente estão apresentados na seguinte figura:

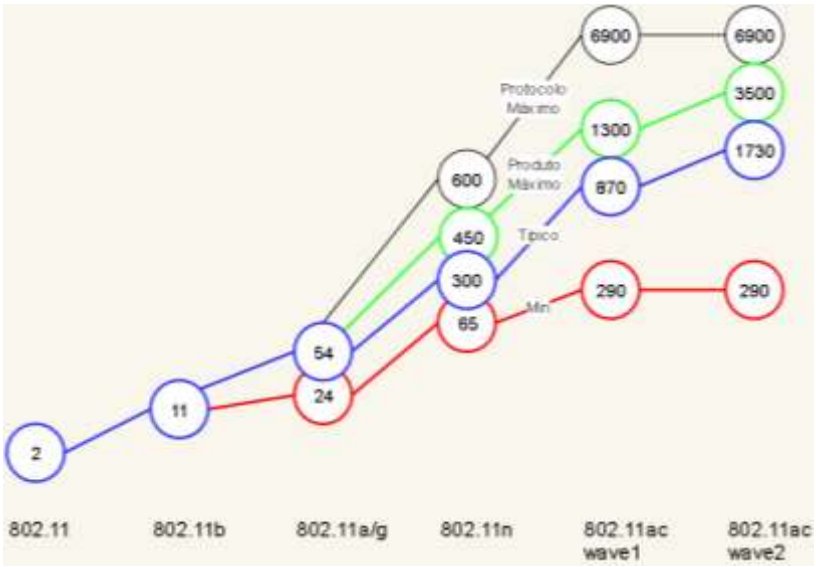


Figura 5 - standards WLAN mais utilizados atualmente

- Nota: IEEE 802.11ac Wave1 e IEEE 802.11ac Wave2 é diferente do WAVE do IEEE 802.11p.

Na Figura 5 estão os bit rates definidos para cada protocolo, em que os protocolos IEEE 802.11, IEEE 802.11b e IEEE 802.11g transmitem na banda livre dos 2.4GHz, os protocolos IEEE 802.11a e IEEE 802.11ac transmitem na banda livre dos 5GHz e o IEEE 802.11n transmite nas duas bandas livres a dos 2.4GHz e a dos 5GHz. Como os mais recentes são o 11n e o 11ac, que acabam por ser melhorias dos outros standards, vai ser apresentado a seguir o funcionamento na camada física e MAC e as melhorias feitas nos últimos dois standards.

2.2.1 Camada física

Na camada física foram inicialmente definidos três padrões no IEEE 802.11, mas nas evoluções seguintes foi usado a norma DSSS (Direct sequence spread spectrum), devido a se conseguirem valores de bit rate superiores, e no protocolo IEEE 802.11a foi introduzido a norma OFDM (ortogonal frequency-division multiplexing). Assim será explicado apenas essa norma.

O DSSS é uma técnica de espalhamento de espetro que usa mais quantidade de Hertz em relação à quantidade de bit/seg transmitidos, isso permite transmitir com uma potência menor, em que divide a banda disponível em canais de 11MHz e seleciona apenas um dos canais para fazer a sua transmissão. Além disso, usava a modulação DBPSK (Differential Binary Phase Shift Keying) com uma taxa de 1Mbps e a modulação DQPSK (Differential Quadrature Phase Shift Keying), com uma taxa de 2Mbps. No protocolo IEEE 802.11b os canais passaram a ser de 20MHz, e foi implementada a modulação CCK (Complementary code keying), em que já tinha taxas de transmissão de 5,5 e de 11 Mbps.

O OFDM, introduzido no standard IEEE 802.11a, divide os canais de 20MHz em 52 subportadoras, que são transmitidas em frequências ortogonais, fazendo com que cada subportadora não crie ruído para as subportadoras adjacentes. E, além disso usa as modulações BPSK (Binary Phase Shift Keying), QPSK (Quadrature Phase Shift Keying), 16-QAM (Quadrature Amplitude Modulation) ou 64-QAM em cada subportadora, assim conseguindo fornecer taxas até 54Mbps no protocolo IEEE 802.11a.

2.2.2 Camada MAC

No IEEE 802.11 foram criadas duas funções de acesso ao meio a DCF (Distributed Coordination Function) e a PCF (Point Coordination Function), sendo que apenas DCF é obrigatória e como poucos dispositivos contêm a função PCF, apenas vai ser explicada a função DCF.

A função DCF contém dois padrões para permitir o acesso ao meio, um deles é baseado em CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), a outra norma utiliza o mecanismo opcional RTS/CTS (Request to send / Clear to send).

Para começar, será apresentado o mecanismo de CSMA/CA, que está demonstrado na Figura 6, sendo explicado em seguida.

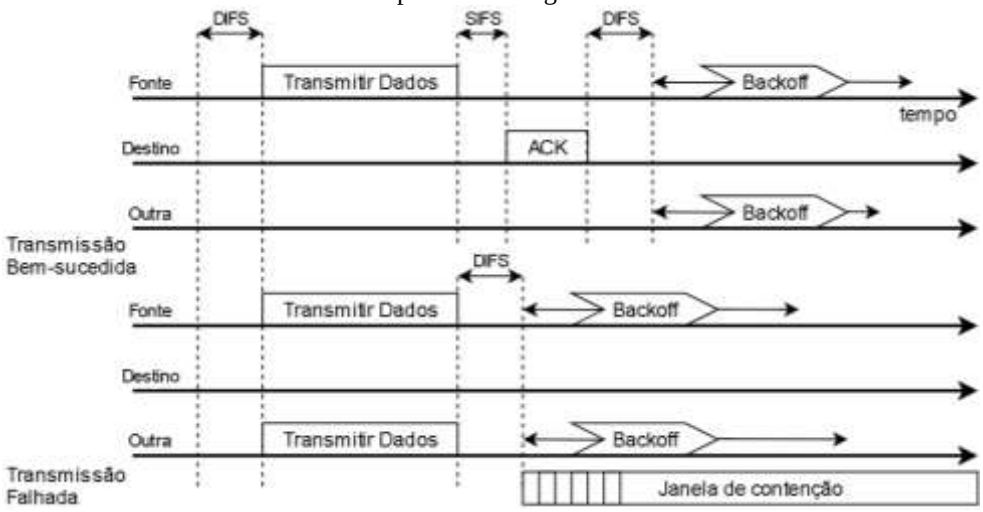


Figura 6 - Mecanismo de acesso ao meio usando CSMA/CA

Este mecanismo de acesso ao meio obriga a que, no momento em que um dispositivo quer transmitir alguma informação, tem de ouvir o meio durante um período de DIFS (Distributed Interframe Space) e, se não detetar nenhuma transmissão no momento, pode começar a transmitir. No caso contrário vai adiar a transmissão e começa um mecanismo de backoff. Esse mecanismo funciona com um temporizador de valor aleatório, compreendido entre zero e o tamanho da janela de contenção. O temporizador vai ser decrementado em uma unidade a cada espaço de tempo definido, sempre que o meio se apresentar livre por um período superior a DIFS, e vai parar sempre que o meio estiver a ser utilizado, sendo que o dispositivo começa a transmitir assim que o temporizador chega a zero. O valor de unidade do temporizador corresponde ao tempo de atraso máximo de ida e volta no BSS (Base Service Set).

No caso de haver uma transmissão, o recetor vai verificar a informação recebida com o código de deteção de erros chamado CRC (Cyclic Redundancy Check) e, caso não pareça ter ocorrido nenhum erro na transmissão, envia um pacote de ACK (acknowledgment), que será transmitido depois de SIFS (Short Interframe Space) (estando definido que o tempo de SIFS é inferior a DIFS) a contar do momento em que acaba de receber a informação.

Nesse meio tempo o dispositivo recetor estará a ouvir o meio: se o transmissor não receber o ACK, vai considerar que a transmissão falhou e entra em backoff. Quando acontece uma falha de transmissão, o valor da janela de contenção irá ser incrementado para a próxima potência de 2 menos 1, sendo que normalmente tem definido o valor mínimo de 7 e o valor máximo de 255. Por falar nisso, também está definido um limite do número de tentativas de retransmissão de um pacote que normalmente é sete e, no caso de algum pacote atingir esse limite, esse pacote será descartado. Para o caso de a transmissão ser bem-sucedida e o transmissor querer enviar outro pacote, teria vantagem na próxima transmissão, pois poderia começar a contar o tempo DIFS, no momento que acaba de receber o ACK, o que iria permitir que um dispositivo conseguisse monopolizar o meio. Para evitar essa situação, no final de cada transmissão o transmissor tem de entrar em processo de backoff.

O outro mecanismo de acesso ao meio, RTS/CTS, é especialmente projetado para evitar o problema do terminal escondido. O terminal escondido consiste na existência de três terminais, A, B e C, em que o terminal B consegue comunicar com o A e o C, e os terminais A e C apenas conseguem comunicar com o terminal B, pelo que, A e C não conseguem comunicar um com o outro, o que pode criar situações de colisão no terminal B. Por exemplo, se A estiver a transmitir para B e C quiser começar a transmitir para B, vai verificar que o meio está livre assim permitindo que transmita, o que criará uma situação de colisão no terminal B.

Na Figura 7 está representado o esquema da transmissão usando os pacotes RTS/CTS, que será explicado em seguida.

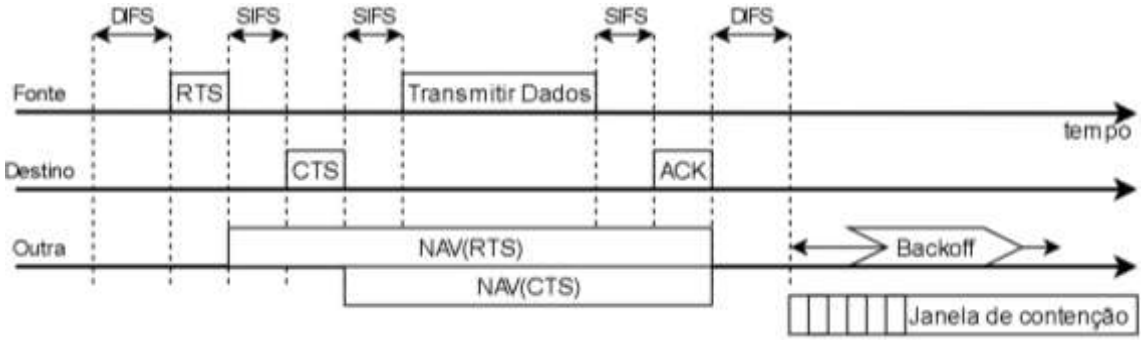


Figura 7 - Transmissão utilizando RTS/CTS

No caso de uma transmissão, o terminal que deseja transmitir irá verificar se o meio está ocupado durante DIFS. No caso de o meio estar ocupado, entra em backoff, como no mecanismo que usa CSMA/CA; mas se o meio estiver, livre irá começar o processo de transmissão enviando o pacote RTS. O terminal recetor, ao receber o pacote RTS irá responder passados SIFS com o pacote CTS se o meio estiver livre. Se o transmissor não receber o pacote CTS de volta irá para backoff. Caso contrário depois de SIFS irá transmitir o pacote que deseja transmitir, em que o terminal recetor irá responder com ACK se o pacote recebido não apresentar erros de transmissão. No caso de o terminal transmissor receber o ACK, irá considerar que foi transmitido com sucesso, senão irá considerar que a transmissão falhou e entra em backoff.

Esta forma de acesso ao meio apresenta algumas vantagens, pois, no caso de colisão um pacote de RTS é de apenas 20 bytes, enquanto que um pacote de dados pode atingir os 2346 bytes, o que reduz muito o tempo perdido em colisões. O recetor irá responder com CTS, o que faz com que todos os terminais ao alcance do recetor e do transmissor saibam que o meio está ocupado, por receberem os pacotes de RTS e de CTS e, nos pacotes vem indicado o tempo em que o meio irá estar ocupado. Assim os outros terminais podem calcular o NAV (Network Allocation Vector) que lhes indicará o tempo em que o meio estará ocupado, evitando colisões durante a transmissão de dados. Mesmo que não detetem o meio ocupado ao ouvi-lo, sabem que existe uma transmissão a acontecer no momento, permitindo assim que os vários terminais adiem as suas transmissões de forma a não ocorrerem colisões. O uso deste método de acesso ao meio é determinado pelos terminais, que podem decidir usar sempre, apenas quando transmitem pacotes grandes ou até nunca usar.

2.2.3 IEEE 802.11n

Como já referido acima, IEEE 802.11n é uma melhoria dos standards mais antigos, com alterações na camada física e na camada MAC. As melhorias implementadas no IEEE 802.11n são: MIMO, agregação de pacotes, ligação de canais e a forma de aceder ao meio quando se ligam canais.

MIMO (multiple input, multiple output) é uma técnica que permite que várias antenas comuniquem ao mesmo tempo, o que torna possível um aumento do bit rate com a mesma quantidade de espetro, utilizando multiplexagem espacial. Tal consiste basicamente na divisão do espaço de comunicação em vários canais distribuídos no espaço aéreo, em que utilizando várias técnicas de transmissão é possível que a interferência entre os vários canais se anule ou seja muito reduzida. Assim, usando a multiplexagem espacial, é possível triplicar o bit rate se o recetor e o transmissor tiverem no mínimo 3 antenas. Com MIMO permitirá atingir os 450Mbps enquanto que, sem usar esta técnica, apenas se conseguiria uma transmissão máxima de 150Mbps.

Ao usar MIMO também se consegue obter uma maior fiabilidade na informação recebida. Se um AP tiver várias antenas, dado que o sinal pode chegar ao AP por diferentes caminhos, cada antena vai receber uma cópia da informação com uma distorção de sinal diferente. Aí, podem-se aplicar técnicas de equalização de sinais MIMO no recetor que faz a combinação de todas as cópias resultando num sinal mais fiável, assim se conseguindo ter menor probabilidade de receber dados errados. Com esta técnica conseguem-se dados mais confiáveis, uma menor quantidade de repetição de envio de pacotes e obter bit rates mais constantes. Para conseguir usar esta funcionalidade do MIMO, é necessário que o número de antenas no recetor seja maior do que o número de "canais de transmissão espaciais".

Além disso, com o MIMO também é possível ter beamforming, que consiste em criar uma transmissão dirigida apenas ao dispositivo de destino em vez de ser radiada em todas as direções. Ao usar beamforming pode-se obter uma maior segurança, pois existe um menor número de dispositivos a conseguir ouvir a mensagem transmitida, evitando sniffing e, como se fornece um sinal direto ao dispositivo, consegue-se evitar a distorção destrutiva causada pelo multipath que afeta bastante os dispositivos com um número reduzido de antenas.

A agregação de pacotes foi uma tecnologia implementada pela primeira vez no protocolo IEEE 802.11n. Antes disso nenhum protocolo Wi-Fi tinha esta tecnologia. Na agregação de pacotes existem duas técnicas de agregação que são a A-MPDU e a A-MSDU demonstrados na Figura 8.

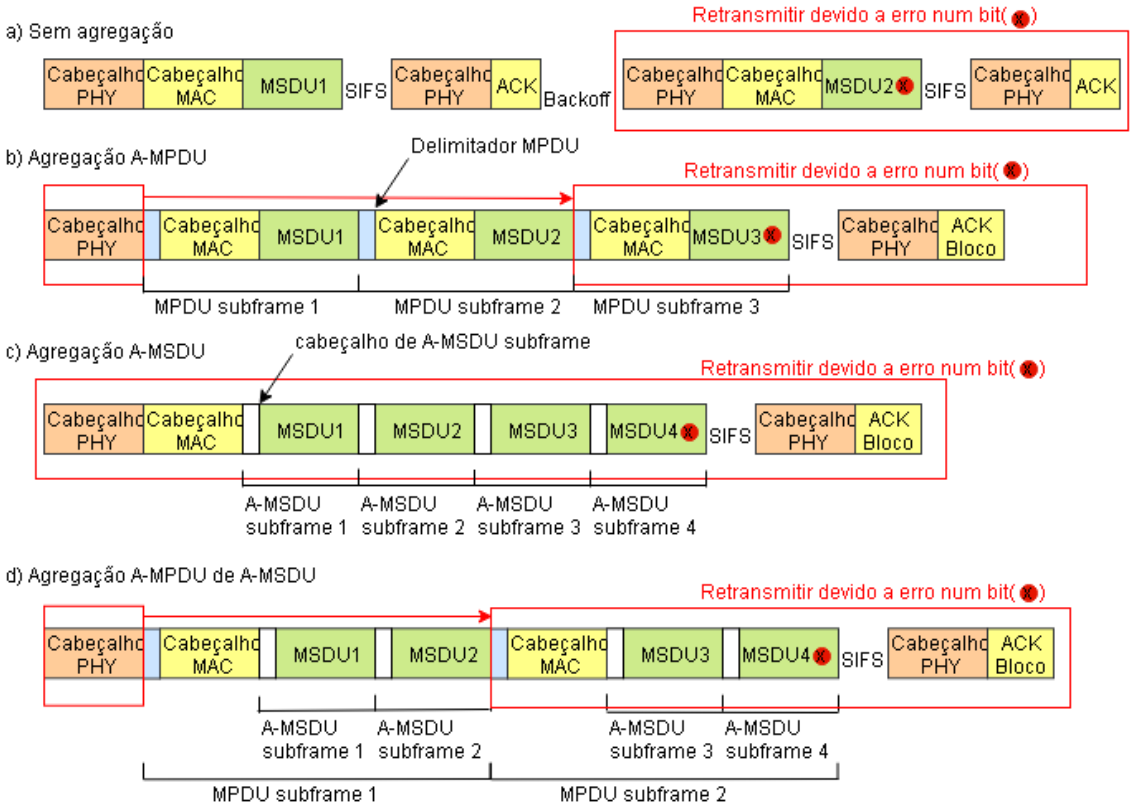


Figura 8 - Agregação de pacotes

Na agregação A-MPDU, o cabeçalho da camada física é apenas enviado no início, mas repete o cabeçalho da camada MAC e um delimitador da agregação para cada pacote transmitido. Isso permite que, no caso de haver erros na transmissão de algum pacote, apenas esse vai ser retransmitido. Esta agregação aumenta a eficiência de transmissão significativamente, pois não repete o cabeçalho da camada física em cada pacote e permite enviar vários pacotes numa só transmissão.

Na agregação A-MSDU, é enviado inicialmente os cabeçalhos das camadas MAC e física e de seguida transmite todos os pacotes com os seus cabeçalhos da agregação, o que apresenta uma maior eficiência de transmissão, mas, no caso de haver um erro de transmissão, todos os pacotes têm de ser retransmitidos. Porém tem uma maior eficiência de transmissão do que a agregação A-MPDU, no caso de não haver erros na transmissão.

Como ambos os tipos de agregação têm as suas vantagens e as suas desvantagens, também foi introduzida a agregação A-MPDU e A-MSDU em conjunto, que apresenta uma eficiência de transmissão que fica entre os dois tipos de agregação, mas, no caso de um erro de transmissão, não precisa de repetir todos os pacotes transmitidos.

No IEEE 802.11n foi introduzida a ligação de canais. Até esse momento cada dispositivo que tivesse Wi-Fi apenas poderia transmitir num canal de 20MHz. Ao adicionar esta funcionalidade em momentos em que 2 canais subjacentes estejam livres, é possível transmitir nos dois ao mesmo tempo, o que permite atingir taxas de transmissão superiores ao dobro do que se pode obter só com 1 canal, devido a poder transmitir nos 2 canais

e na banda de guarda presente entre ambos. Ao ser introduzida a ligação de canais teve de se rever a forma de acesso ao meio, pelo facto de os aparelhos não conseguirem fazer a verificação de canal livre nos dois canais ao mesmo tempo. Por isso, optou-se por fazer uma verificação normal no primeiro canal e, antes da transmissão, verifica-se o segundo canal durante um curto espaço de tempo, para averiguar se este está livre. Todavia, isso faz com que a verificação do segundo canal seja uma forma incompleta de verificação.

2.2.4 IEEE 802.11ac

Como já foi referido, o protocolo IEEE 802.11ac é uma melhoria dos protocolos mais antigos, fazendo uso das suas melhores especificações, enquanto que as especificações que não são usadas ou inúteis, são simplesmente esquecidas e não são implementadas neste protocolo. Portanto, é possível encontrar algumas especificações nos protocolos mais antigos que foram descontinuadas neste.

Primeiro de tudo, serão indicadas algumas especificações que IEEE 802.11ac manteve do IEEE 802.11n que foram: o short guard interval, que pode ser implementado nos dispositivos opcionalmente; o uso do código de correção de erros LDPC (low-density parity check), que ajuda a aumentar as taxas de transmissão à distância evitando erros de transmissão; o uso de códigos STBC (space-time block code), mas apenas os modos 2x1, 4x2, 6x3 e 8x4, apesar de se considerar que apenas o modo 2x1 vai ser utilizado, pois nas restantes situações poder-se-ão obter melhores resultados com beamforming. Além dos referidos, também foi mantido beamforming, mas adicionando a opção de usar o mecanismo de explicit compressed feedback; manteve-se a ligação de canais, mas estendendo a ligação de canais dos 40MHz para os 80MHz ou 160MHz, em que como no IEEE 802.11n é usado o método de verificação normal em 20 MHz e apenas se verifica com CCA (clear-channel assessment) durante breves instantes antes da transmissão nos outros canais; manteve-se também os métodos de agregação de pacotes, mas passou a ser obrigatória a implementação da agregação A-MPDU.

Na definição das especificações do IEEE 802.11ac deu-se especial ênfase ao aumento da velocidade de transmissão e à robustez, com o objetivo de obter um melhor desempenho.

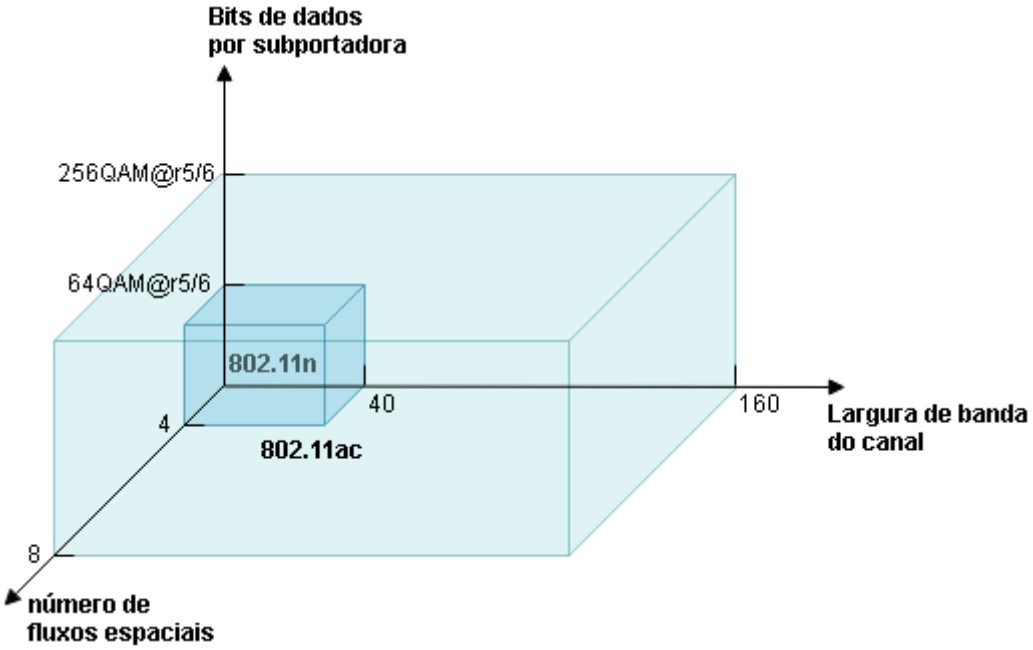


Figura 9 - Como IEEE 802.11ac aumenta o bit rate em relação ao IEEE 802.11n

Como representado na Figura 9, foi através da melhoria das seguintes três tecnologias: a constelação das subportadoras, o MIMO nos fluxos espaciais e a junção de canais, assim conseguiu-se aumentar a velocidade de transmissão. Por este motivo, no IEEE 802.11ac consegue-se obter taxas de transmissão de 6.9Gbps no limite máximo do protocolo.

Ao ser adicionada a constelação 256QAM com rate de 5/6, consegue-se melhorar a taxa de transmissão em 33%, quando a distância entre o AP e o ED é reduzida. O aumento dos fluxos espaciais permitiu aumentar o bit rate de 4x para 8x, assim duplicando as taxas de transmissão em relação ao IEEE 802.11n. No entanto esta funcionalidade só pode ser usada quando o transmissor e o recetor têm 8 antenas, sendo que o número mínimo de antenas entre o recetor e o transmissor é o número máximo de fluxos espaciais. Contudo, normalmente os dispositivos móveis querem ter um número reduzido de antenas para reduzir o consumo energético, por isso esta funcionalidade é raramente usada com oito fluxos espaciais. Além destas funcionalidades, foram adicionados também canais com uma maior largura de banda, o que será bastante útil em situações onde existe um número reduzido de APs, permitindo a transmissão em vários canais ao mesmo tempo, quando não estão a ser usados. Desta forma, consegue-se aumentar o bit rate para uma taxa superior a 4 em relação ao IEEE 802.11n quando se usa a ligação de canais com 160MHz.

Levando isto em consideração, existe uma fórmula simples de calcular o bit rate disponível, demonstrada na seguinte tabela.

Camada física	Largura de banda (como número de subportadoras)		Número de fluxos espaciais		Bits de data por subportadora		Tempo por Símbolo		bit rate camada física (bps)
802.11n e 802.11 ac	56 (20MHz)	X	1 a 4	X	Até 5 / 6 * log2(64) =5	/	3.6 microsegundos (short guard interval)	=	
	106 (40MHz)						4 microsegundos (long guard interval)		
apenas 802.11ac	234 (80MHz)		5 a 8		Até 5 / 6 * log2(256) = 6.67				
	468 (160MHz)								

Tabela 2 - Cálculo da taxa de transmissão para IEEE 802.11n e IEEE 802.11ac

Utilizando a fórmula presente na Tabela 2 consegue-se obter o bit rate para cada situação. Por exemplo no caso de transmissão com 80MHz, 2 fluxos espaciais, 64QAM e long guard interval, obter-se-iam 585Mbps.

No que diz respeito ao aumento da robustez no IEEE 802.11ac, esse acréscimo é devido às especificações a seguir apresentadas.

O protocolo IEEE 802.11ac foi desenhado para operar apenas na banda dos 5GHz, de forma a evitar todo o ruído criado pelos aparelhos que não pertencem à norma IEEE 802.11, mas transmitem nos 2.4GHz (como o Bluetooth e os micro-ondas). Assim, ao transmitir apenas nos 5GHz consegue usar uma banda mais livre obtendo uma maior robustez, além de que a banda dos 5GHz é a mais usada no mundo. Foi implementado também a extensão do mecanismo RTS/CTS para as transmissões com mais de um canal.

Além das especificações antes referidas no IEEE 802.11ac, também foi melhorada a tecnologia MIMO que nos padrões anteriores era restrita, onde apenas se poderia usar para a transmissão com um dispositivo de cada vez. Assim poderia acontecer um AP ter várias antenas sem transmitir devido ao ED apresentar poucas antenas. Devido a isso, a transmissão com MIMO para apenas um ED foi designada como SU-MIMO (single-user MIMO), no IEEE 802.11ac foi introduzido o MU-MIMO (multiuser MIMO), que permite um AP transmitir ao mesmo tempo e no mesmo canal para vários EDs usando antenas diferentes para transmitir para cada ED.

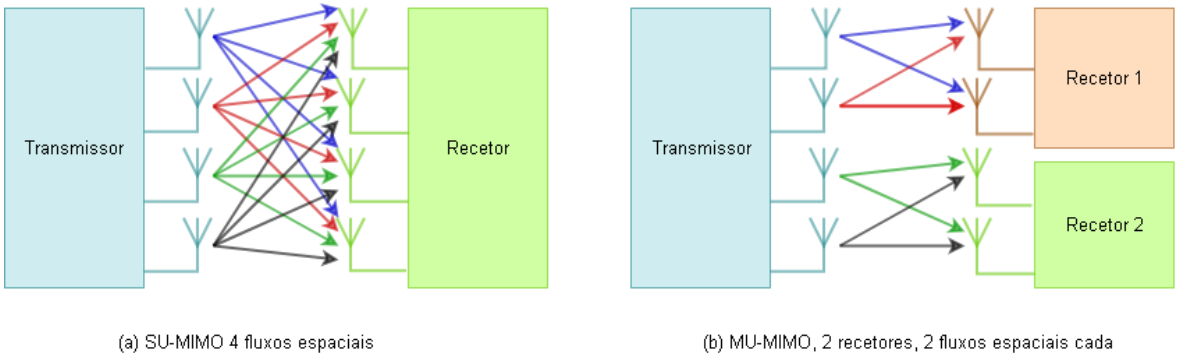


Figura 10 - Esquemático de SU-MIMO e MU-MIMO [11]

Como se pode visualizar pela Figura 10, ao usar SU-MIMO o AP utiliza todas as antenas para transmitir para apenas um ED de cada vez, enquanto que ao usar MU-MIMO o AP pode usar apenas algumas das antenas disponíveis para transmitir para cada ED, assim permitindo transmitir para vários EDs ao mesmo tempo usando o mesmo canal.

2.2.5 HyperLAN

HyperLAN [50] é uma WLAN cada vez menos conhecida e usada. Este protocolo foi definido pela ETSI (European Telecommunications Standards Institute) como uma alternativa aos protocolos IEEE 802.11. Este norma atua na camada física e na parte MAC da camada de ligação de dados do modelo OSI.

A HyperLAN faz o uso da banda livre dos 5GHz, para evitar o ruído presente nos 2.4GHz. Na primeira versão, chamada HyperLAN/1, é usado camada física as modulações FSK (frequency-shift keying) e GMSK (gaussian minimum-shift keying). Na camada MAC é colocado protocolos de encaminhamento, segurança e poupança de energia. Nesta versão conseguiu-se transferências até os 20Mbps e um alcance de 50 metros.

Na segunda versão, chamada HyperLAN/2 já atingiu transferências de 54Mbps. Nesta versão já se usou BPSK, QPSK, 16QAM e 64QAM para a camada física. Também foi adicionado segurança permitindo que o AP e o ED tivessem uma forma de autentificação na sua comunicação.

A HyperLAN perdeu a competição com os protocolos IEEE 802.11 e nunca conseguiu uma boa posição no mercado. Acabando por algumas das suas tecnologias serem usados nos protocolos IEEE 802.11 e estar a ser esquecida.

2.3 Redes veiculares

As redes veiculares ou VANETs (veicular ad-hoc network) são um dos tipos de redes mais complicados de implementar devido à constante alteração das posições dos EDs, assim tornando difícil saber a topologia da rede, o que exige a constante verificação da topologia da rede para poder comunicar. Cada unidade tem de apresentar um alcance de algumas centenas de metros em áreas rurais e autoestradas para conseguir comunicar com outras unidades. Além disso tem de conseguir comunicar com dispositivos que estão em movimento e conseguir apresentar um valor baixo de latência, pois um carro a 100km/h equivale a 27.8m/s num espaço de 0.1seg o carro deslocou-se 2.7metros o que pode fazer diferença numa situação de risco de acidente, por isso é exigido uma reduzida latência.

Existem neste momento vários standards passíveis de utilização, que estão apresentados na tabela seguinte:

Norma wireless	Taxa de transmissão de dados	Alcance	Interferência de sinal	Forma de acesso ao meio	Segurança	Mobilidade máxima (km/h)	Adequado para aplicações seguras
Celular	129 Mbps	50 km	Baixa	Baseado em conteúdo	Alta	250	Não
IEEE 802.16e	70 Mbps	50 km	Baixa	Agendado	Alta	250	Sim
MBWA	4.5 Mbps	15 km	Alta	Agendado	Alta	250	Não
IEEE 802.11a	54 Mbps	100 m	Baixa	Baseado em conteúdo	Baixa	120	Não
IEEE 802.11b	11 Mbps	100 m	Alta	Baseado em conteúdo	Baixa	150	Não
IEEE 802.11g	54 Mbps	140 m	Alta	Baseado em conteúdo	Baixa	120	Não
IEEE 802.11n	100 Mbps	250 m	Alta	Baseado em conteúdo	Alta	120	Não
IEEE 802.11p	27 Mbps	1 km	Baixa	Baseado em conteúdo	Alta	150	Sim
CALM M5	6 Mbps	10 km	Alta	Baseado em conteúdo	Alta	150	Sim
Infravermelhos	4 Mbps	100 m	Baixa	Baseado em conteúdo	Alta	250	Não
Bluetooth	24 Mbps	100 m	Alta	Agendado	Baixa	30	Não
Zigbee	250 Kbps	100 m	Alta	Agendado	Alta	20	Não
UWB	100 Mbps	10 m	Baixa	Baseado em conteúdo	Alta	20	Não

Tabela 3 - standards wireless possíveis de usar em VANETs

Para a escolha da tecnologia a utilizar, como os carros estão em constante movimento e interessa minimizar o número de equipamentos a instalar, a comunicação tem de apresentar um alcance mínimo de algumas centenas de metros, com uma taxa de transmissão de algumas dezenas de Mbps para ter uma latência pequena. Pelos valores presentes na tabela anterior, apenas as tecnologias IEEE 802.11, o WiMAX e o sistema celular cumprem os requisitos.

Como o sistema celular exigiria um contrato com uma operadora, não apresenta grande interesse. E tanto o sistema celular como as normas IEEE 802.11g e 802.11n não estão desenhadas para rede veiculares, o que faria ter uma latência mais elevada do que a desejada. Portanto, apenas serão apresentadas as duas seguintes tecnologias: o protocolo IEEE 802.11p, também conhecido por WAVE e o IEEE 802.16e, também conhecido como Mobile WiMAX.

2.3.1 IEEE 802.11p – WAVE

IEEE 802.11p [8] é um standard que altera algumas das funcionalidades presentes nos outros protocolos da IEEE 802.11, de forma a ser possível implementar em redes veiculares. Este standard faz uso da banda licenciada dos 5.9GHz, que é uma banda específica para redes veiculares. É projetado para ter unidades de comunicação em cada carro, chamadas por OBU (onboard unit) e unidades de comunicação nas bermas da estrada, chamadas RSU (roadside unit), sendo que estas deverão estar conectadas à internet.

As comunicações podem ser feitas de duas formas: entre dois carros [que são as V2V(vehicle-to-vehicle)] e entre um carro e uma RSU [que são as V2I (vehicle-to-infrastructure) ou V2R (vehicle-to-roadside unit)]. Ao poder comunicar das duas formas, é possível dar alerta de possíveis perigos a carros que se encontram nas

proximidades do primeiro a detetá-los com comunicação V2V; assim como é possível informar carros fora do seu alcance comunicando através das RSU usando comunicação V2R, que comunicará com outra RSU e informará os carros mais distantes. Ao ter as RSUs conectadas à internet, torna possível fornecer serviço de internet aos carros em movimento, assegurando, contudo, que os serviços gerais de internet deverão ter uma prioridade inferior aos pacotes de informação sobre a estrada.

Este protocolo apresenta uma latência baixa, com taxas de transmissão de até 27Mbps e tem um alcance garantido de 300 metros, sendo possível atingir os 1000 metros como indicado na Tabela 3 e no documento [7].

2.3.2 IEEE 802.16e – Mobile WiMAX

O Mobile WiMAX [8] [7] neste momento está a utilizar os 5.5GHz na Europa. WiMAX consegue fornecer voz, vídeo e dados, além de suportar mobilidade e autentificação de dados. Tem taxas de transmissão que rondam dos 30 aos 70 Mbps e tem um longo alcance que consegue atingir perto de 50km, o que faz dela uma das melhores tecnologias a ser aplicada em redes veiculares.

Para atingir as especificações antes referidas, o WiMAX suporta na camada física OFDM (ortogonal frequency division multiplexing) e OFDMA (ortogonal frequency division multiple access) o que, ao dividir a frequência em canais mais pequenos, possibilita que seja usada com melhor eficiência, assim permitindo que se tenham melhores data rates. Além disso, como os canais são mais pequenos, têm uma melhor resposta ao ruído em cada canal, assim permitindo um maior alcance. Na camada MAC existem 2 configurações possíveis que é a PMP (point to multipoint) e a mesh. A PMP é idêntica à usada em redes celulares, onde os EDs apenas podem comunicar com a BS, sendo que não podem comunicar entre si, e a BS pode comunicar com vários EDs ao mesmo tempo. Na configuração mesh, todos os EDs podem comunicar entre si e com as BSs, e é permitido na configuração mesh que os EDs funcionem como routers, logo em algumas situações os EDs podem fazer o roteamento de pacotes de informação que não são destinados a eles.

2.4 Controlo e fiabilidade

O controlo e a fiabilidade são duas definições distintas que se utilizam muito em engenharia.

O controlo [40] tem por objetivo obter modelos de sistemas dinâmicos e a partir desses modelos conseguir criar unidades (controladores), que irão fazer o sistema reagir da maneira desejada. Este tipo de metodologia tem sido cada vez mais aplicado nos sistemas modernos do dia a dia com que lidamos, desde o cruise control e as ajudas de estacionamento que estão a ser aplicadas nos carros mais recentes, aos simples métodos pré programados e mecanismos de funcionamento dos eletrodomésticos, que se encontra nos mais antigos como máquinas de lavar, máquinas de café ou frigoríficos, até aos mais recentes que são total ou quase totalmente automatizados. Cada vez é mais comum os aparelhos elétricos apresentarem alguma forma de malha de controlo pré-programada.

A fiabilidade [41] é o estudo da percentagem de vezes que um determinado processo vai correr da maneira desejada ao ser repetido múltiplas vezes. A fiabilidade pode ser ilustrada da seguinte forma. Ao pegar num

número elevado de telemóveis iguais e ligá-los todos ao mesmo tempo, a fiabilidade pode ser estudada por, ao final de 1 ano de estarem ligados, apurar quantos estão a funcionar corretamente, considerando que todos os telemóveis tiveram um uso previsto para o consumidor comum. Este pode ser um dos estudos de fiabilidade de um produto.

2.4.1 watchdog

O watchdog é um conceito que tenta melhorar a fiabilidade ao usar malhas de controlo, pois o objetivo do watchdog é controlar se um dispositivo está a funcionar normalmente.

Watchdog [42], ou temporizador watchdog, normalmente é usado para verificar o correto funcionamento de computadores. O que acontece normalmente é que, se o computador estiver a funcionar normalmente, deverá fazer o reset ao temporizador do watchdog regularmente. No caso de acontecer uma falha no computador, o temporizador irá chegar ao seu tempo limite e nesse momento o watchdog deverá iniciar um processo de restauro do computador, que, por norma é colocar o computador num estado seguro e de seguida retomar o estado de funcionamento normal.

Os watchdogs são frequentemente usados em qualquer dispositivo eletrónico que não apresentem fácil acesso ou em computadores que controlem sistemas críticos. Nesse tipo de situação, o computador tem de ser autossuficiente e conseguir resolver qualquer problema que apareça, por isso se o computador "ficar congelado", ele tem de conseguir restaurar o seu modo de funcionamento normal sozinho. Como por exemplo, qualquer computador integrado nas sondas que são enviadas para o espaço, é uma das situações que no caso de o computador não ser autossuficiente, pode acontecer uma falha do sistema a meio de uma missão e todo o equipamento ficar inutilizável. Também estão implementados watchdogs no caso de computadores de controlo de centrais nucleares, em que se o computador não for autossuficiente, existe um grande risco de acidente na central nuclear no caso de o computador "ficar congelado".

Os watchdogs podem ser distinguidos em dois tipos: os watchdog de temporizador único, em que caso o tempo limite passe, executa o reiniciar do sistema; ou os watchdog de vários temporizadores, que no fim de cada um tenta executar uma forma de corrigir o problema, se não for resolvido pelos vários temporizadores e chegar ao fim do último temporizador executa um reiniciar.

2.4.2 Gaiola de faraday

A gaiola de faraday [51] é uma boa forma de proteger dispositivos eletrónicos aumentando a sua fiabilidade. Esta gaiola consegue proteger todos os equipamentos que estão no seu interior de campos elétricos e campos magnéticos externos.

Foi descoberto por Michael Faraday que, quando se aplica um campo elétrico a uma estrutura com extremidades condutoras, essa estrutura irá colocar cargas elétricas nas extremidades de forma a cancelar o campo elétrico externo. Como representado na figura seguinte:

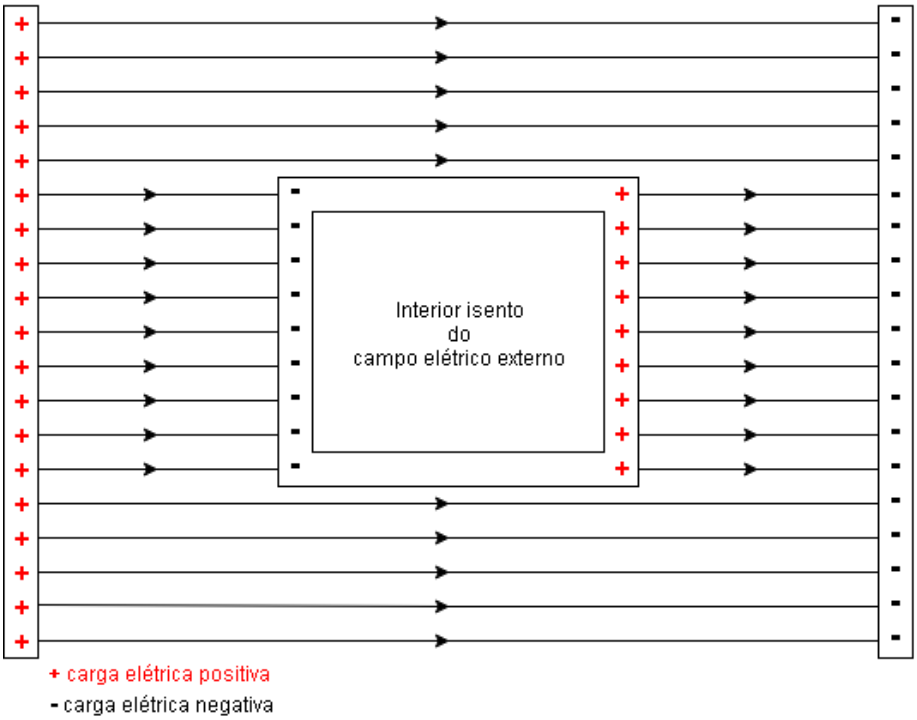


Figura 11 – Gaiola de Faraday

Faraday para provar os seus estudos, contruiu uma gaiola de metal e carregou-a eletricamente com um gerador de alta tensão, provando que era seguro permanecer no seu interior ao entrar dentro da gaiola. Esta barreira também é chamada de blindagem eletrostática.

A gaiola de faraday é muito aplicada nos aparelhos modernos: o aparelho que mais se pode associar com a gaiola de faraday é o micro-ondas. O micro-ondas usa a gaiola de forma para manter os campos elétricos e magnéticos gerados para aquecer a comida no seu interior. É também usado em equipamentos mais sensíveis às radiações eletromagnéticas externas, ou equipamentos que precisão de bloquear a radiações que produzem, para não afetar o ambiente à sua volta.

3. O projeto PASMO

A rede PASMO [19] foi o nome dado à plataforma que contextualiza o trabalho apresentado neste documento, é um projeto que está a ser implementado por uma parceria entre o IT (Instituto de Telecomunicações) e a Câmara Municipal de Ílhavo. O projeto tem por objetivo fornecer uma plataforma aberta, onde as empresas poderão desenvolver e experimentar soluções de tecnologias de redes veiculares e de redes de sensores. Este projeto é financiado pelo programa Centro 2020 em que, ao disponibilizar esta rede, se pretende atrair empresas que desenvolvam soluções de mobilidade para o distrito.

3.1 A plataforma

Este projeto está pensado para fornecer principalmente 3 tipos diferentes de serviço.

1) Visa fornecer Wi-Fi com os protocolos IEEE 802.11 pelas praias da Barra e da Costa Nova, sendo para o efeito colocados vários Access Points ao longo da praia, assim fornecendo acesso livre a qualquer pessoa que se encontre na praia.
2) Irá também fornecer cobertura de LoRa para toda a área da localidade da Barra, em que na plataforma irão ser integrados dois tipos de sensores LoRa: sensores de controlo atmosférico e sensores de estacionamento.

   Os sensores de controlo atmosférico serão colocados na zona da praia e na área do porto, que são zonas consideradas mais críticas. Estes dois sensores irão controlar o nível de radiação e as condições atmosféricas no local em que forem colocados. As informações obtidas pelos sensores podem ser usadas para estudos e para o controlo de qualidade atmosférica nessas zonas.

   Os sensores de estacionamento serão colocados ao longo da Avenida Fernão de Magalhães onde vão permitir controlar o estacionamento nessa área.

   As informações obtidas pelos sensores de estacionamento e pelos sensores de atmosfera, serão disponibilizadas através de um site ou aplicação, o que permitirá saber os estacionamentos livres e as condições atmosféricas no momento.
3) Além da rede Wi-Fi e da rede de sensores fornecida, será colocada uma rede veicular na A25. Para implementar esta rede serão necessários RSUs, que suportam IEEE 802.11p nas bordas da estrada ao longo de toda a zona onde irá ter cobertura. Também serão criados alguns OBUs, que serão disponibilizados para que quem necessite desta plataforma, a possa usar para fazer os seus testes e demonstrações. Estes OBUs estão projetados de forma a poder ser usados em todos os veículos mais comuns, e permitem ambas as comunicações do protocolo, a V2V e a V2R. Além disso, os RSUs estarão conectados à internet através de fibra, o que permitirá à rede automóvel fornecer internet, para além das funcionalidades de segurança e controlo necessárias para as redes veiculares.

Todos os componentes da plataforma estarão ligados à internet, onde será aplicada uma ligação privada nas camadas mais altas da internet, que estará conectada com um servidor localizado no IT de Aveiro, de onde será

possível controlar toda a rede PASMO. No servidor estará a correr um programa que permitirá interagir com os vários componentes da rede, e também será onde a aplicação irá buscar as informações da rede.

Para se poder controlar o estado de cada componente e de forma a evitar que algum equipamento não responda devido a eventuais falhas, será implementada uma rede de controlo, que irá ter um sistema a verificar se cada um dos componentes está a funcionar bem. Esses sistemas de verificação terão comunicação para o IT através da internet e através de LTE, por onde se poderão reiniciar os vários componentes sem a necessidade de deslocação de uma pessoa ao local.

Por fim, também serão colocadas técnicas de segurança nas ligações entre os vários componentes e o servidor, para garantir a fiabilidade da informação e para a proteger de ataques indesejados.

3.2 Cobertura rádio

Para a cobertura rádio do projeto, temos de analisar quais os locais que irão ter cobertura rádio de cada uma das componentes:

O IEEE 802.11p será implementado com a seguinte cobertura de rádio:

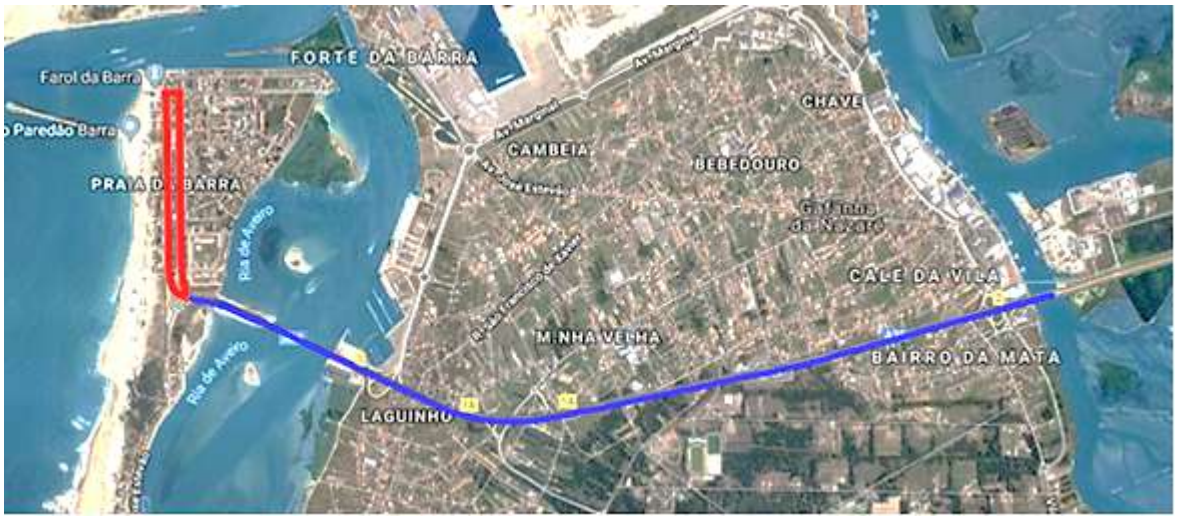


Figura 12 – Área com cobertura de rádio de IEEE 802.11p

Pode-se ver pela Figura 12 a área coberta por IEEE 802.11p, a abranger na primeira implementação do projeto que será implementado na A25 em toda a área de estrada que está demarcada com linha azul, e que deverá abranger desde o início da ponte da Barra mais perto do mar até à ponte da "Friopesca". A linha vermelha demarca as duas avenidas da Barra mais perto do mar, e essa área não vai ser desde já coberta com

IEEE 802.11p, mas, se o projeto for continuado, deverá ser uma das próximas áreas a ser coberta o protocolo.

Figura 13 – Área com cobertura rádio de Wi-Fi

A área a abranger por Wi-Fi será aproximadamente toda a zona de praia que está assinalada a vermelho, sendo que fora dessa área pode apresentar algum sinal, mas o serviço de internet poderá ser lento ou apresentar grandes falhas. Estando previsto os Access Points terem antenas omnidirecionais, prevê-se que toda a área da praia da Barra tenha Wi-Fi e a avenida mais próxima deverá apresentar também algum sinal, dependendo dos obstáculos presentes entre os bares de praia (locais onde serão colocados os APs) e essa avenida. Na praia da Costa Nova também se deverá verificar cobertura Wi-Fi em toda a área junto ao realçado a vermelho, prevendo-se que na área das estradas mais próximas haja algum sinal.

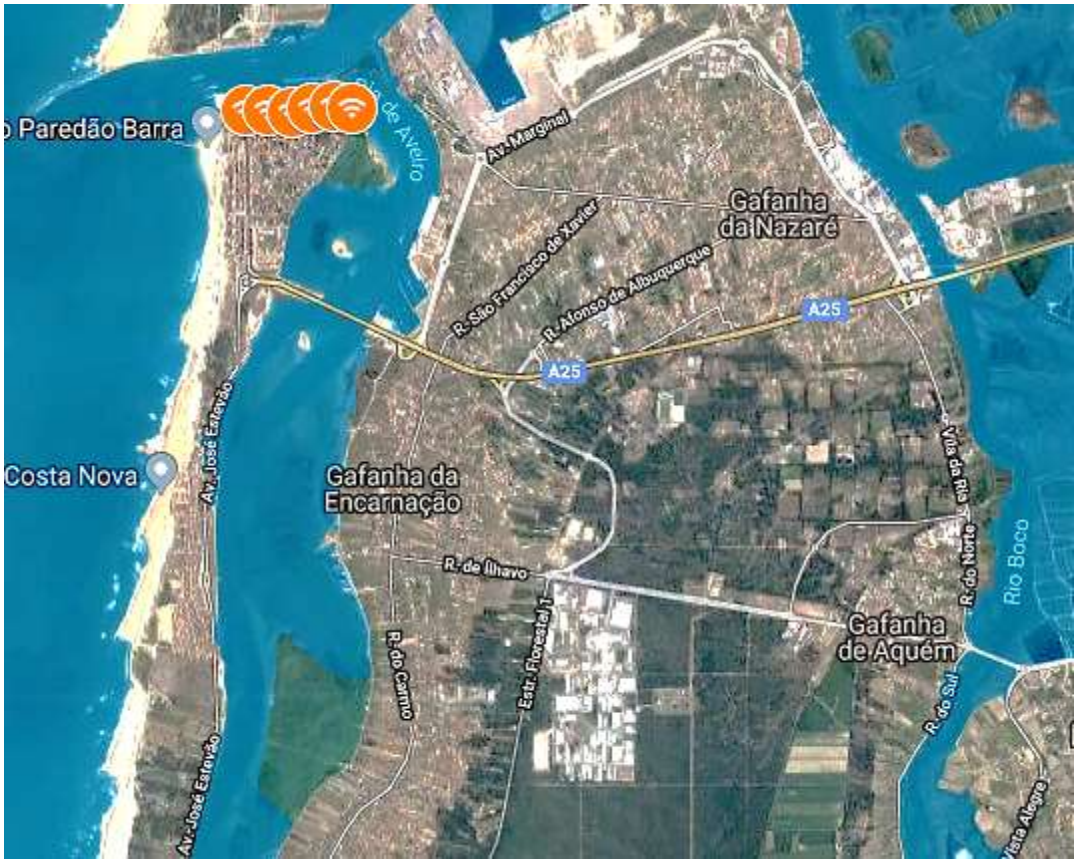


Figura 14 – Área com cobertura rádio de LoRa

A zona em que LoRa prestará serviço será toda a área presente na imagem. Para assegurar a cobertura, serão colocados alguns gateways espalhados pela Barra e será também feita uma cobertura mais intensiva no local que se encontra assinalado pelos símbolos laranja, em que serão colocados vários gateways de forma mais densa por ser a área de colocação dos sensores de estacionamento. Como estes se encontram junto ao chão, muitas vezes debaixo de carros e envolvidos em resina para os proteger, terão um alcance de comunicação bastante reduzido. Daí a necessidade de adensar a colocação de vários gateways num curto espaço.

3.3 Infraestrutura lógica

Na Figura 15 está representado um esquema da infraestrutura que será usada na plataforma.

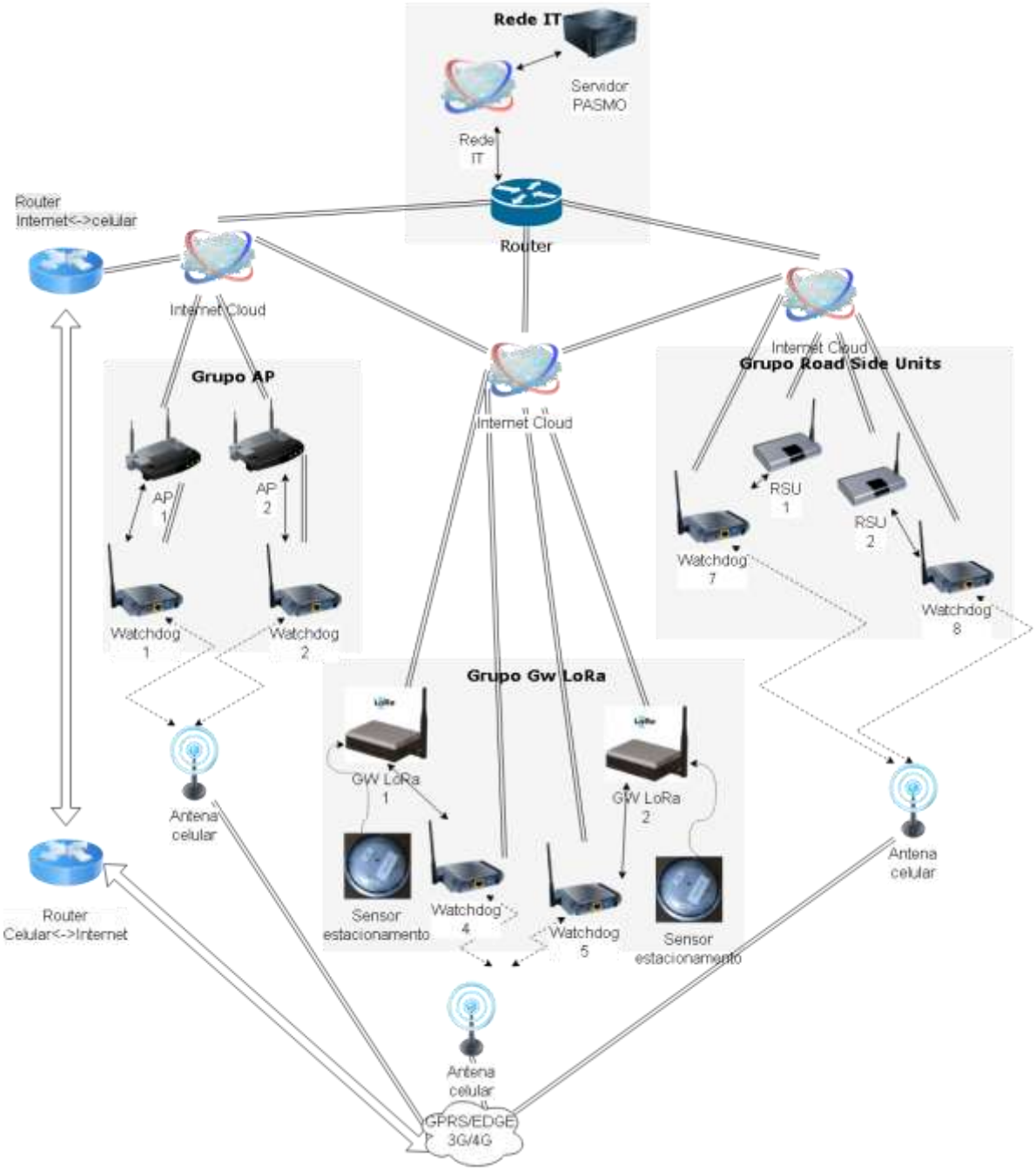


Figura 15 - Esquemático da infraestrutura lógica

Esta plataforma vai ser composta por três grupos distintos de serviço fornecido, instalados no local, que são:

1) O grupo dos APs (Figura 16) que vai fornecer Wi-Fi nas praias da Barra de Aveiro e da Costa Nova.

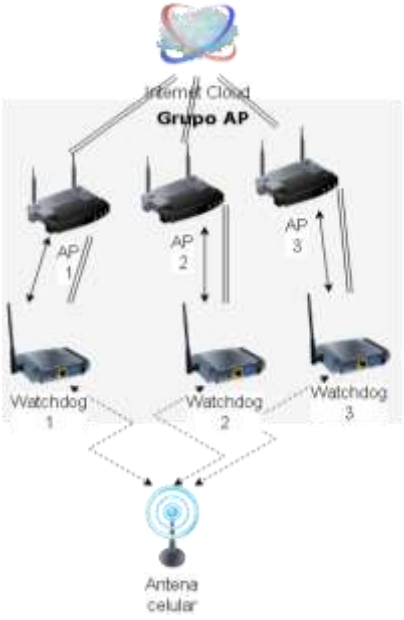


Figura 16 – Esquemático APs

2) O grupo de Gateways LoRa (Figura 17) que irá fornecer cobertura por toda a Barra de Aveiro e Costa Nova, e também será fornecido por este grupo os sensores de controlo de estacionamento e de controlo atmosférico. Esses sensores estarão ligados por LoRa aos Gateways.

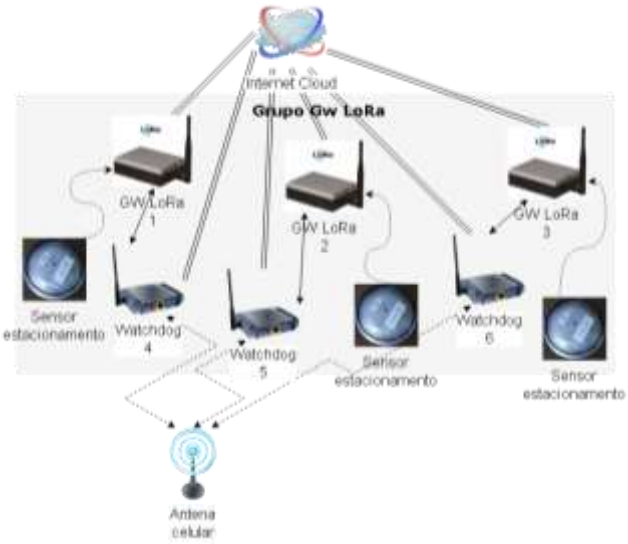


Figura 17 - Esquemático Gateways LoRa

3) O grupo de Road Side Units (Figura 18) será o que fornecerá a cobertura de IEEE 802.11p na A25.

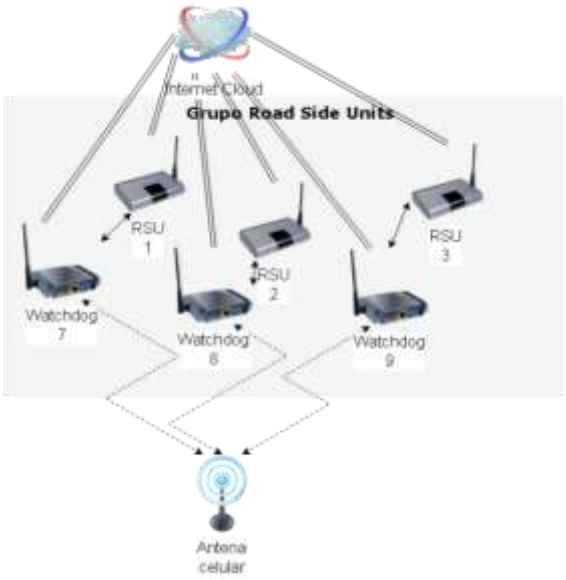


Figura 18 - Esquemático Road Side Units

Além dos dispositivos que fornecem serviço, estarão também watchdogs conectados a cada equipamento em todos os grupos. Estes servirão para garantir o bom funcionamento de cada componente da plataforma. Para se conseguir controlar o funcionamento da plataforma, todos os dispositivos estarão conectados a um servidor na rede do IT por internet. Além da conexão por internet, todos os watchdogs estarão equipados com comunicação celular, que será usada como rede de backup. Esta rede será usada no caso de haver problemas na conexão pela internet, assim permitindo comunicar com os watchdogs e com os componentes da plataforma.

Figura 19 – Rede IT

O servidor dentro da rede IT (Figura 19) terá os programas que permitirão a comunicação com todos os componentes pertencentes à plataforma, de onde se poderá controlar cada um deles, ver o seu estado e os registos de atividade que contenham.

3.4 Trabalhos semelhantes

Nos últimos anos tem crescido o interesse em implementar tecnologias que irão ser usadas em cidades inteligentes, o que aumentou o interesse de criar laboratórios vivos para desenvolver as várias tecnologias existentes e testar a sua resposta nos ambientes urbanos. De seguida serão apresentados alguns desses projetos:

- Smartsantander [15] é uma plataforma de IoT (Internet of Things), que fornece algumas vantagens do IoT aos cidadãos, é que além disso permite que qualquer empresa possa fazer testes de IoT de grande escala.
- DRIVE-IN [16] uma plataforma colocada no Porto para comunicações veiculares, em que os transportes públicos comunicam utilizando o protocolo IEEE 802.11p. Esta plataforma foi incluída no projeto Cidades Futuras [17], cujo objetivo é implementar naquela cidade outras tecnologias que possam vir a ser usadas em cidades inteligentes.
- A universidade de Michigan implementou um sistema de comunicação veicular na cidade de Ann Arbor [18], programado inicialmente para abranger perto de 9000 carros, mas já delineada para aumentar o número de carros pertencentes à plataforma.
- Na Eslovénia, na cidade de Liubliana, foi implementado o projeto AV living lab [33], que é focado em redes veiculares baseado em IEEE 802.11p. Este projeto aproveitou o fato da cidade ser relativamente pequena, o que reduz o investimento para cobrir toda a cidade, mas, como apresenta uma grande afluência turística, faz com que exista uma grande quantidade de pessoas a ajudar nos vários testes executados na plataforma. Além da rede veicular, este projeto também fornece IoT e câmaras de videovigilância, o que pode ajudar a obter informações mais detalhadas dos testes executados na plataforma sem ter de estar alguém presente.
- Na Espanha foi criado o projeto Catalonia living lab [34], por uma parceria entre o governo e várias empresas ligadas à mobilidade, envolvendo várias ruas espalhadas pela Catalunha. Para selecionar as ruas onde instalar a rede veicular, foi definido um conjunto de critérios de classificação de estradas e ruas, e, posteriormente selecionando aquelas que apresentavam valores mais elevados em pelo menos um dos critérios, assim possibilitando os testes serem executados em situações extremas o que garante uma maior fiabilidade da tecnologia usada para redes veiculares.
- Em Amesterdão foi criado o IoT living Lab [35], que é apenas focado em IoT, utilizando a tecnologia LoRa, com o objetivo de desenvolver soluções de IoT nas várias áreas onde pode ser usado.

Além destes projetos, foi criada em 2006 na Europa uma federação de laboratórios vivos chamada ENoLL[36] (European Network of Living Labs), que em 2014 já tinha mais de 340 projetos de laboratórios vivos aprovados, envolvendo laboratórios de várias áreas, em que uma delas é a área das smartcities.

Da área de smartcities tem vários living labs como:

- ❖ Synchronicity [45], em que o objetivo inicial é usar várias cidades voluntárias da Europa, como teste piloto de várias tecnologias IoT, levando a que posteriormente outras queiram implementar essas tecnologias, assim fazendo o desenvolvimento das tecnologias IoT mais rápido.

- Specify [46], que tem como objetivo o desenvolvimento da internet do Futuro, sendo focado no desenvolvimento das tecnologias de Fibra e wireless.
- ECIM [46], que é uma solução baseada na cloud, em que o objetivo é auxiliar as smartcities, aplicando o estado da arte das tecnologias nos serviços de transporte, tornando a mobilidade de pessoas e bens mais seguro, mais barata e mais amiga do ambiente.
- Periphéria [46], em que o objetivo é implantar plataformas e serviços que promovam estilos de vida sustentáveis pela internet do futuro.

Além destas, a ENoLL está presente em muitas mais plataformas de laboratórios vivos espalhadas pelo mundo todo.

4. Desenvolvimento de soluções para o projeto PASMO

4.1 Planeamento de cobertura

Nesta secção será explicado como foram feitos testes de desempenho de Wi-Fi e de LoRa, e as opções de localização dos gateways LoRa e dos APs aconselhadas com base nos resultados dos testes feitos.

4.1.1 Desempenho Access Point + LoRa

Desempenho Access Point

Para ver o desempenho dos APs, é preciso estudar a largura de banda e potência de sinal que eles apresentam a várias distâncias.

Para obter medições de forma a que os testes tivessem o mínimo de interferência não intencionada possível e um ambiente mais parecido com o local de posicionamento dos APs – proximidade do mar – foi escolhido um local onde se poderia colocar o AP a cerca de 5 metros de altura, sem obstáculos por perto, conseguindo linha de vista superior a 500 metros e sem casas.

A ausência de habitações é importante para evitar ruído causado por outros aparelhos que trabalhem com Wi-Fi, ou com outras tecnologias que usem a mesma banda de frequência.

O local selecionado, apresentado na Figura 20, dista cerca de 1km da localidade mais próxima e a casa de apoio visível na foto também dista mais de 400 metros de outras casas, assim apresentando pouco ruído não desejado.

O referido local também foi selecionado por ter mais fácil acesso pessoal, em detrimento do local onde serão colocados equipamentos, onde seria muito mais difícil obter condições para realizar o trabalho.

Figura 20 – Local de teste com Wi-Fi

Além das razões descritas, também o facto de conhecermos os donos da referida casa, e obtermos a sua permissão pesou para a seleção deste local para os testes de Wi-Fi. Explorou-se a altura da casa para se colocar o AP usado para os testes a cerca de 5 metros de altura. As medidas foram feitas a cada 50 metros, até uma distância máxima de 500 metros.

Figura 21 – Local de teste Wi-Fi imagem tirada entre os 475 e os 500 metros

Foi decidido não efetuar testes para além de 500 metros, dada a presença da duna presente na Figura 21, que poderia influenciar os resultados. Este monte de areia está localizado a cerca de 520 metros do local onde se coloca o AP.

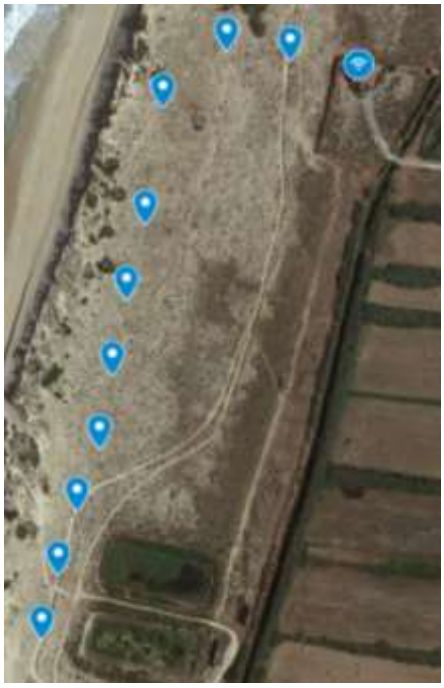


Figura 22 – Pontos dos testes de Wi-Fi

Os pontos indicados na Figura 22 foram os vários locais usados para os testes, a distâncias de 50, 100, 150, …, 450 e 500 metros do local onde se encontra o AP.

Os testes feitos para estudar o desempenho dos APs são de dois tipos:

a) Um deles consiste em, com apenas um computador ver as variações da largura de banda e de potência de sinal para várias condições de tempo.
b) O outro compreende a utilização de dois computadores, para fazer testes de largura de banda, de forma a avaliar quanto é que afeta ter mais de um computador ligado ao mesmo router.

Para executar os testes, foi utilizado um router wrt1200AC, posicionado a 5 metros de altura no local apresentado. Como o chão onde foram realizados os testes é irregular, todos os pontos de teste podem apresentar alturas ligeiramente diferentes em relação ao router, o que poderá influenciar os resultados.

Os testes com um computador (acima referidos na alínea "a)") foram executados com dois programas, que são o "iperf3" e o "Wi-Fi Analyzer".

Para executar o iperf3, o router estava conectado por cabo a um computador que servia de servidor, enquanto outro computador, este por sua vez cliente, foi tirando as medidas às várias distâncias indicadas.

O computador com função de servidor contém a placa de rede, Realtek PCIe GBE Family Controler, enquanto que o computador com função de cliente contém a placa de rede wireless, Intel(R) Dual Band Wireless-AC 3160. Os testes foram todos realizados nos 2.4GHz, de forma a testar a banda em que a maioria dos dispositivos atuais conseguem utilizar Wi-Fi.

Com o iperf3 obtiveram-se os valores de largura de banda transferindo pacotes UDP durante 10 segundos (foi usado os 10 segundos por ser o tempo definido por defeito para os testes de iperf), dos quais se apontou o valor

médio da largura de banda disponível. Para obter os valores apresentados abaixo, foi executada cinco vezes (é feita cinco repetições para se obter um valor mais próximo da média) a transferência de pacotes UDP em cada ponto escolhido e foi selecionada a média dos valores obtidos.

Os valores de potência de sinal foram obtidos a partir do software "Wi-Fi Analyzer" e foi registado o valor médio que se apresentava em cada ponto.

Existem quatro grupos de variáveis ambientais presentes no momento dos testes:

- Dia, condição temporal de dia sem chuva nem nevoeiro.
- Noite, condição temporal de noite sem chuva nem nevoeiro.
- Chuva, condição temporal de dia com chuva e sem nevoeiro.
- Nevoeiro, condição temporal de dia sem chuva, mas com nevoeiro.

Antes de se executar os testes pensávamos obter resultados de potência de sinal e de largura de banda com um decrescimento linear, que seria aproximadamente o mesmo de dia e de noite e mais acentuado nas condições de nevoeiro e de chuva. No final verificaram-se poucas diferenças, como se explicará.

Foi inicialmente pensado usar um simulador além dos testes em condições reais para comparar os resultados, mas, verificou-se ao fazer os testes que a variação dos valores de largura de banda e de potência de sinal era diferente. Como o interesse era saber até que distância se tinha uma largura de banda aceitável, o que não se obtém por simuladores, acabou por não se usar nenhum modelo teórico ou simulador.

Foram realizados vários testes a diferentes condições climatéricas, estando os resultados apresentados a seguir:

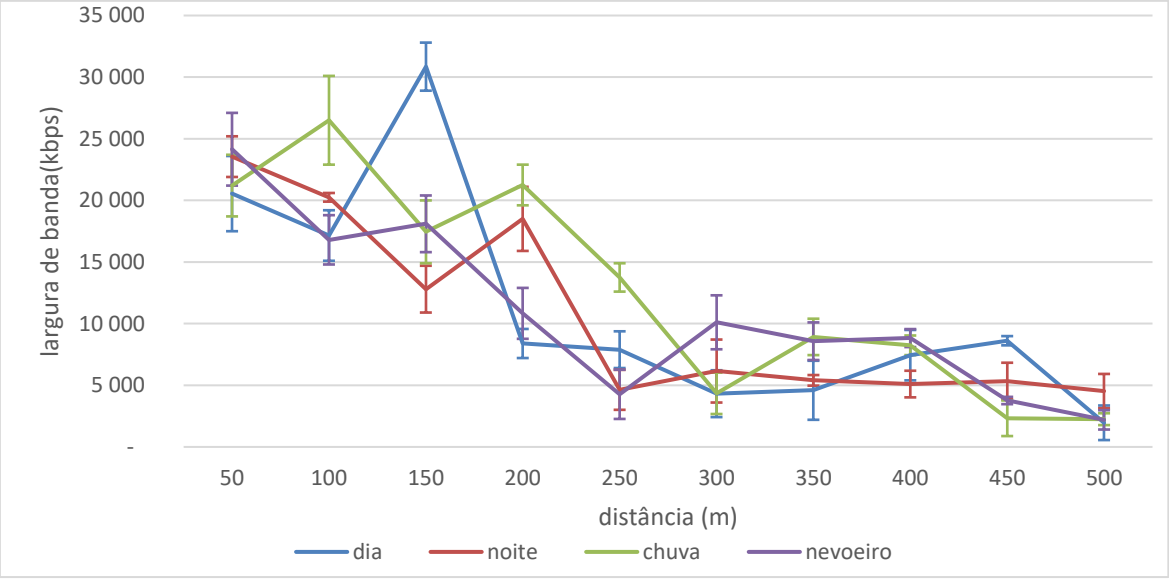


Figura 23 – Largura de banda medida nos vários pontos

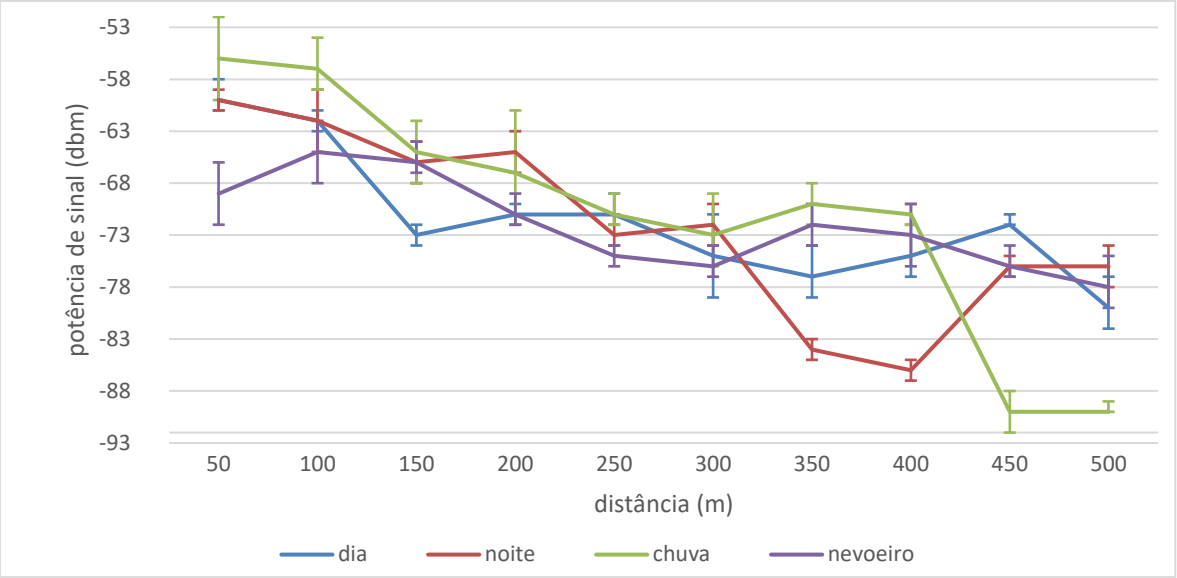


Figura 24 – Potência de sinal medido nos vários pontos

Analisando os gráficos acima, nota-se que não existe grande variação nos valores para as várias condições climatéricas e, pelo gráfico de largura de banda, conclui-se que a partir dos 200 metros os valores de largura de banda ficam muito reduzidos.

Como esperado inicialmente a potência de sinal apresenta aproximadamente um decrescimento linear, apesar de esse decrescimento ser quase constante para todas as condições climatéricas testadas (o que não se estava a espera, conforme já referimos). Além disso também se verifica nos dois gráficos anteriores, que a variação da potência de sinal é diferente da variação da largura de banda, apresentando esta um decrescimento mais linear até aos 200 metros e depois altera o declive a partir dessa distância (se não se considerar os picos de largura presente nos resultados).

Os valores de largura de banda foram obtidos com o programa "Wi-Fi Analyzer" aberto, tendo-se verificado mais tarde que afetava o valor obtido. Foram então realizados novos testes de largura de banda noutro dia. Nestes testes foram realizados durante um minuto e retirado o seu valor médio, para se obterem valores mais estáveis, e foram repetidas 3 vezes cada em cada local. Os valores do gráfico abaixo são a média dessas três medidas, assim obtendo o seguinte gráfico:

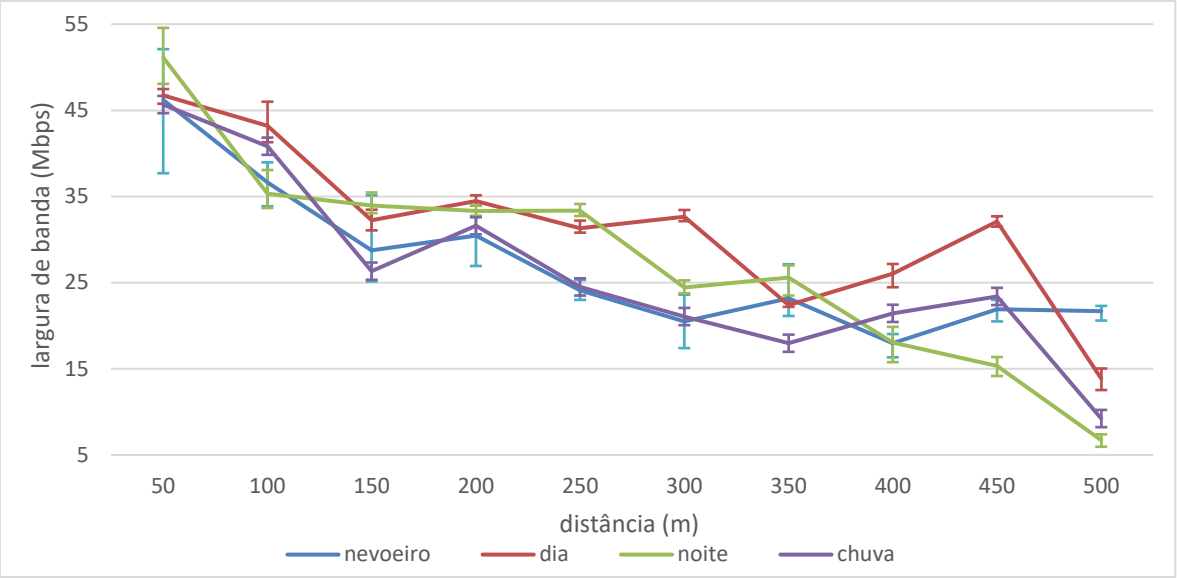


Figura 25 – Largura de banda medida nos vários pontos

Nestas medidas, em que não havia nenhum programa a afetar os resultados, consegue-se ver que existe uma largura de banda superior a 10 Mbps até aos 450 metros. Apesar de, com chuva e de noite haver menos que 10 Mbps aos 500 metros, ainda existe sinal e uma largura superior a 5 Mbps.

Para este teste o programa "Wi-Fi Analyzer" não estava aberto no computador cliente e os resultados já têm uma maior semelhança com os valores obtidos para a potência de sinal. Efetivamente, apresenta um decrescimento linear da largura de banda, sem grande variação dos valores para as várias condições temporais, como se visualizou nos resultados da potência de sinal.

Também se nota que as várias condições ambientais dos testes não afetam muito a largura de banda e o sinal, por isso a não ser em situações extremas (situações não testadas), é garantido um alcance de pelo menos 500 metros e até aos 450 metros tem-se pelo menos 10 Mbps de largura de banda.

O segundo tipo de teste, atrás referido na alínea "b)", serve para verificar o impacto da ligação simultânea de vários computadores na rede. Para isso fez se um teste com dois computadores a transmitir ao mesmo tempo quando estão à mesma distância, e outro quando apresentam distâncias diferentes do router.

Para este teste foram ligados dois computadores por cabo ao router, ambos como servidores, com as placas de rede Realtek PCIe GbE Family Controler e Realtek PCIe GBE Family Controler, respetivamente. Depois de se fazerem vários testes com computadores diferentes como clientes, verificou-se que o facto de ter dois computadores diferentes como clientes poderia afetar os resultados. Por isso, decidiu-se executar este teste com dois computadores iguais a servir de cliente, em que as placas de rede deles é Intel Dual Band Wireless-AC 8260. Por outro lado, para que os computadores que estavam a servir de servidor não afetassem os resultados nos clientes, em cada local de teste era executado o iperf3 duas vezes para um servidor e outras duas vezes para o outro.

Este teste foi executado no mesmo local que os testes anteriores, em que as condições climatéricas eram consideradas de "bom tempo" (sem chuva, nem nevoeiro e durante o dia).

Para estes testes verificou-se que se necessitava de cerca de 60 segundos para os valores serem mais estáveis. Por isso, cada valor indicado nos gráficos corresponde à média de 60 segundos a transmitir pacotes UDP com iperf3.

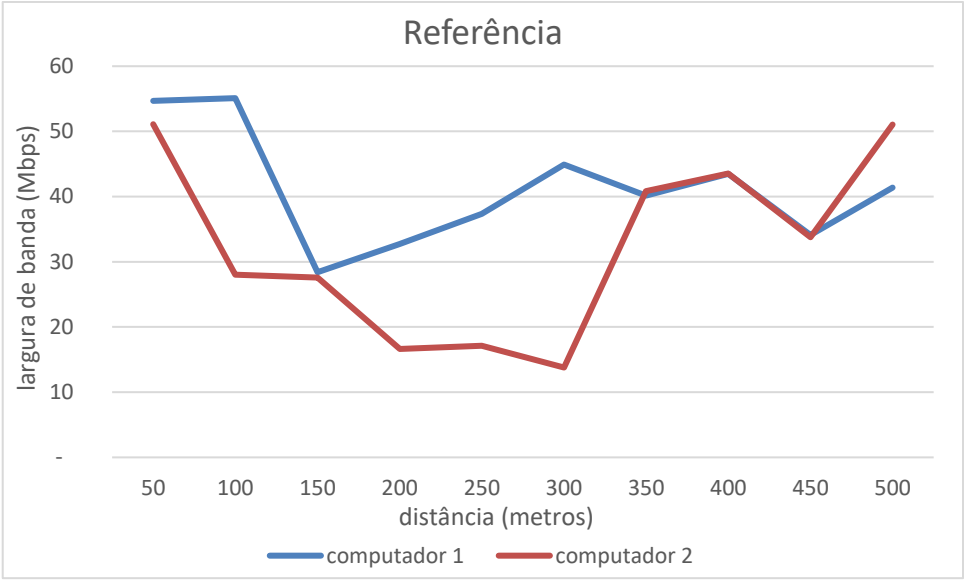


Figura 26 – Gráfico de referência dos computadores

O gráfico da Figura 26 serve como referência para os testes com os dois computadores, em que se faz o teste com cada um dos computadores separadamente. Verificou-se o decaimento dos valores de largura de banda entre os 150 e os 350 metros, mas não se conseguiu descortinar o motivo. Uma possibilidade será a negociação de bit-rate.

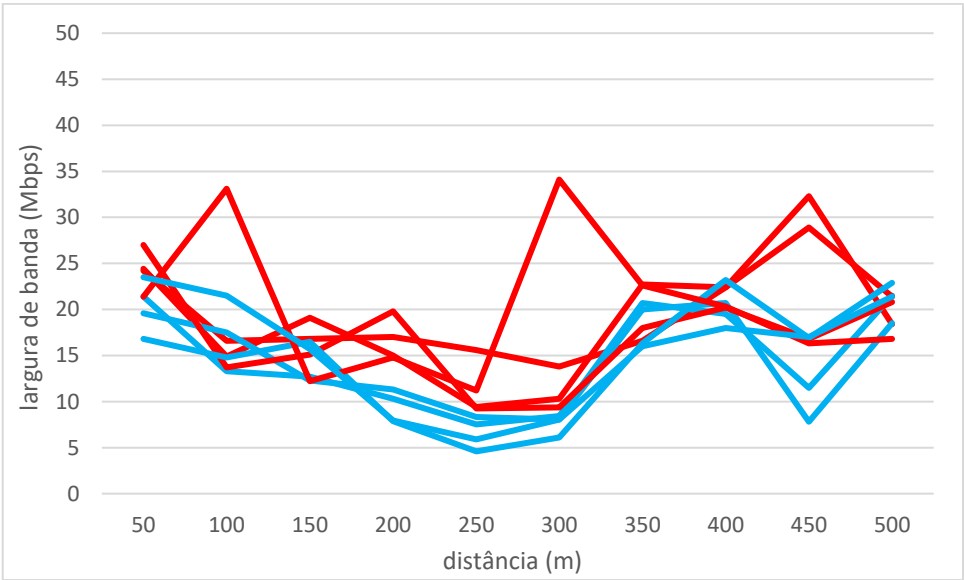


Figura 27 – Valores obtidos com 2 computadores a transmitir simultaneamente com o Wi-Fi sempre ligado

Representados no gráfico da Figura 27, estão a vermelho os valores obtidos por um dos computadores e a azul os valores obtidos pelo outro (sendo que os dados são obtidos com os dois computadores a transmitir em

simultâneo), notando-se, apesar dos computadores serem iguais, uma diferença de resultados. Os valores deste gráfico obtiveram-se sem desligar nenhuma vez o Wi-Fi durante todo o teste.

Como se pode ver pelos resultados, ao manter uma conexão durante todo o teste, a diferença de largura de banda entre os dois computadores é exígua, o que significa que o AP fez a negociação de largura de banda de forma a ser igualmente distribuída.

Foi realizado um segundo teste, em que se desligava o Wi-Fi quando se saia de um ponto e ligava-se de novo quando se chegava ao ponto seguinte. Assim a largura de banda teria de ser "negociada" entre o router e o computador quando se estivesse à distância do teste.

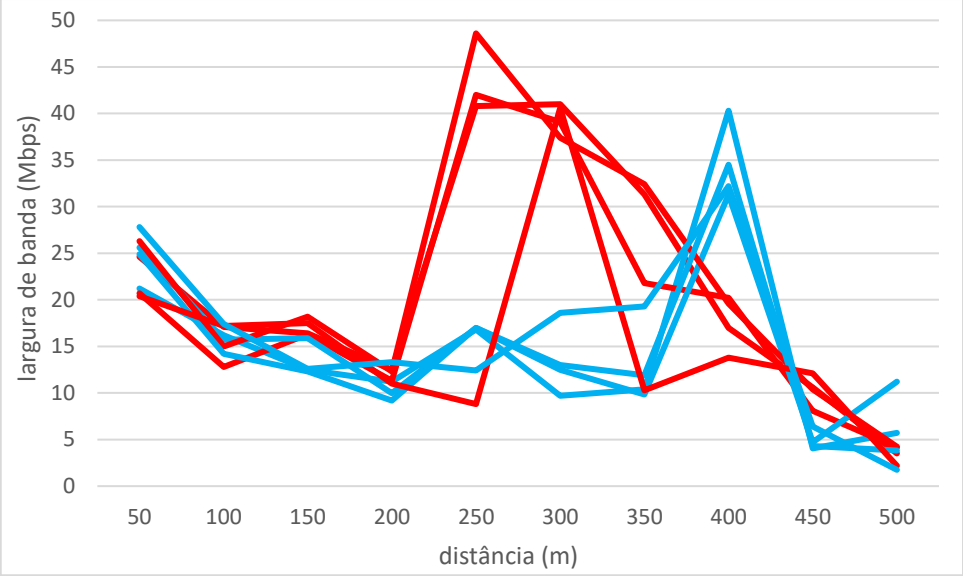


Figura 28 – Valores obtidos com 2 computadores com o Wi-Fi ligado em cada ponto

Os resultados deste segundo teste estão representados na Figura 28 e pode-se verificar que os valores obtidos são idênticos até aos 200 metros e que, dos 200 até aos 400 metros, os valores obtidos por ambos os computadores são bastante diferentes. Verifica-se que um deles apresenta sempre valores inferiores aos do primeiro teste, enquanto o outro apresenta valores muito superiores. Nos valores consegue-se visualizar que, em certos pontos entre os 200 e os 350 metros a diferença de valores entre os computadores pode chegar a ser de 4 vezes mais. Por fim, verifica-se uma diminuição grande da largura de banda a partir dos 450 metros em ambos os computadores.

Ao analisar os resultados nota-se que os valores são instáveis e podem variar de computador para computador mesmo que tenham especificações iguais. Mas também se pode concluir que se vai obter uma largura de banda útil até aos 500 metros.

Com os resultados obtidos ao ligar o computador ao AP apenas no local do teste, já se verifica que as larguras de banda são bastante discrepantes, o que pode ter sido provocada pelo facto de os computadores terem sido ligados em momentos diferentes. Tal facto pode levar o AP a fornecer a máxima largura de banda ao primeiro a conectar-se e, quando se liga o segundo, o AP fornece apenas a largura de banda disponível. Esta situação

também pode ser temporária, acabando os valores de largura de banda a estabilizarem num nível igualmente distribuído, obtendo-se os valores do primeiro teste.

Foram também executados testes com os computadores a distância diferentes, em que se obteve os seguintes resultados:

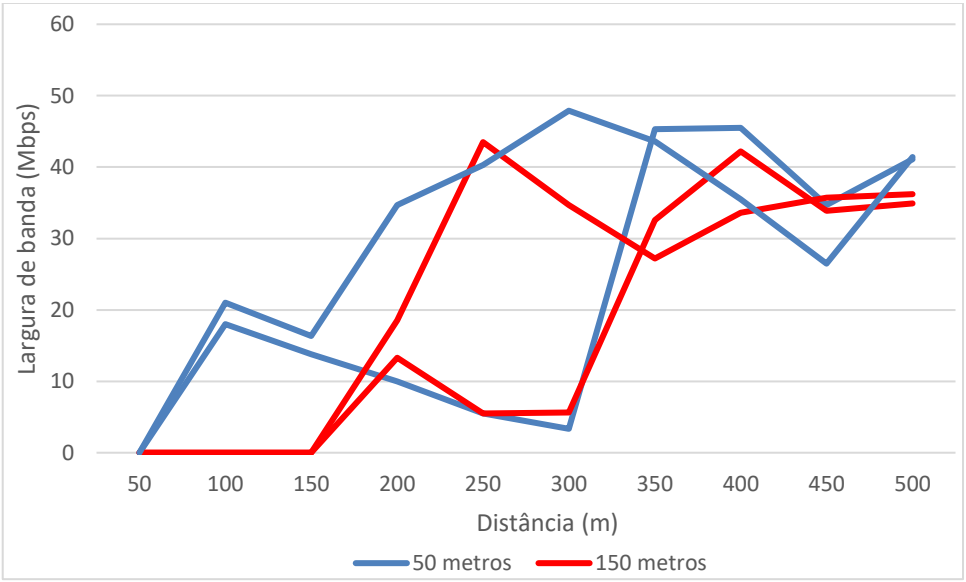


Figura 29 – Valores obtidos com 2 computadores a distâncias diferentes

Na Figura 29 estão representadas duas situações quando um computador está a 50 metros e a 150 metros do router e o outro se desloca, em que os valores presentes são os obtidos no computador que se desloca.

Pode se verificar que com o computador á mesma distância os valores obtidos aos 250 metros e aos 300 metros variam bastante. Isto porque uma vez os testes foram iniciados de perto do router para os 500 metros e na outra foi ao contrário. Estes resultados apoiam a situação que se pensa de que a negociação do bit-rate está a influenciar os resultados entre os 250 e os 300 metros. Esta situação poderá derivar de, pelo facto de o sinal estar a piorar, ser negociada uma largura de banda mais baixa, assim evitando falhas nas transmissões de pacotes.

Ao comparar estes valores com os valores de referência destes computadores nota-se que a maioria são inferiores, como era de se esperar. Mas está garantido que se vai ter um bom serviço nos 500 metros.

Desempenho LoRa

No estudo do LoRa foi usado um sensor e um recetor LoRa desenvolvidos pela empresa MicroIO.

Figura 30 - LoRa Sniffer

Figura 31 - Sensor LoRa (vista de cima e vista de baixo)

O Sniffer é equivalente ao recetor LoRa que a empresa MicroIO usa nos seus Gateways, mas com a facilidade de se conseguir conectar por USB a um computador, e se conseguir ver os pacotes que recebe diretamente num programa terminal no computador. O sensor está totalmente envolvido em resina para o proteger das condições adversas do tempo. Este sensor deteta se está debaixo de um carro ou não; para isso tem integrado um sensor que mede o campo magnético, que muda o valor que apresenta quando o metal da viatura está em cima, fazendo o sensor LoRa atuar. Este sensor está programado para transmitir quando, uma superfície metálica é colocada ou retirada de cima dele.

Para estudar o desempenho da tecnologia de comunicação LoRa, apenas interessa o alcance que se consegue transmitir com estes sensores. Apesar do protocolo estar desenhado para alcances na ordem dos milhares de metros, como os sensores de estacionamento estão localizados junto ao chão, muitas vezes debaixo de carros e envolvidos em resina, o alcance é bastante reduzido. Devido a essas condições o alcance esperado deverá rondar as poucas centenas de metros. Para estudar o alcance desses sensores, é preciso uma localização com linha de vista de algumas centenas de metros, posicionar o sensor sob uma viatura e ver até que distância se consegue receber os pacotes enviados pelo mesmo.

Para isso foram estudadas várias situações, consistindo a primeira em apurar qual o impacto no alcance em função da posição do sensor relativamente ao carro. Para fazer esse estudo decidimos estudar o impacto no alcance para cinco pontos do carro.

Na Figura 32 dá para ver os locais de colocação estudados, que são: à frente, atrás, no centro e em cada um dos lados, ao meio.

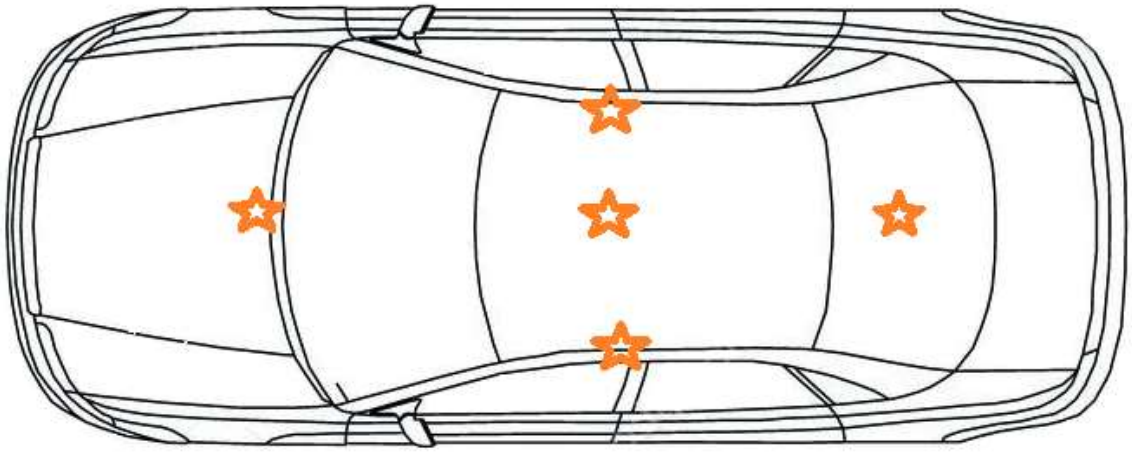


Figura 32 - Pontos do carro onde foi decidido colocar o sensor para o estudo

Depois disso foram feitos testes sob várias condições temporais em que se registou o estado de tempo (chuva, nevoeiro, noite e dia), a temperatura, a hora e a humidade, para ver se a variação destes parâmetros causa algum impacto ao alcance da transmissão do sensor.

Todos os testes executados são de 25 em 25 metros e é verificado qual é o alcance máximo para cada teste.

De forma a evitar a manipulação dos resultados dos testes de tempo com a variação da posição do sensor relativamente ao carro, começou-se por esse teste.

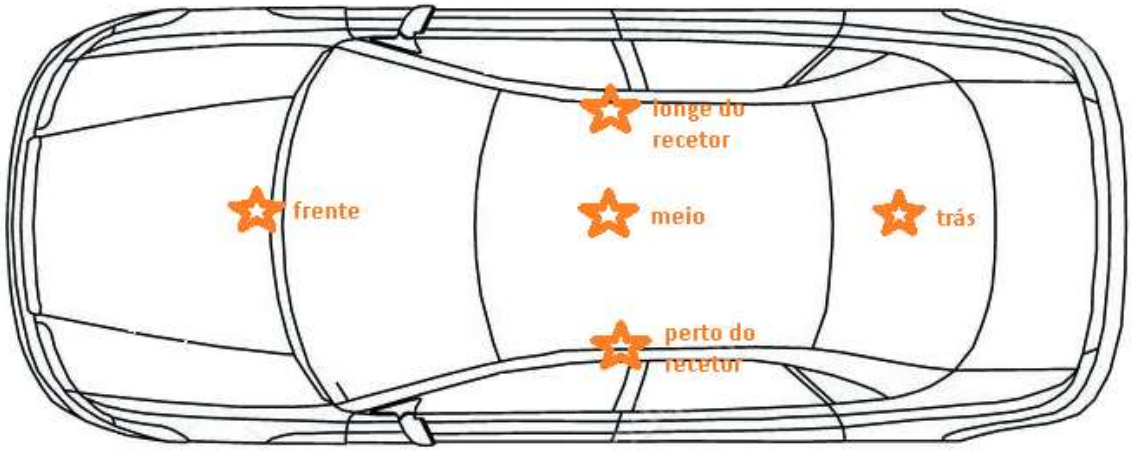


Figura 33 - Posições do carro estudadas com legenda

Usando a legenda de cada ponto presente na Figura 33 está presente a seguinte tabela com os resultados obtidos:

Frente	Longe do recetor	Meio	Perto do recetor	Trás
125 metros	100 metros	100 metros	+ 175 metros	125 metros

Tabela 4 – Medidas LoRa de posicionamento em relação ao carro

O último ponto deste teste foi aos 175 metros, visto que o único ponto que ainda transmitia não é muito relevante para estacionamentos.

Ao verificar os resultados do teste anterior verificou-se que os pontos da frente e de trás são os melhores para a colocação do sensor. Também se pode concluir que, as melhores posições para os sensores nos estacionamentos em espinha seria entre 0.75 a 1.25 metros do passeio, para garantir que ficam debaixo de qualquer carro, mas não ficam no centro do carro (pelo menos dos mais compridos). Para os estacionamentos em paralelo já se poderiam colocar entre 40 a 70 cm do passeio.

Após a verificação do alcance nos vários pontos do carro, fez-se outro teste em que se usou o ponto de trás indicado no teste anterior em todas as medidas. Neste teste estudou-se o resultado à variação de várias mediadas atmosféricas: a hora do dia, a temperatura, a humidade relativa e a condição atmosférica em que se obtiveram os seguintes resultados:

Tempo	bom tempo	noite	nevoeiro	dia	noite	dia	noite	noite nevoeiro	dia
temperatura	21º	18º	17º	33º	20º	24º	16º	13º	23º
humidade	76%	91%	93%	25%	65%	38%	76%	85%	47%
Hora	17h	1h	8h	15h	21h	16h	22h	2h	14h
Distância máxima	**100**	**150+**	**100**	**100**	**100**	**100**	**125**	**75**	**150+**
Tempo	noite	noite	noite	dia	dia	dia	noite	noite	dia
temperatura	13º	16º	16º	18º	23º	21º	19º	18º	22º
humidade	56%	85%	87%	81%	64%	72%	72%	73%	64%
Hora	0h	23h	4h	9h	14h	18h	0h	5h	10h
Distância máxima	**150+**	**100**	**150+**	**100**	**100**	**100**	**125**	**150+**	**125**
Tempo	noite	noite chuva	noite chuva	noite	dia				
temperatura	10º	11º	13º	10º	14º				
humidade	69%	98%	97%	88%	71%				
Hora	2h	1h	21h	4h	16h				
Distância máxima	**100**	**150+**	**150+**	**125**	**125**				

Tabela 5 – Medidas LoRa a várias condições temporais

Existem seis condições de tempo/luz nos testes que identificam a condição temporal em que foram feitos:

- Dia, condição temporal de dia sem chuva nem nevoeiro.
- Noite, condição temporal de noite sem chuva nem nevoeiro.
- Chuva, condição temporal de dia com chuva e sem nevoeiro.
- Nevoeiro, condição temporal de dia sem chuva, mas com nevoeiro.
- Noite chuva, condição temporal de noite com chuva sem nevoeiro.
- Noite nevoeiro, condição temporal de noite sem chuva com nevoeiro.

Este teste não foi feito a mais de 150 metros visto ter se começado a notar fracos resultados aos 100 metros. Foi considerado que não valia a pena ver distâncias superiores a 150 metros, por termos apurado o máximo de 100 metros, para que a comunicação fosse sucedida na maioria das vezes.

Ao analisar o resultado dos vários testes anteriores, verifica-se que a distância mínima obtida é 75 metros numa noite de nevoeiro, às 2h da manhã, com 13º de temperatura e 85% de humidade. Nessa noite o nevoeiro era tão intenso que a visibilidade máxima era de cerca de 30 a 50 metros. Considerando que este caso é um acontecimento raro, pode se verificar que temos maioritariamente um alcance de 100 metros ou superior. Assim sendo, podemos considerar que o alcance do sensor é sempre superior a 100 metros, exceto em condições extremas.

4.1.2 Seleção dos pontos de acesso

Para a seleção dos possíveis pontos de acesso, foi usado o "Google Maps" e identificados os vários estabelecimentos comerciais ou edifícios públicos. De notar que, apesar de estar assinalada uma loja ou edifício do governo nas imagens do "Google Maps", essas informações podem estar desatualizadas e não foi verificado se ainda se encontram neste momento lá, nem se os mesmos se encontram abertos.

Geo location Access point

Para escolher locais possíveis para APs na praia, procurámos construções que se assemelham a bares de praia, obtendo-se os pontos representados nas seguintes imagens.

Figura 34 – Possíveis locais para APs na Praia da Costa Nova

Figura 35 – Possíveis locais para APs na Praia da Barra

Dependendo dos resultados de desempenho do AP serão selecionados alguns dos locais identificados nas figuras Figura 34 e Figura 35, para a colocação dos APs.

Geo location LoRa

A colocação dos gateways LoRa é feita em estabelecimentos comerciais ou da administração pública localizados na Avenida Fernão de Magalhães, conforme demonstrado na seguinte imagem.

Figura 36 – Possíveis locais de posicionar gateways LoRa para os sensores de estacionamento

Ao analisar os locais obtidos, verifica-se que são relativamente poucos os locais possíveis para a colocação de gateways na metade mais a este da avenida, face à necessidade da sua proximidade antes exposta.

Com os locais identificados verifica-se que existe pouca escolha, devido a existirem poucos locais, fazendo com que os locais selecionados não irão variar muito com os resultados. Sendo que os dois pontos marcados á direita, estão considerando serem colocados no aldeamento triângulo Norte, pois para cobrir essa área deverá ser preciso dois Gateways. Apesar de tudo ao usar os locais indicados na Figura 36 poderá haver locais com falhas na cobertura.

Geo location IEEE 802.11p

A seleção dos pontos onde se colocam os Road Side Units do IEEE 802.11p foi feita de forma diferente da seleção para LoRa e para Wi-Fi. Na autoestrada, como existem pontos de fibra e eletricidade, foi negociado com a empresa Ascendi (concessionária da A25) a utilização dos mais adequados para o efeito.

Em resultado desses contactos os pontos disponibilizados são os presentes na seguinte figura:

Figura 37 – Possíveis locais para RSU na A25

Pode-se ver na Figura 37 que os vários pontos têm duas cores diferentes. Os pontos com cor verde, têm bastidores da autoestrada onde há eletricidade e fibra, enquanto que os pontos com cor azul têm telefones de apoio apenas com fibra.

Também se pode reparar que existem distâncias significativas, em que se não se colocar nenhum RSU, poderão resultar falhas de cobertura. Assim, irão ser colocados RSUs nos locais intermédios onde mais se justificam. Nos locais de instalação dos RSUs que não apresentem energia será preciso instalar painéis solares para alimentar os equipamentos e, nos locais que não apresentam fibra, será necessária uma conexão wireless para conectar os RSUs à internet.

Para a conexão à internet dos locais sem fibra, foram projetadas as seguintes conexões wireless:

Figura 38 – Conexões wireless ponto a ponto

As conexões ponto a ponto presentes na Figura 38 são feitas com um aparelho wireless com antena direcional, que permite conectar com o outro aparelho idêntico no ponto seguinte.

Assim ficam definidos os seguintes locais para colocação dos RSUs:

Figura 39 – Todos os pontos possíveis de colocar RSU na A25

4.2 Sistema de heartbeat

4.2.1 Conceito

Hoje em dia é bastante frequente qualquer pessoa lidar com dispositivos eletrónicos, sendo também crescente o uso de dispositivos com capacidade de processamento. Na utilização cada vez mais intensiva deste tipo de aparelhos, já todos tivemos situações em que o aparelho deixa de responder.

Há alguns anos via-se mais frequentemente quando o aparelho parava de responder e tinha de se desligar da fonte de energia e voltar a ligar para se conseguir retomar a atividade. Ultimamente já existem algumas seguranças de forma a evitar o total bloqueio do aparelho (por exemplo no caso dos computadores que quando surge um problema, em vez de ficarem bloqueados sem responder, aparece o tão conhecido "blue screen" e ele reinicia automaticamente). Apesar de essas seguranças serem cada vez mais comuns, existe sempre a possibilidade de esse tipo de segurança falhar, o que poderá levar o aparelho a ficar bloqueado.

Para obviar este tipo de anomalias que ocorrem nos dispositivos com processamento incluído, foi decidido criar uma segurança para o momento em que uma situação destas aconteça, de forma a evitar a deslocação de alguém ao local, para executar o reiniciar do aparelho.

Para resolução destas falhas de forma simples e rápida, propõe-se construir um sistema que faça o controlo de cada aparelho visado, verificando constantemente se está a funcionar normalmente. Caso o dispositivo não esteja a responder, o sistema de controlo obriga-o a fazer reset. Para isso há duas opções, uma por soft reset, em que existe uma ligação entre o sistema de controlo e o dispositivo visado, que o pode obrigar a reiniciar por essa ligação, ou por hard reset que o sistema de controlo desliga a eletricidade e volta a ligar de forma a forçar o aparelho a reiniciar. Para cumprir esta última função o sistema precisa de estar conectado ao aparelho a controlar e à sua fonte de energia, de forma a fazer o corte de energia quando necessário.

4.2.2 Circuito

Para controlar a fonte de energia é necessária a construção de um circuito eletrónico e, para que este circuito consiga evitar o máximo de falhas possíveis, é necessário antecipar que falhas podem acontecer. Esses

problemas podem consistir na falha do dispositivo, ou na do controlador do sistema de heartbeat, sendo que na segunda situação o circuito eletrónico necessita de fazer o reset ao controlador do sistema heartbeat. Para simplificar o circuito e reduzir componentes foi decidido sempre que o controlador do sistema heartbeat falhar será executado um hard reset ao dispositivo a controlar e ao próprio sistema heartbeat.

Para essa função, a entrada do circuito que está a controlar o hard reset recebe periodicamente do microcontrolador um pulso e, caso o dispositivo pare de responder ou caso o microcontrolador falhe, o pulso deverá parar de ser enviado, o que fará com que o circuite ative o relé que vai cortar a fonte de energia. Desta forma o circuito eletrónico tem de controlar o relé para permitir passar corrente no momento em que o sistema e o dispositivo são ligados e sempre que os pulsos apareçam com a periodicidade definida.

Na busca de um circuito que cumpra os requisitos e tivesse um tempo de cerca de 1min e saída ativa a VCC, feita no site da farnell [53], verificamos que os circuitos que cumpriam os requisitos tinham a saída ativa a 0V ou tempo demasiado reduzido. Então foi decidido contruir um circuito que cumpra todos os requisitos.

Para ter um circuito que respondesse às exigências apresentadas inicialmente foi pensado o seguinte esquema:

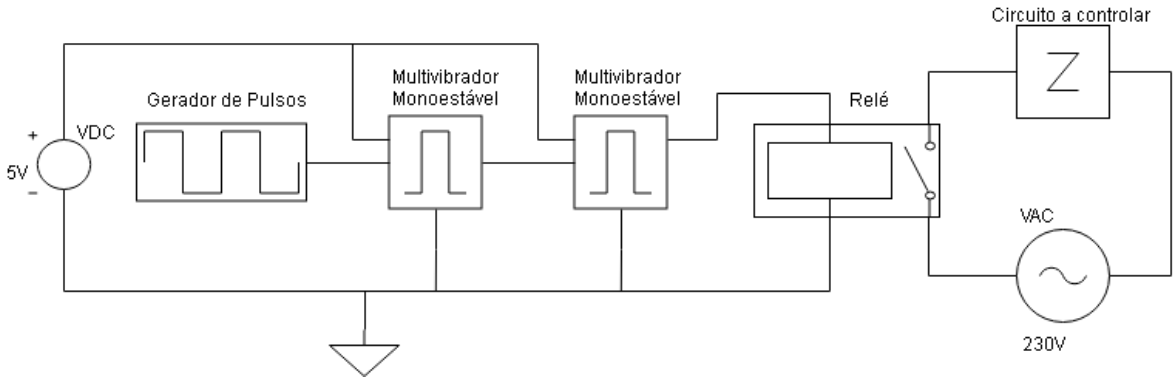


Figura 40 – Esquema do circuito inicial

No circuito constam dois multivibradores monoestáveis que respondem com um pulso na saída mediante a variação do valor da sua entrada, de maneira a ativar o relé caso o gerador de pulsos não esteja a enviar pulsos.

Os monoestáveis apresentam um pulso na saída sempre que a entrada apresenta variação do sinal de 0 para 1 ou de 1 para 0, dependendo de como estiver construído o circuito. O tempo do pulso da saída é controlada pelos valores de uma resistência e de um condensador.

No caso de o monoestável receber um pulso na entrada durante o decorrer de um pulso na saída, a contagem do tempo do pulso da saída volta a zero, sendo assim distendido o tempo do pulso que já tinha começado.

Assim, o relé apenas será ativado quando o segundo monoestável tiver um pulso na saída, o que apenas ocorrerá quando, o pulso do primeiro monoestável acabar, e que, por sua vez, apenas acontecerá se não receber nenhum pulso durante um espaço de tempo definido.

4.2.3 Implementação

Para a seleção dos componentes do sistema de heartbeat, é preciso saber que portas existem nos aparelhos principais presentes em cada um dos tipos de pontos que vão existir na plataforma. Há três tipos de dispositivos principais, que são os Access Points, as gateways LoRa e as RSUs.

Dependendo das portas existentes, define-se de que forma é verificado se os vários aparelhos estão funcionando normalmente. Será então possível saber que interfaces são exigidas no sistema de heartbeat.

Posteriormente será também necessário definir que tipo de sistema heartbeat se quer:

- Um sistema sem comunicação que apenas se limita a fazer controlo do funcionamento do dispositivo, e no caso de ocorrer problemas executa o hard reset ou o soft reset (se tiver disponível).
- Um sistema com uma comunicação simples que faz o controlo do dispositivo, mas que também envia algumas informações programadas, e permite que se possa pedir um reset remotamente.
- Uma outra opção, um controlador com um sistema operativo que vá além do que as outras opções oferecem, permitindo aceder remotamente e controlar todo o sistema de heartbeat e até, se necessário, alterar o programa que está a controlar o dispositivo.

No momento de desenvolver uma solução de watchdog para os equipamentos foram verificadas as opções comerciais como o WiReboot [54] e também se pesquisou por tomadas inteligentes, mas, todos os equipamentos que encontrámos não cumpriam todos os requisitos que se pretendiam. Os principais requisitos em falta eram: simultaneamente ter comunicação através da internet e por uma rede alternativa, poder obter informações da monitorização do watchdog e poder fazer o reset ao próprio watchdog.

Para além das informações anteriores, também vai ser apresentada na secção 5.2.3 como funciona a solução desenvolvida para um watchdog com sistema operativo. Nesta solução foi desenvolvido um programa para correr no sistema de heartbeat que funciona como watchdog para os APs, de forma a manter o AP a funcionar corretamente.

Serão indicados os meios de verificação usados no programa, de forma a controlar se o dispositivo está a funcionar devidamente ou não, e que decisões o programa toma em função dos resultados dessas verificações. Além disso, será exposto como é controlado o circuito desenvolvido pelas decisões do programa. Daremos ainda explicações de valores colocados em algumas variáveis que ajudam no decorrer do programa e como o watchdog irá reagir se, depois de um reinício, o erro que o motivou, volta a aparecer.

Por fim, serão apresentadas algumas soluções que aumentem a fiabilidade do sistema de heartbeat, protegendo-o de problemas causados por fatores externos.

4.3 Sistema de rede

4.3.1 Configurador

No configurador é preciso escrever um programa que consiga ter acesso a cada um dos watchdogs. Por o programa o utilizador deve conseguir:

- Reiniciar o watchdog;
- Ver registos de erros;
- Enviar ficheiros para os watchdogs;
- Ver o estado atual de erros;
- Controlar todo o sistema heartbeat.

Levando isto em consideração, na secção 5.3.1, será apresentado qual o resultado final da interface gráfica desenvolvida para controlar os vários watchdogs presentes na plataforma.

Sobre essa interface gráfica será apresentado na mesma secção: o seu aspeto, quais as interações que o utilizador tem disponível, quais as funcionalidades que cada interação apresenta e a resposta para cada interação. Será também apresentado alguns motivos das decisões tomadas na interface, e quais interações estão implementadas entre a interface gráfica e os programas que controlam o funcionamento de cada watchdog.

Além do mais será explicado quais as ferramentas usadas para o funcionamento do programa.

4.3.2 Rede Backup

Nas situações em que a internet falha por causa de problemas na rede ou de anomalias nos APs, por eles não fazerem o encaminhamento dos pacotes, convêm existir uma forma alternativa de comunicar com o sistema heartbeat. Para ser possível identificar o problema e tentar resolvê-lo, sem a necessidade de deslocação ao local optou-se por colocar uma conexão alternativa dos watchdogs ao servidor.

Para essa conexão, pensou-se na possibilidade de usar qualquer uma das tecnologias presentes na seguinte tabela, onde serão apresentadas as vantagens e desvantagens de cada uma.

Tecnologia	**LoRa**	**GSM**
Vantagens	– Não precisa subscrição – Baixo consumo energético – Toda a comunicação pode ser feita dentro da rede do pasmo	– Consegue ter conexões mais complexas – Transferência de dados rápida – A limitação das interações depende de como for feita conexão – Menor latência
Desvantagens	– Transferência de dados lenta ou poucas quantidades – Limitadas interações – Conexões simples	– Precisa de subscrição pagamento mensal – Limite de dados mensal dependendo da subscrição

Tabela 6 – Tecnologias para rede backup

A grande vantagem do LoRa é, no caso de não estar a ser usada, não existirem custos adicionais na plataforma, enquanto que no GSM tem de se manter a subscrição com a operadora e tem um custo mesmo quando não é necessária.

A tecnologia selecionada para a rede de backup foi a GSM, por fornecer uma maior liberdade na comunicação, o que permite ao utilizador ter uma maior quantidade de interações e também uma latência menor por não ter a restrição de dados que o LoRa apresenta e, por outro lado, ter maior largura de banda disponível, o que constitui uma grande vantagem face ao LoRa.

Estando selecionada a tecnologia a usar, será explicado na secção 5.3.2 como funciona a extensão do raspberry pi que fornece conexão GSM e GPRS. Além da explicação sobre a extensão, irá ser explicado como foi desenvolvida a rede de backup, que restrições apresenta e como faz a comunicação entre o configurador e a extensão do rapsberry.

Na comunicação pela rede de backup será necessário poder fazer o seguinte:

- Reiniciar o watchdog;
- Ver registos de erros;
- Ver o estado atual de erros;
- Poder controlar grande parte do sistema heartbeat.

5. Resultados

5.1 Análise cobertura e seleção dos pontos de acesso

Os testes feitos para o planeamento foram ortodoxos, pois podíamos ter usado simuladores para saber a cobertura, que seria um processo mais simples. Porém, foi usado este método pelo facto dos simuladores não apresentarem a largura de banda que um AP fornece às várias distâncias e, no caso do LoRa, como era um sensor específico numa situação muito peculiar, era difícil obter bons resultados por simuladores.

O planeamento feito não usa a metodologia clássica em que, além da previsão teórica, se faz o "site survey", pelo facto das coberturas de LoRa e do 802.11p serem destinadas a estradas sem grandes obstáculos nem grandes variações de altitudes. Para o caso do Wi-Fi, como é na praia e o terreno está em constante alteração devido ao movimento da areia com o mar e com o vento, e também pelo facto da altura desde os bares de praia até ao mar baixar constantemente, não se fez o "site survey". O resto dos espaços que são cobertos pelas tecnologias não têm grande importância no projeto.

Para selecionar os locais de colocação dos APs, analisamos os resultados obtidos nos testes do AP e foram escolhidas duas opções: a distância máxima entre AP e uma distância confortável aproveitando o alcance, mas não maximizando de forma a evitar falhas de rede em condições mais adversas do que as testadas.

Então para a distância máxima foi usado um alcance de 500 metros, obtendo uma distância máxima de 1 km entre cada AP e, uma distância confortável de 200 metros de alcance, o que seria no máximo 400 metros entre cada AP. Foi escolhida, a distância favorável de apenas 200 metros, para evitar que o número de aparelhos que tentem ligar a um AP seja superior ao número máximo que ele suporte.

Na seleção dos locais para a colocação dos Gateways LoRa, considera-se que o alcance máximo é de 100 metros, sendo um máximo de 200 metros entre cada Gateway. Considerando esse limite, foram então selecionados os locais onde se podem colocar os Gateways, que serão apresentados mais à frente.

5.1.1 Geo location AP opção 1

Na seleção dos pontos para os APs tivemos de nos restringir aos locais identificados no segmento Geo location Access point da secção 4.1.2.

Figura 41 – Localização e cobertura dos APs na Praia da Barra para alcance de 500 metros

Locais dos APs
Restaurante Barra Mar
Salina Club

Tabela 7 – Nome dos locais selecionados Barra

Pode se ver na Figura 41, em que foram selecionados os locais com o nome na Tabela 7, a cobertura que se obteria ao colocar 2 APs e considerando um alcance de 500 metros para cada AP, se toda a zona dentro dos círculos tivesse linha de vista para os APs. Devido à presença de edifícios, dunas e outros obstáculos, apenas deve estar correto a cobertura feita na zona da praia, a parte urbanizada deverá apresentar falhas de sinal mesmo dentro dos círculos que representam a cobertura.

Figura 42 – Localização e cobertura de APs na Costa Nova para alcance de 500 metros

Locais dos APs
Costa Nova Beach Club
Ambiente Bar

Tabela 8 – Nome dos locais selecionados Costa Nova

Como explicado para a figura que representa a Praia da Barra, a Figura 42 demonstra a cobertura da Praia da Costa Nova, ao posicionar os APs nos estabelecimentos cujo nome está na Tabela 8. Também dá para ver a zona que deve ser coberta, sem esquecer que poderá haver falhas de sinal em qualquer zona que não apresente linha de vista para os APs.

Utilizando esta opção, pode se verificar pelas imagens acima que apenas se usam 4 APs para conseguir colocar cobertura de Wi-Fi na Praia da Barra e na Praia da Costa Nova. Esta solução é a mais barata, mas como exige que cada AP faça a cobertura de uma grande área, pode fazer com que tenha mais aparelhos a tentarem-se conectar do que os que consegue suportar. Isto pode causar falhas no serviço, não fornecendo internet a todos os utilizadores que desejem utilizar.

Esta solução também utiliza o máximo alcance testado às várias condições, o que deve garantir cobertura na maior parte das condições atmosféricas. Mas, poderá vir a apresentar falhas em condições mais adversas do que as testadas, pois não se sabe a margem entre os 500 metros considerados e o alcance máximo nas várias condições atmosféricas testadas.

5.1.2 Geo location AP opção 2

Na seleção dos pontos para os APs tivemos de nos restringir aos locais identificados no segmento Geo location Access point da secção 4.1.2.

Para esta solução consegue-se ver pelas duas seguintes imagens a localização dos APs no caso de cada AP ter um alcance de 200 metros, e qual é a área que cada AP deverá abranger.

Figura 43 – Localização e cobertura dos APs na Praia da Barra para alcance de 200 metros

Figura 44 – Localização e cobertura de APs na Costa Nova para alcance de 200 metros

Barra
Farol
Restaurante Barra Mar
Bar offshore 2n Aveiro
The Beach House
Salina Club
Costa Nova
Costa Nova Beach Club
Assalam – Bar de praia
Ambiente Bar

Tabela 9 – Nome dos locais selecionados Costa Nova

Como se pode ver pelas imagens, para se fazer a cobertura em que se considera que os APs têm um alcance de 200 metros, serão precisos 8 APs para cobrir ambas as praias.

Apesar de esta solução necessitar de mais APs em relação à anterior, tem a vantagem dos APs fazerem a cobertura de uma área menor, o que torna menos provável haver mais dispositivos ativos na área do que os que o AP consegue suportar. Além disso, como nos testes feitos está garantido que os APs devem conseguir pelo menos 500 metros de alcance, fica uma margem de 300 metros entre o alcance testado e o alcance usado, por isso é muito menos provável haver falhas de sinal por condições mais adversas do que as testadas. Além disso como tem uma margem de 300 metros não usados, apresenta redundância que no caso de um AP falhar, a área continua a ser abrangida com sinal dos APs adjacentes.

5.1.3 Geo location LoRa

Na seleção dos pontos para os Gateways LoRa tivemos de nos restringir aos locais identificados no segmento Geo location LoRa da secção 4.1.2.

Considerando o alcance de 100 metros de cada Gateway LoRa foram escolhidos os pontos presentes na seguinte figura:

Figura 45 – Pontos selecionados para a localização dos Gateways LoRa

Marito-snack-bar Unipessoal Lda.	Barba Azul, The Sushi House	Pizzaria Brasão	C.A.S.C.I. - Centro de infância da Barra	Aldeamento Triangulo Norte	Aldeamento Triangulo Norte

Tabela 10 – Nome dos locais selecionados para gateways LoRa

Pela imagem acima, consegue-se ver os pontos selecionados para cada Gateway e a sua cobertura para os sensores de estacionamento, em que os nomes dos locais selecionados estão presentes na Tabela 10. Como havia uma grande limitação do número de locais que se podiam selecionar para os Gateways, não é possível apresentar várias soluções. Mas, esta solução fornece cobertura para toda a rua, garantindo um gateway a cobrir cada zona da rua considerando o alcance de 100 metros.

5.1.4 Geo location IEEE 802.11p

Na seleção dos pontos para os RSUs tivemos de nos restringir aos locais identificados no segmento Geo location IEEE 802.11p da secção 4.1.2.

Como outros colegas fizeram testes aos RSUs usados para a plataforma onde foi medido o seu alcance, que concluíram ser cerca de 500 metros, optou-se por não ultrapassar 500 metros de alcance para a plataforma. Com o alcance de 500 metros foram selecionados os pontos, que se vêm na imagem seguinte, bem como a cobertura fornecida.

Figura 46 – Pontos selecionados para a localização dos Gateways LoRa

1-Início ponde da Barra lado do mar	2-Início ponte da Barra lado de Aveiro	3-Junto a placar indicativo de localidades	4-Ao lado a ponte da R. Afonso de Albuquerque	5-Ao lado de placar eletrónico
6-km 3.5 da A25	7-A meio da estação de serviço	8-No telefone de apoio SOS	9-Bastidos km 4.85 da A25	10-Junto á primeira entrada da Gafanha da Nazaré

Tabela 11 – Identificação dos locais selecionados para os RSUs

Como se pode ver, com a cobertura dos 500 metros existe grande sobreposição, isto permite evitar falhas de cobertura o máximo possível, mesmo para condições bastante adversas. Como as redes veiculares são para ser usadas como uma forma de segurança, convêm que não existam falhas independentemente das condições do tempo.

5.2 Sistema de heartbeat

5.2.1 Circuito

Para construir o circuito pensado inicialmente e que está representado na Figura 40, comprou-se a lista de componentes presentes no anexo 1.i. Com estes componentes e usando ainda resistências e condensadores disponíveis na Universidade, fizeram-se os testes necessários para o circuito.

Montou-se, assim, o seguinte circuito:

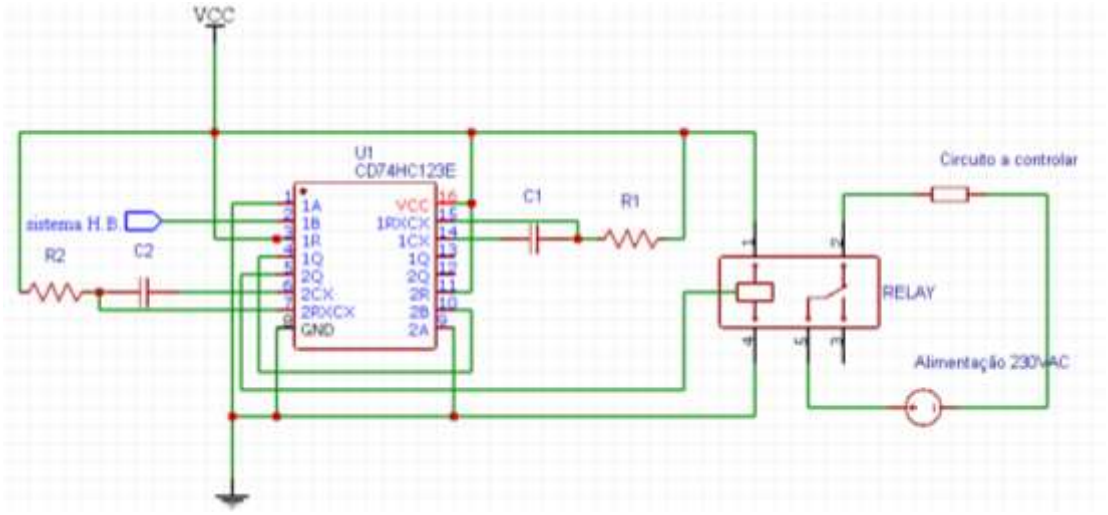


Figura 47 – Circuito inicial

Depois de se montar o circuito da Figura 47, verificou-se que, sempre que se ligam os condensadores estão descarregados (como é normal). Devido a isso tanto a saída do primeiro como do segundo monoestável apresentam logo um pulso inicial, que é igual ao tempo de carregar os condensadores. Esta ocorrência provocava corte de eletricidade ao ligar o circuito, pois era indicado ao relé para cortar a energia, desligando todo o sistema. Assim sendo, teve de se alterar o circuito de forma a que esta situação fosse resolvida.

Para resolver essa situação idealizaram-se dois circuitos diferentes:

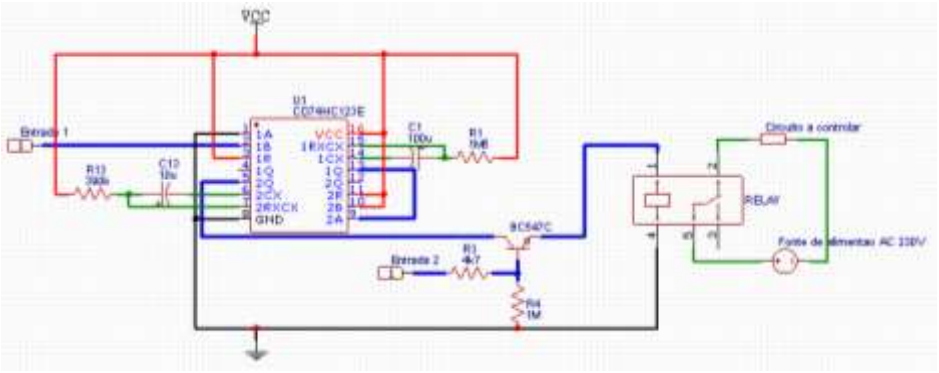


Figura 48 – Circuito final primeira solução

O primeiro circuito idealizado está apresentado na Figura 48. Nesta solução fez-se com que o transístor não deixasse passar sinal nos primeiros segundos até que o segundo monoestável acabasse o pulso gerado ao ligar o circuito e, a partir desse momento, o transístor deixava que o circuito funcionasse normalmente. A resistência R4 é necessária para o bom funcionamento do transístor, enquanto que a resistência R3 serve apenas para que o circuito apresente mais estabilidade. Esta solução consistiu em colocar o transístor para resolver o problema inicial com software.

Este circuito é uma possível solução, mas não é a melhor, pois exige uma grande quantidade de componentes, duas entradas e complica o entender do funcionamento do circuito. Por isso, mais tarde chegou-se a uma segunda solução, mais simples e que não depende do transístor, nem de duas entradas.

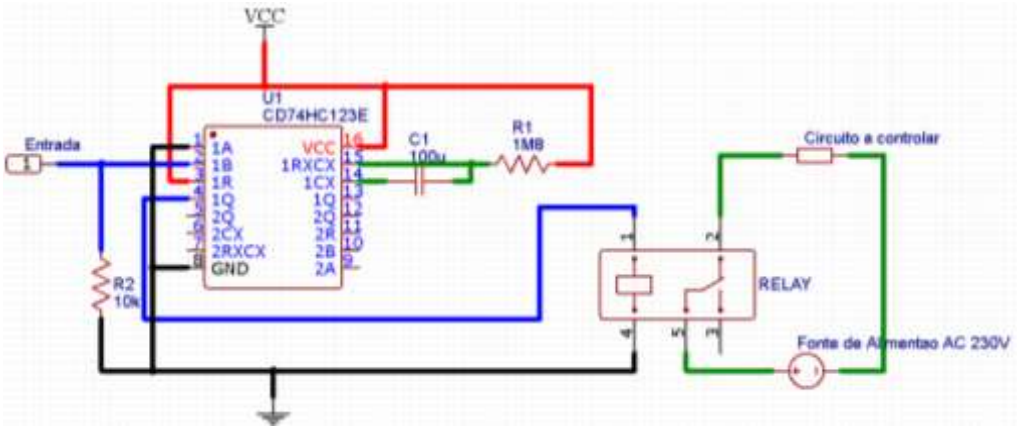


Figura 49 – Circuito final segunda solução

Nesta solução usa-se o pulso inicial, devido à sua duração ser mais de um minuto que é superior ao tempo necessário para um microcontrolador ligar (momento desde que é ligado à corrente até finalizar o processo de ligar). Concluiu-se que dava para usufruir do pulso inicial, que demora mais tempo do que o tempo definido para o pulso normal, devido ao facto de o condensador estar totalmente descarregado. Caso o microprocessador ou single board computer usado para controlar o circuito tenha um tempo de arranque muito próximo ou superior ao tempo do pulso inicial, esta solução já não seria possível, podendo ser corrigida com o transístor antes do relé, como consta na primeira solução.

Depois de testar o circuito já na solução integrada, notou-se que muitas vezes a entrada ficava sem valores definidos. Se o controlador não colocar o pino num valor constante. Nesse caso, a entrada fica sem valor definido e o circuito considera que na entrada está sempre a receber pulsos, dando origem a que o relé nunca corte a energia e o watchdog não funcione corretamente. Para resolver esse problema foi adicionada uma resistência de 10kΩ a ligar a entrada do circuito à massa, evitando assim que a entrada fique sem valor definido nessas situações.

Posteriormente fizeram-se vários testes dos valores do condensador e da resistência até o tempo se aproximar do desejado e, ao fim desses testes, verificou-se que com um condensador de 100µF e uma resistência de 1.8MΩ teríamos um valor de tempo de pulso próximo do desejado. Assim sendo, os materiais para construir este circuito são os presentes no anexo 1.ii.

Depois de se conseguir obter o circuito, com os tempos desejados, fez-se o seu estudo, para ver a forma como reagia em cada situação. Para isso usou-se um osciloscópio com 2 pontas de prova, em que cada ponta apresenta uma resistência de 10MΩ. O osciloscópio usado é o Tektronix TBS 1052B-EDU. Para executar os testes do circuito e ver a resposta do mesmo usou-se um Arduíno UNO. Assim sendo, os pontos estudados foram o da saída do monoestável que liga ao relé e o ponto de ligação entre o condensador e a resistência.

Para gerar os pulsos de controlo do circuito usaram-se as seguintes linhas de código:

digitalWrite(2, HIGH);

delayMicroseconds(10);

digitalWrite(2, LOW);

O que estas linha de código fazem é colocar a entrada do circuito a 5V, esperar 10µs e voltar a colocar a entrada a 0V. Assim, o Arduíno gera um pulso com uma duração um pouco superior a 10µs.

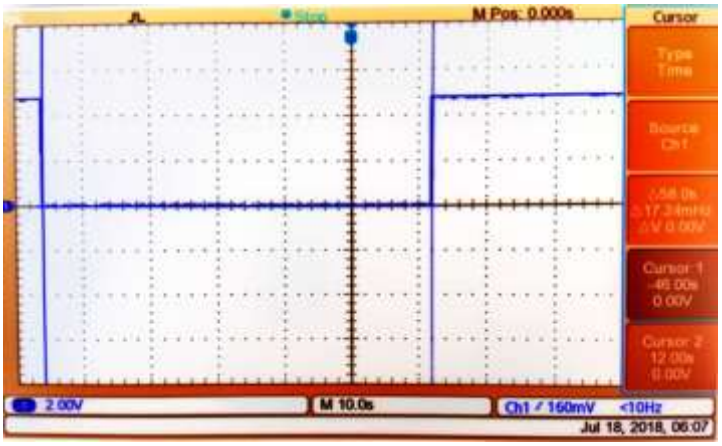


Figura 50 – Resposta na saída a um pulso

Pela Figura 50 dá para ver o tempo que demora o pulso do monoestável que é de 58seg (pode-se ver o tempo na imagem no Δ58.0s que indica o tempo entre os dois cursores no ecrã – retas verticais azuis). Depois do último pulso do Arduíno o circuito espera 58 segundos até ligar o relé para cortar a corrente, obrigando o hard reset de todos os circuitos controlados pelo sistema heartbeat.

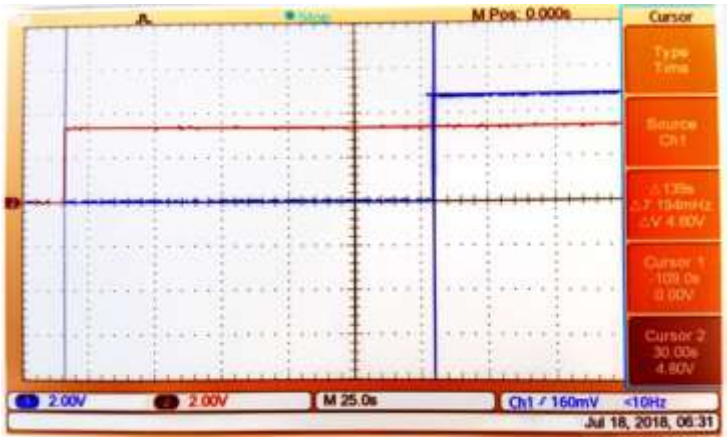


Figura 51 – Tempo do pulso quando o circuito é ligado a energia, a ponta de prova 2(vermelha) está ligada aos 3.3V do arduino para identificar momento em que é ligado

Olhando para a Figura 51, consegue-se ver o tempo mínimo, desde que o circuito é ligado à energia, até se poder ligar o relé para cortar a energia. Como se pode ver, este pulso tem uma maior duração que o pulso do monoestável, pelo facto do condensador começar completamente descarregado

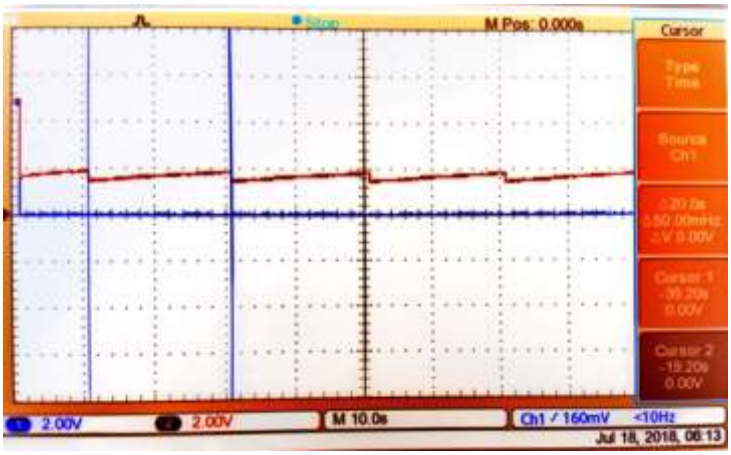


Figura 52 – Resposta da saída (linha azul / ponta de prova 1) e do ponto entre o condensador e a resistência (linha vermelha / ponta de prova 2) a pulsos gerados a cada 20 segundos

Na Figura 52, está representada a forma como a saída responde (linha azul) e como reage o circuito no ponto em que o condensador liga a resistência (linha vermelha), quando na entrada são aplicados pulsos a cada 20 segundos. Pode-se verificar que entre os pulsos, o condensador está a carregar e no momento que atinge os 5V o pulso irá acabar. Ao aplicar outro pulso na entrada durante o pulso na saída, verifica-se que o condensador volta ao ponto inicial fazendo com que o pulso dure mais 58seg.

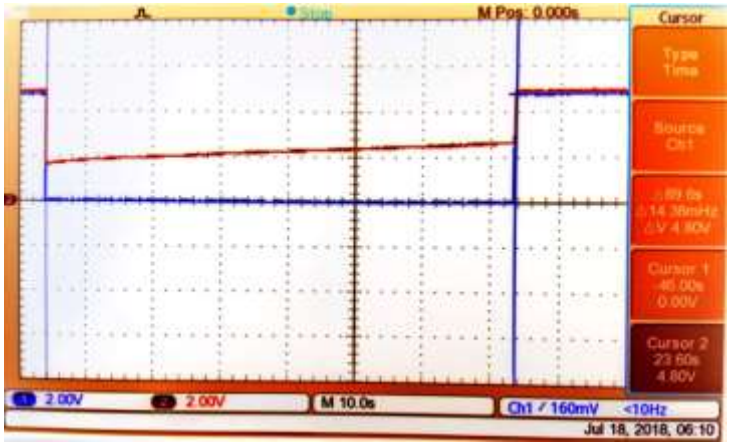


Figura 53 – Resposta da saída (linha azul) e do ponto que liga a resistência e o condensador (linha vermelha) a um pulso

Olhando para a Figura 53, consegue-se ver como o circuito reage entre a resistência e o condensador durante um pulso, e também como reage a saída. Pode-se ainda verificar que quando é mandado o pulso na entrada, o condensador descarrega até perto dos 1.6V e a saída passa para os 0V; de seguida vai carregando à medida que o tempo passa até cerca dos 2.7V. No momento que atinge esse valor, é carregado em breves instantes até aos 5V e a saída também passa para os 5V.

Nesta imagem pode-se verificar que o tempo do pulso é superior ao tempo medido anteriormente. Esta situação acontece pelo facto de o osciloscópio apresentar uma resistência de 10MΩ, que é próxima dos 1.8MΩ que estamos a usar na resistência. Isso faz com que a corrente que o osciloscópio recebe afete o circuito, e faça com

que o condensador demore mais tempo a carregar. Naturalmente isto afeta o tempo do pulso, desta forma fazendo com que o pulso demore mais tempo do que demoraria normalmente.

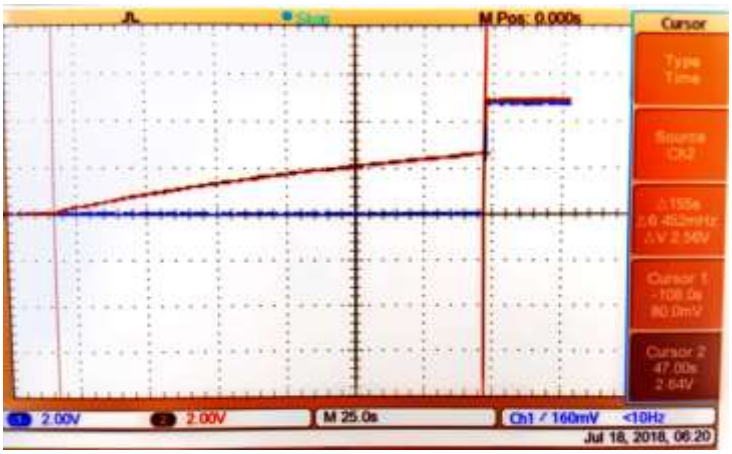


Figura 54 – Resposta gerada, quando é fornecida energia, na saída (linha azul) e no ponto que liga a resistência e o condensador (linha vermelha)

Analisando a Figura 54, pode-se ver a resposta do circuito quando é ligado à energia, onde se verifica que a tensão inicial no condensador é de 0V, em vez de ser os 1.6V resultantes de quando se descarrega o condensador ao gerar um pulso na entrada. Devido a isso, o condensador demora mais tempo a atingir os 2.7V, o que faz com que o pulso gerado na saída, quando se liga à energia, demore mais tempo do que o pulso na saída, gerado pelo pulso na entrada. Como se pode verificar o tempo apresentado na imagem Figura 54 é superior ao tempo apresentado na Figura 51 devido ao osciloscópio também estar a descarregar o condensador, aumentando o tempo necessário para a saída passar a 5V.

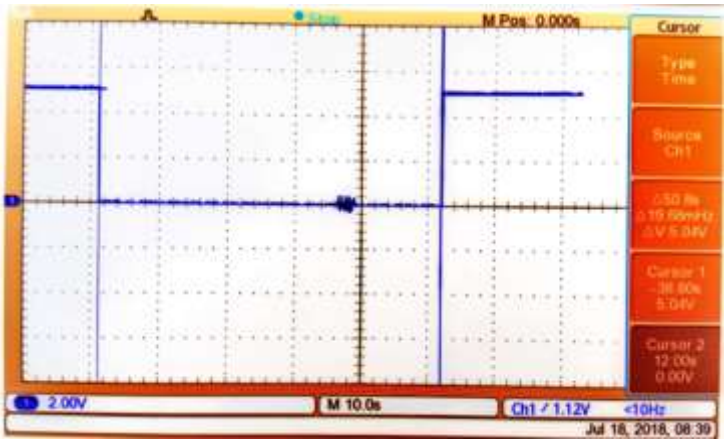


Figura 55 – Imagem dum pulso na saída quando o Arduíno está ligado com um adaptador 12V DC 2A

A imagem da Figura 55, foi obtida para analisar se ao ligar o Arduíno com um adaptador à corrente, em vez de ser alimentado por um computador, haveria alguma diferença nos resultados. Pode-se notar uma ligeira diminuição do tempo, que em vez de ser os 58segundos, passa a ser 50.8segundos.

Apesar de apresentar um tempo menor do que pensado inicialmente, não se considera um problema pois o tempo próximo do desejado. E caso se usem outros valores de resistência e condensadores disponíveis,

podíamos ter um tempo de pulso superior a 1 min, o que se quer evitar para não ter os dispositivos sem funcionar durante muito tempo no caso de falha.

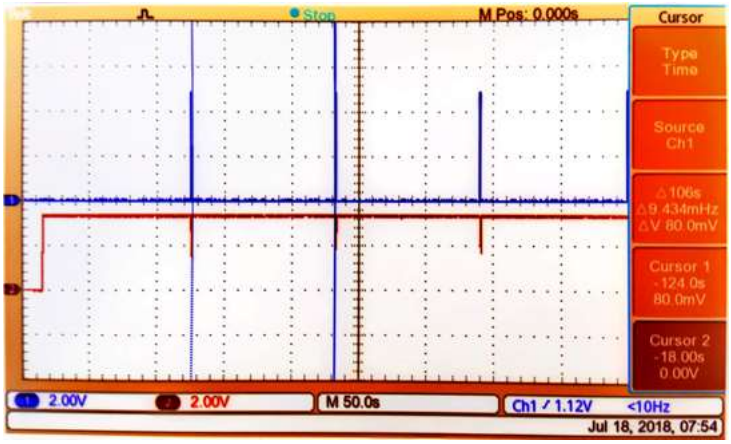


Figura 56 - Resposta da saída do circuito (linha azul) e da tensão de 3.3V (linha vermelha) quando o circuito controla a energia fornecida ao arduino

A imagem anterior foi obtida ligando o circuito ao Arduíno e o relé foi ligado de forma a conseguir cortar a energia do Arduíno. Foi medida pelo osciloscópio a resposta na tensão de 3.3V do Arduíno e na entrada do relé. Pode-se verificar pela Figura 56 que o tempo mínimo entre o Arduíno ligar e poder ser cortada a energia, se o Arduíno não gerar nenhum pulso na entrada do circuito, é de 106 segundos, aproximadamente. Também se pode ver pela imagem que a energia é cortada durante alguns segundos, e que depois volta a ligar, sem necessidade de interação humana.

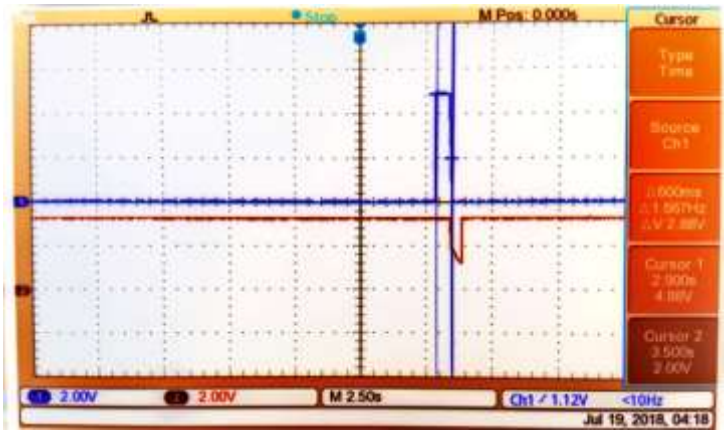


Figura 57 – Saída do circuito e alimentação de 3.3V quando se corta a energia, tempo relé ligado

Na Figura 57, consegue-se ver o tempo em que o relé vai estar ligado a cortar a energia, que vai ser 600ms até toda a energia no adaptador e no Arduíno acabar, e mesmo o relé ficar sem alimentação para poder cortar a energia. Assim sendo, vai voltar a permitir passar corrente, e os dispositivos voltam a ser alimentados.

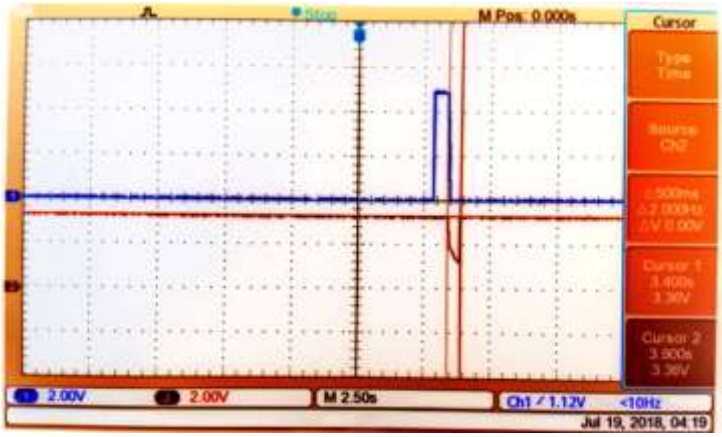


Figura 58 – Saída do circuito e alimentação de 3.3V quando se corta a energia tempo até a energia ser restabelecida

Ao observar a Figura 58 dá para ver que o tempo decorrido desde que o relé fica sem energia, até a energia do Arduíno ficar restabelecida é cerca de 500ms.

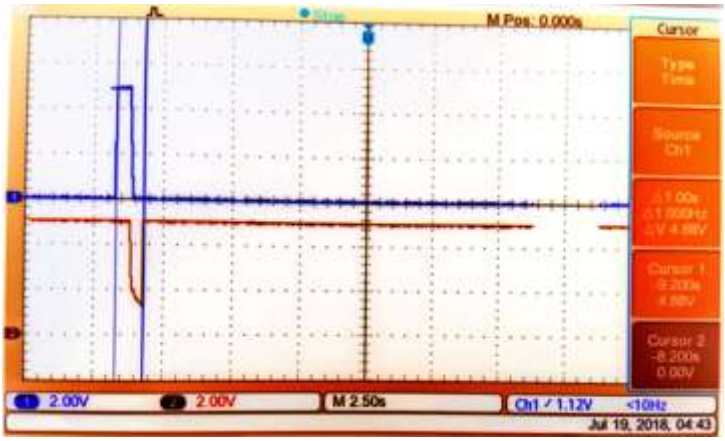


Figura 59 - Saída do circuito e a alimentação de 5V quando se corta a energia

Como se estava à espera pelas imagens anteriores, pode-se verificar pela Figura 59, que o tempo desde que o relé é ligado até a energia do Arduíno ser totalmente restabelecida, é de aproximadamente 1 segundo. Se se contar com o tempo aproximado de reset do Arduíno, que é de 1.7segundos, pode-se dizer que durante 2.7segundos o sistema heartbeat vai estar inoperacional, que acontece desde que o relé liga até o Arduíno estar totalmente operacional e a correr o programa.

O circuito depois de integrado em PCB ficou com o seguinte aspeto montado:

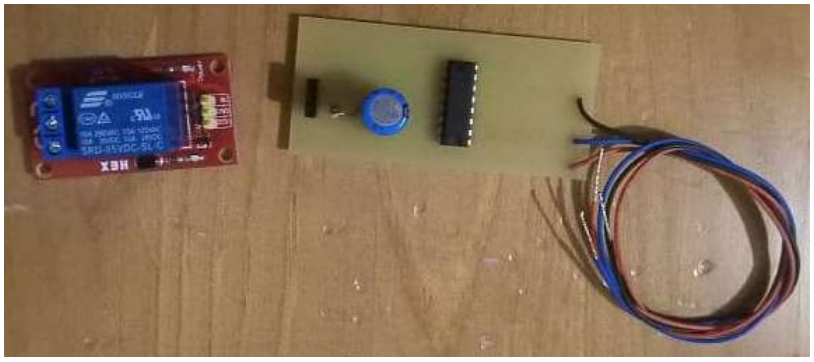


Figura 60 – Circuito montado em PCB lado dos componentes

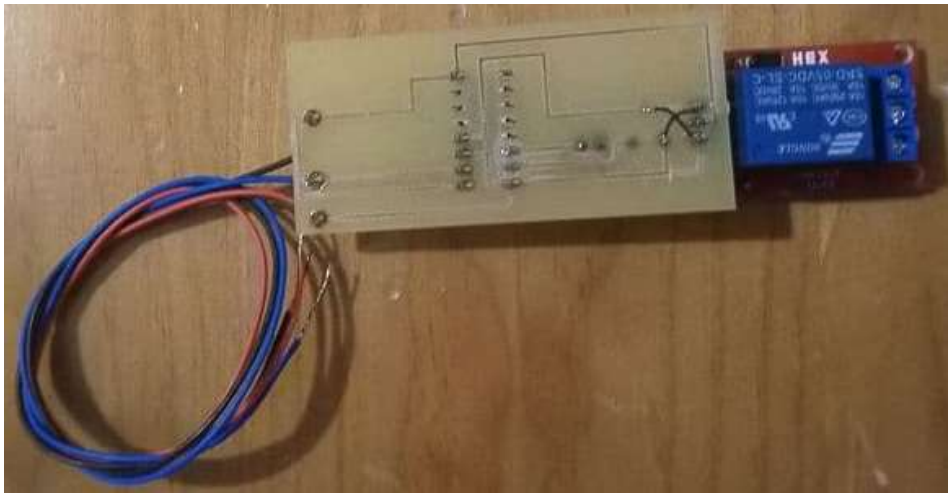


Figura 61 – Circuito montado em PCB lado das pistas

Quando foi impresso apresentava um erro nas pistas e ainda não tinha sido integrada, a resistência de 10kΩ (como é visível). O PCB final teria a seguinte board:

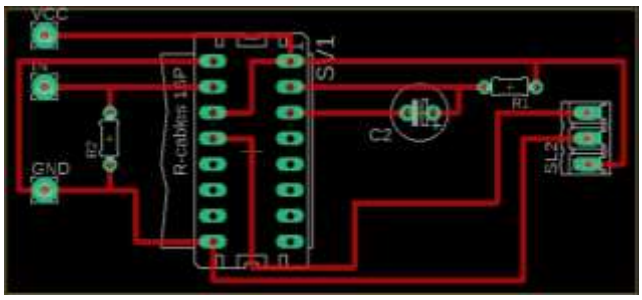


Figura 62 – Board para PCB do circuito

5.2.2 Tipo de Watchdog

Para decidir como vai ser o watchdog, temos de saber que portas estão disponíveis em cada aparelho que vai ser monitorizado. Assim sendo, temos de ver que portas existem em cada dispositivo e ver quais não são usadas noutras funções.

Para isso teve de se identificar os dispositivos que serão monitorizados, que serão gateways LoRa, RSUs e APs.

Nos gateways LoRa temos disponíveis as seguintes portas:

- 1 x Conexel Weidmuller 3 pinos, que usa o protocolo RS232
- 1 x Conexel Weidmuller 2 pinos, que usa o protocolo RS485
- 4 x pin I/O

Nos RSUs temos disponíveis as seguintes portas:

- 2 x RJ-45
- 1 x USB

Nos APs estão disponíveis as seguintes portas:

- 1 x RJ-45
- 1 x RJ-45 console port
- 1 x USB

Sabendo as portas disponíveis, temos agora três opções para o watchdog que são:

a) Sem nenhuma comunicação com o exterior, em que apenas serve como sistema fail-safe;
b) Com comunicação usando um microprocessador sem sistema operativo;
c) Com um sistema operativo e comunicação.

Para escolher o microcontrolador que é usado para as primeiras duas opções, como as necessidades de processamento são básicas, o importante é ter facilidade em arranjar extensões que tenham as portas necessárias para as várias conexões que cada dispositivo monitorizado apresenta. Por isso, foi decidido que apenas se precisava de um Arduíno Uno, que é fácil de utilizar, tem um custo baixo e tem uma grande quantidade de extensões disponíveis para o que for necessário.

Watchdog opção 1

Para a opção "sem nenhum tipo de comunicação", o watchdog apenas pode monitorizar o dispositivo e, em caso de falha, executa o reset, que pode ser o hard reset ou o soft reset se estiver disponível.

Assim sendo, para esta opção apenas seria preciso o circuito projetado (secção 5.2.1), um Arduíno uno e a extensão necessária para a comunicação com o dispositivo (que para os APs e os RSUs usa-se a extensão de internet e nos gateways LoRa pode usar os pinos I/O). Adicionalmente, precisava da alimentação do Arduíno e uma tripla para conectar o relé. Os componentes necessários estão no anexo 2.i.

Watchdog opção 2

Para a opção que tem comunicação mas sem sistema operativo, o watchdog pode monitorizar o dispositivo para, em caso de falha, executar o reset, que pode ser o hard reset ou o soft reset se estiver disponível. Com a presença de alguma comunicação permite configurar e controlar o sistema, mas apenas para situações pré-programadas no Arduíno.

Assim sendo, para esta opção seria preciso o circuito projetado, um Arduíno Uno, a extensão necessário para a comunicação com o dispositivo (que para os APs e os RSUs usa-se a extensão de Ethernet) e nos gateways LoRa pode usar os pinos I/O, ou no caso de se querer alguma forma de configuração, usar o RS232 ou o RS485. Além disso, é necessária a ficha de alimentação do Arduíno, uma tripla para conectar o relé e decidimos ainda colocar uma extensão de LTE ou GSM para uma comunicação de reserva, necessitando da extensão e um cartão SIM. Assim sendo, os componentes necessários estão presentes no anexo 2.ii.

Watchdog opção 3

Na opção 3 do watchdog já seria usado um single board computer, que consegue suportar um verdadeiro sistema operativo, em vez de apenas um microcontrolador, o que vai permitir fazer o acesso remoto, o controlo remoto e configurar remotamente, além de poder fazer o soft reset, o hard reset e o controlo básico do sistema.

Além disso deveria ter uma porta de Ethernet para poder conectar aos APs e aos RSUs, em que no caso do gateway LoRa se poderá usar um cabo USB para RS232 3 pinos ou pinos I/O, caso não haja uma porta RS232. A comunicação entre o dispositivo e o watchdog teria de ser alterada para que seja permitido ao watchdog configurar o dispositivo. Para além da monitorização, e é necessário garantir uma conexão à internet para se poder aceder remotamente. Também será necessário LTE/GSM para ter uma rede de comunicação de backup e os pinos I/O necessários para controlar o circuito de hard reset.

Um single board computer que preenchia estes requisitos era o APU3 [26], mas existem outras placas que cumprem estes requisitos, ou pelo menos parte deles, e que, com as entradas que apresentam, poder-se-iam completar os requisitos adicionais com extensões que pudessem preencher as lacunas, como por exemplo:

- Banana Pi BPI-R2 [29]
- AIMB-215 B1 [30]
- Mitac PD10AI-N4200 [31]
- Raspberry Pi 3 [39]
- Asus Tinker Board S [32]
- Rock64 Media Board [32]
- Odroid-C2 [32]
- Banana Pi M64 [32]
- Orange Pi Plus2 [32]
- NanoPC-T3 Plus [32]
- Le Potato [32]
- LattePanda [32]

As placas acima referidas conseguem preencher a maioria dos requisitos, mas nenhuma apresenta comunicação por LTE/GSM integrado, o que seria necessário implementar à parte.

Os watchdog não precisam de um single board computer muito potente, e além disso os RSUs usam apu3 e os watchdog devem ser compostos por single board computers menos potentes do que o dispositivo a controlar,

por isso, o selecionado foi o Raspberry Pi 3. Então os componentes necessários para esta opção estão numa tabela no anexo 2.iii.

De seguida apresentamos as vantagens e desvantagens de cada opção.

	Vantagens	**Desvantagens**
Opção 1: Sem comunicação e sem sistema operativo	• Bastante simples de implementar • A opção mais barata • Menos probabilidade de falhar visto que o programa é bastante simples	• Não tem qualquer comunicação • Em caso de falha não pode ser monitorizado • Não é possível nenhum tipo de configuração ou controlo remoto
Opção 2: Com comunicação e sem sistema operativo	• Simples de implementar • Tem comunicação • Pode executar configurações remotas • Em caso de falha pode ser monitorizado	• Todas as configurações estão restritas á pré programação antes feita • Mais cara que a primeira opção
Opção 3: Com comunicação e com sistema operativo	• Pode ser mais um componente da plataforma que pode ser usado • Tem comunicação • Pode-se aceder remotamente • Consegue-se fazer configuração manual remota • Pode executar funções mais complexas • Apresenta uma maior flexibilidade na monitorização	• A opção apresenta um elevado nível de complexidade • Mais difícil de implementar (exige mais conhecimentos)

Tabela 12 – Tecnologias para rede backup

Nas desvantagens esta presente na opção 1, "em caso de falha não pode ser monitorizado", pois mesmo que estes sistemas estejam desenhados para responder com um hard reset em caso de falha, existe a possibilidade deste sistema falhar.

5.2.3 Watchdog programa de controlo

O programa de controlo que se desenvolveu serve para controlar se um AP está a funcionar corretamente. Para isso, pensou-se quais as possíveis situações que o AP poderia não estar a funcionar corretamente, e pensou-se nos casos possíveis de falha do AP que são três: não responder, não estar a fornecer Wi-Fi e não estar a fazer o encaminhamento de pacotes.

Para testar cada uma das situações descritas usaram-se formas diferentes. Para ver se o AP está a responder usaram-se dois métodos: se o AP respondia a pings diretos, e se o AP respondia a pedidos de http. Com o ping consegue-se verificar se o AP está ligado, e com o pedido de http, como o AP já tem de mandar uma resposta, deve verificar se está a funcionar corretamente.

Para verificar se está a fornecer Wi-Fi, faz se um scan de todas os Wi-Fis disponíveis, e verifica-se se o Wi-Fi do AP está ativo.

Por fim, para apurar se está a fazer o encaminhamento de pacotes, mandam-se pings para vários sites distintos.

Depois de definir as formas de verificação foi escrito um programa com o seguinte esquema:

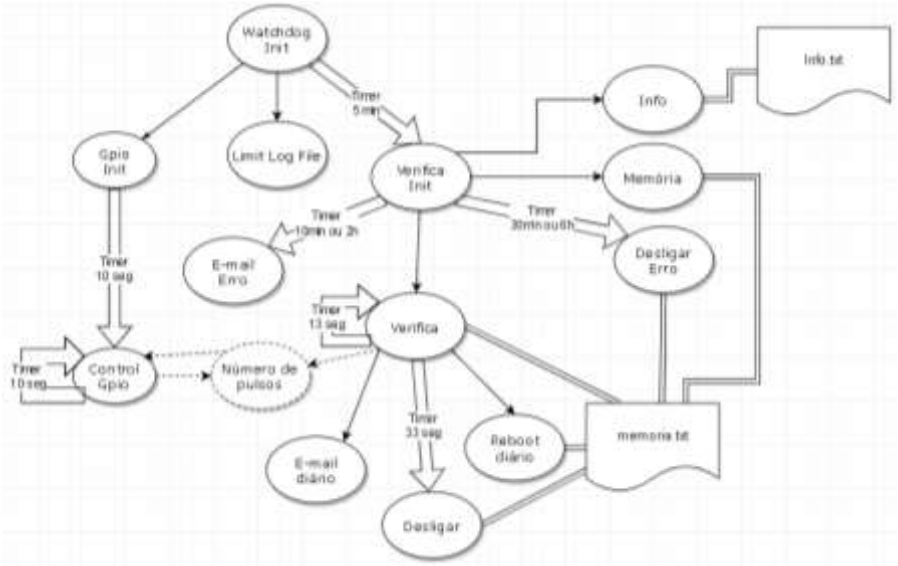


Figura 63 – Esquema básico do programa de watchdog

Pelo esquema básico apresentado na Figura 63 podem-se ver as interações entre as várias funções do programa, e também quais threads estão a correr no programa em paralelo. Na figura as linhas com seta no fim representam uma função a chamar outra, mas a correr na mesma thread; as setas que têm o tempo do timer indicado, correspondem a uma iniciação de uma thread com timer, em que a função irá ser executada no fim do tempo do timer.

Vê-se também um círculo a tracejado que é uma variável que conecta a thread de *verificar* e a thread de *controlo de Gpio*, que serve para indicar como essas funções interagem. A função *verifica* sempre que não ocorre nenhum erro vai colocar o valor da variável "*número de pulsos"* num valor constante e a função de *control gpio* sempre que precisa de mandar um pulso reduz o valor da variável em um.

Também existem dois ficheiros de texto presentes no esquema, que fazem parte do programa. Um deles é o *info.txt*; que contém os valores de várias constantes que podem variar entre cada watchdog, e para não se alterar o programa principal, esses valores são guardados num ficheiro texto. O ficheiro *memoria.txt* serve como uma memória para o watchdog, onde se guarda os dados dos erros que acontecem, sendo assim possível saber que erros aconteceram antes do último reiniciar.

Além destes dois ficheiros presentes é também criado outro ficheiro de texto, mas como não afeta diretamente o programa, não está representado no esquema. Este é o ficheiro de log que guarda as informações dos erros, dos reiniciares e o momento em que cada um acontece.

A partir de agora vai ser explicado o funcionamento de cada função e a explicação de algumas decisões feitas na programação.

A função representada no esquema chamada *Limit Log File* serve apenas para limitar o tamanho do log file. Como está previsto que o watchdog seja colocado e funcione sem nenhuma interação humana, convém que o ficheiro log não preencha todo o espaço livre em disco.

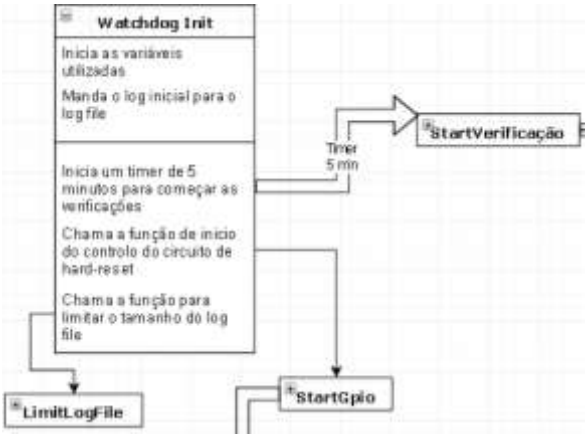


Figura 64 – Função Watchdog Init

Pela Figura 64 conseguem-se identificar as principais funções do *Watchdog Init*, que são: a inicialização das várias variáveis necessárias durante a execução; mandar um log para o log file a indicar que o reiniciar acabou e a data e hora; de seguida começa uma thread com timer que vai executar a função que começa as verificações e, por último, chama as funções *StartGpio* e *Limit LogFile*.

O tempo do timer foi definido como 5 min, de forma a garantir que o dispositivo controlado já está totalmente funcional antes de se começar a verificar se tem algum problema. Além disso, se o AP apresenta problemas nos primeiros 5 minutos, é provável que outro reiniciar não resolva esse problema. Além destas funções também chama a função

Figura 65 – Função Gpio Init

Na figura acima está explicado um resumo do que a função *Gpio Init* executa. Nesta função são feitas as configurações iniciais para controlar os pinos I/O; é enviado o primeiro pulso para o circuito de maneira a evitar que seja feito um reiniciar quando o programa ainda está iniciar; executa uma configuração para que no momento em que se desliga o watchdog o pino que controla o circuito fique a 0. Isto permite que quando for preciso executar um hard reboot se possa desligar o watchdog antes de se retirar a energia, para proteger o watchdog de não ser danificado ao se retirar a energia enquanto está ligado.

No *Gpio Init* também são configurados os valores dos tempos entre cada pulso para o circuito, e por fim é iniciada uma thread com timer que vai executar a função *Controlo Gpio*.

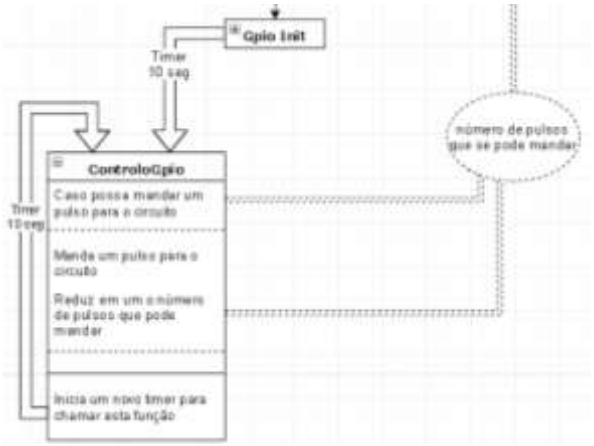


Figura 66 – Função ControloGpio

A função *ControloGpio* é uma função simples, que apenas tem de verificar se a variável *"número de pulsos"* é superior a um. Se o valor for superior envia um pulso para o circuito e reduz o valor da variável em um e, por fim inicia uma thread com timer a chamar se a si própria.

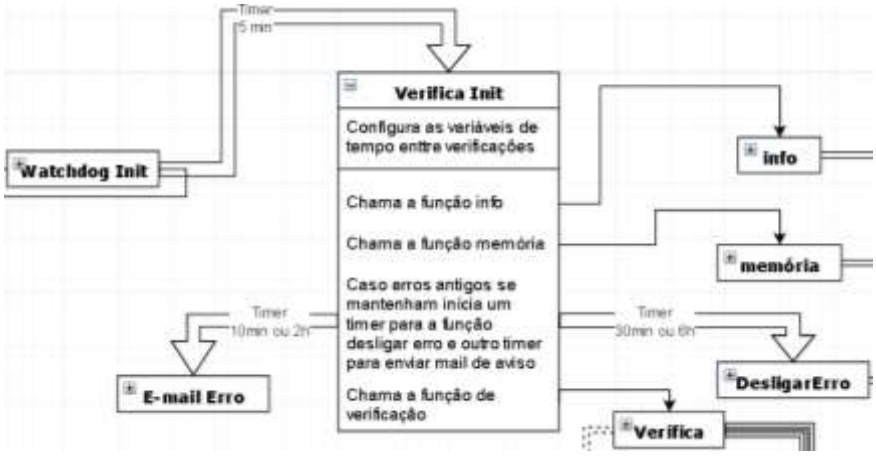


Figura 67 – Função Verifica Init

Ao executar a função *Verifica Init* serão configuradas as variáveis que definem o tempo entre cada verificação, e chamadas as funções *info* e *memória*. A função *memória* retorna os erros que se estão a repetir depois do reiniciar. De seguida, se houver erros a repetir-se depois do reiniciar, existem duas hipóteses de chamar as funções: *Desligar Erro* e *E-mail Erro*. Caso o AP não esteja a fornecer Wi-Fi ou não responda, será iniciado o

timer de 30 min para a função *DesligarErro* e o timer de 10 min para a função *E-mail Erro* (os timers servem para verificar se o problema se resolve sozinho, pois como já foi feito um reiniciar e não resolveu, assim sendo pode ser um problema que não dá para resolver ao reiniciar); caso todos os pings aos sites falhem, será iniciado o timer de 6h e o de 2h. Estes valores foram escolhidos porque se apenas os IPs de fora não responderem, pode não ser um problema no AP, mas um problema externo e, se for esse caso, não queremos estar a forçar os equipamentos a hard reboots repetidos por problemas que não se podem resolver. Por fim será chamada a função de *verificação*.

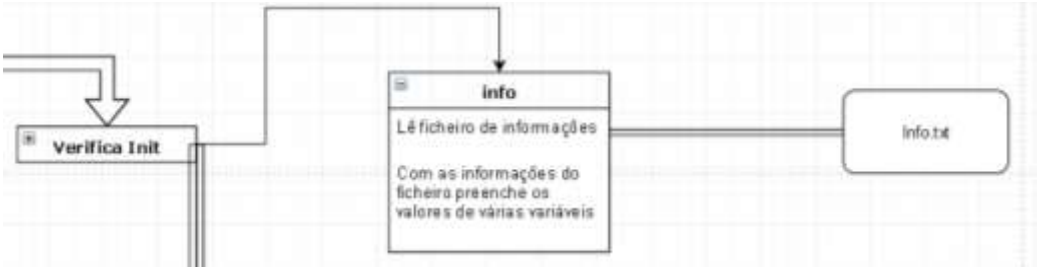


Figura 68 - Função Info

Esta função serve para ler o ficheiro *info.txt*, que tem o valor de várias constantes crucias para o funcionamento do programa. Depois de ler o ficheiro a função irá colocar os valores nas variáveis respetivas.

Figura 69 – Função Memoria

Esta função vai ler o ficheiro *memoria.txt* que contém os erros que estavam a acontecer no momento em que o último reiniciar aconteceu, e faz a verificação se esses erros ainda estão a ocorrer. Se estiverem, guarda numa variável os erros que se mantêm e esta variável é a que contém os "erros antigos".

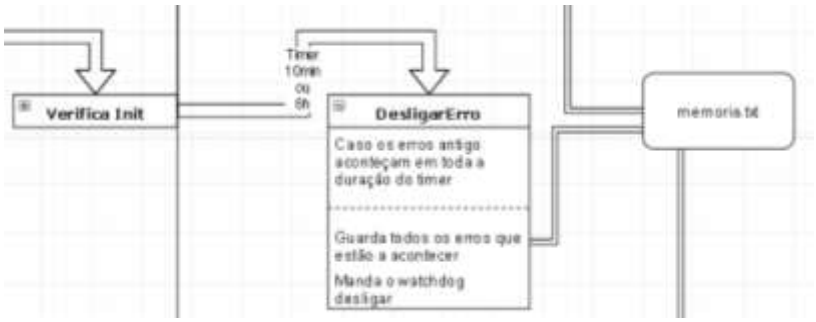


Figura 70 – Função DesligarErro

A função *Desligar Erro* irá fazer reiniciar se os erros que aconteceram no último reiniciar continuarem a ocorrer durante todo tempo que o timer esteve a contar. Nesse caso guarda os erros no ficheiro *memoria.txt* e manda o watchdog desligar. Caso o erro tenha parado de acontecer, esta função não irá fazer nada, contudo, se:

- Continuar a ocorrer os erros em todos os pings a sites;
- Mas não ocorrer mais nenhum erro.

Então ela irá iniciar um timer que complete as 6h em que irá voltar a chamá-la.

Figura 71 – Função E-mail Erro

A função *E-mail Erro* irá enviar um email ao responsável pela plataforma, se os erros que aconteceram no último reiniciar continuarem a ocorrer durante todo tempo que o timer esteve a contar, envia um email com todos os erros que estão a ocorrer para o responsável. Caso o(s) erro(s) tenha(m) parado de acontecer, esta função não irá fazer nada. Mas, se:

- Continuar a ocorrer os erros em todos os pings a sites;
- Mas não ocorrer mais nenhum erro.

Então ela irá iniciar um timer que complete as 2h em que irá voltar a chamá-la.

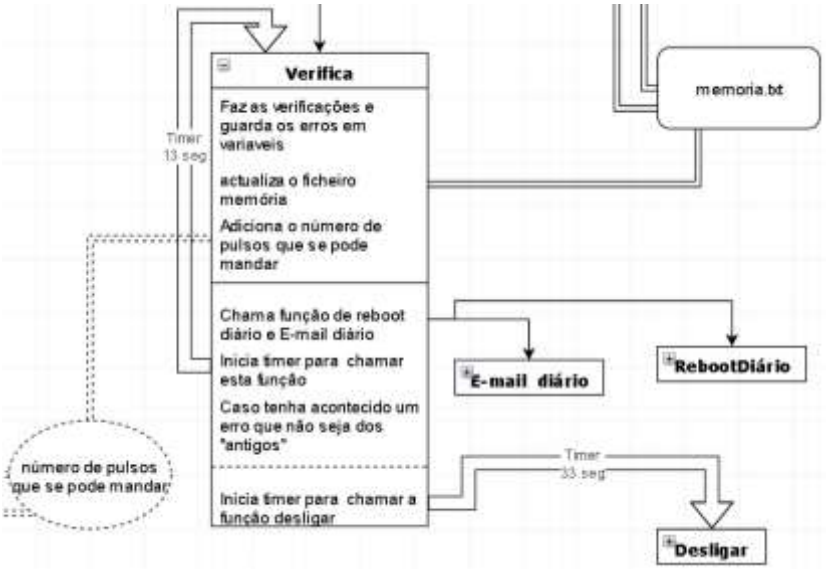


Figura 72 - Função Verifica

Na função *Verifica* começa-se por fazer as várias verificações e, caso alguma falhe, irá ser escrita no *memoria.txt*. No caso de alguma das verificações que esteja nos "erros antigos" não falhe, essa será removida dos mesmos. Se não ocorrer nenhuma falha nas verificações ou apenas as que estão na lista de "erros antigos"

falharem, será colocado o valor da variável "número de pulsos" num valor constante, caso contrário será iniciado um timer que irá chamar a função Desligar. De seguida será chamada a função *RebootDiário* e a função *E-mail diário*. Por fim será iniciado um timer que irá chamar esta função.

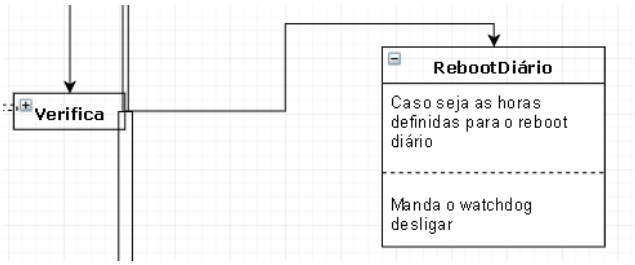


Figura 73 – Função Reboot Diário

A função *Reboot Diário*, apenas verifica qual é a hora atual e caso seja a hora definida para o reiniciar diário, manda o watchdog desligar o sistema.

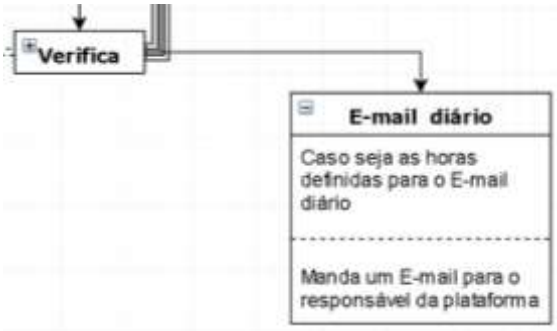


Figura 74 – Função E-mail Diário

A função *E-mail Diário*, apenas verifica qual é a hora atual e, caso seja a hora definida para o E-mail diário, manda um mail ao responsável pela plataforma. Estes mails servem como uma forma de informar e verificar se tudo está a funcionar corretamente.

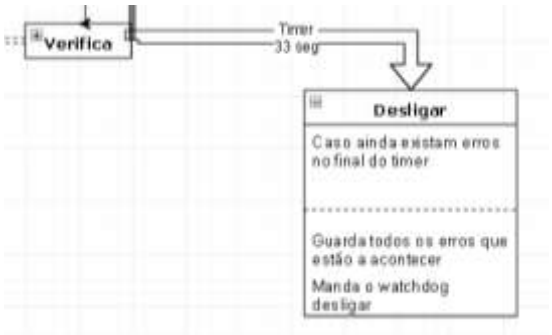


Figura 75 - Função Desligar

Por último existe a função *desligar* verifica se existe algum erro no momento e caso exista guarda os erros no ficheiro memoria.txt e desliga o watchdog.

Faltou indicar que todas as funções de desligar emitem uma mensagem para o ficheiro log, a identificar os erros que estão a acontecer e o momento em que foi iniciado o reiniciar. E na função *Verifica*, sempre que ocorre um erro, irá ser escrita uma mensagem que indica o erro que ocorreu e o momento em que ocorreu.

5.2.4 Watchdog formas de aumentar fiabilidade

Como foi falado até agora, os watchdogs são para ser colocados em ambientes reais, que podem ser afetados de muitas maneiras. Como são ambientes não controlados, os fatores que podem afetar os watchdogs, podem ser: radiações eletromagnéticas, humidade, temperatura, chuva, detritos no vento, rajadas de vento, a estabilidade da fonte de alimentação, entre outros.

Dos referidos fatores não se consegue prever quais possam acontecer, a sua intensidade, nem o tempo em que surgem, mas é possível reduzir as probabilidades de falha com várias formas de proteção que serão explicadas a seguir.

Proteção de água, poeira e temperatura

Na proteção contra água e poeira empurrada pelo vento que possam afetar o watchdog, pensou-se no uso de uma caixa de proteção com classificação de IP66 ou superior, definida no índice de classificação IP (Ingress Protection).

Este índice de classificação IP [52] é uma forma de avaliar a proteção de um objeto contra água e poeira e tem tabelas de classificação desde apenas proteger de chuva vertical, até proteção de submersão total, na proteção de líquidos. Relativamente a sólidos, hádesde classificação de proteção contra poeira com diâmetro superior a 50mm até classificação de totalmente protegido da poeira.

A classificação de IP66 garante a total proteção de poeira e proteção contra jatos potentes de água. Isto poderá ser necessário, por alguns locais colocação os equipamentos serem muitas vezes locais abertos (com poucas construções, árvores ou outros obstáculos por perto), podendo o vento atingir velocidades grandes e motivar maior intensidade de precipitação, por isso é necessário garantir uma boa proteção.

Proteger de temperaturas demasiado elevadas é complicado, mas uma forma simples seria a caixa que envolve o watchdog ter uma cor clara, assim tendo mais capacidade de reflexão, diminuindo a absorção. Doutra forma, pode ser usada uma caixa com aberturas de forma a circular ar, evitando aquecimento, mas isso pode retirar a proteção IP66 requerida (água e poeiras). Outras soluções a ser consideradas na colocação seriam: sombras para evitar a exposição solar direta, ou locais mais abertos permitindo estar exposto a alguma brisa de ar.

Proteção da fonte de alimentação

A proteção da fonte de alimentação é importante, pois mesmo que por norma a rede garanta os 230VAC com frequência de 50Hz, existe sempre algum ruído. Esse ruído, geralmente é de frequência elevada e em certas situações pode causar problemas aos aparelhos,pelo que é necessário colocar condensadores na alimentação.

Nesta proteção existem duas hipóteses: colocar os condensadores do lado da rede elétrica em relação ao relé, o que protege todos os componentes do watchdog e o equipamento da plataforma; ou colocar pouco antes do microcontrolador, sabendo que esta escolha protegerá melhor o watchdog, pois a quantidade de cabo entre o

microcontrolador e os condensadores é mínima, ficando assim com menos fio onde radiações eletromagnéticas possam criar ruído. Por sua vez, na segunda opção descrita, o relé e o equipamento não ficarão protegidos, a não ser que se coloquem condensadores para cada um dos componentes (em princípio o relé não deve precisar desta proteção).

Os condensadores usados seriam: um condensador cerâmico entre os 100pF e os 1nF, e um condensador eletrolítico entre os 1µF e os 100µF. O condensador eletrolítico serve para filtrar as frequências médias, mas para frequências mais elevadas não funciona tão bem (pois, os condensadores eletrolíticos têm uma má resposta a altas frequências), por isso, usa-se o condensador cerâmico que vai filtrar as frequências mais elevadas.

Para colocar os condensadores, deverá ser como está representado na Figura 76.

Figura 76 - Filtro de frequência na fonte de alimentação

Proteção para radiação eletromagnética

A proteção de radiação eletromagnética é importante, pois muitos equipamentos usados atualmente emitem radiação, o que aumenta o risco de acidentes eletromagnéticos. Além dos equipamentos que geram radiação eletromagnética, o sol também emite, e no caso de uma explosão solar, as radiações emitidas podem ser elevadas o suficiente para afetar equipamentos eletrónicos.

Por estes motivos é necessário usar proteção da radiação eletromagnética em equipamentos colocados em locais remotos e sistemas autónomos. Assim sendo, uma forma de proteção bastante conhecida e muito eficaz de proteger de radiação eletromagnética é a Gaiola de Faraday.

Para aplicar gaiola de Faraday é apenas necessário envolver o equipamento desejado com uma caixa de material condutor. Porém, se os equipamentos dentro da gaiola precisarem de ter comunicação wireless será necessário colocar as antenas do lado de fora da caixa, porque a caixa vai bloquear a radiação desejada e a indesejada.

Esta caixa também pode proteger de descargas elétricas indesejadas. Ao ligar esta caixa com um fio à terra qualquer descarga será direcionada para a terra sem atingir o equipamento. Uma descarga elétrica pode acontecer no caso de um relâmpago atingir o poste que segura os equipamentos.

5.3 Sistema de rede

5.3.1 Configurador

Para o configurador foi escrito um programa que faz o uso da biblIoTeca livre GTK que ajuda na criação de interfaces gráficas. Com esta biblIoTeca dá para fazer programas de interface gráfica dos mais variados. Assim com a utilização desta biblIoTeca foi feito o programa descrito a seguir:

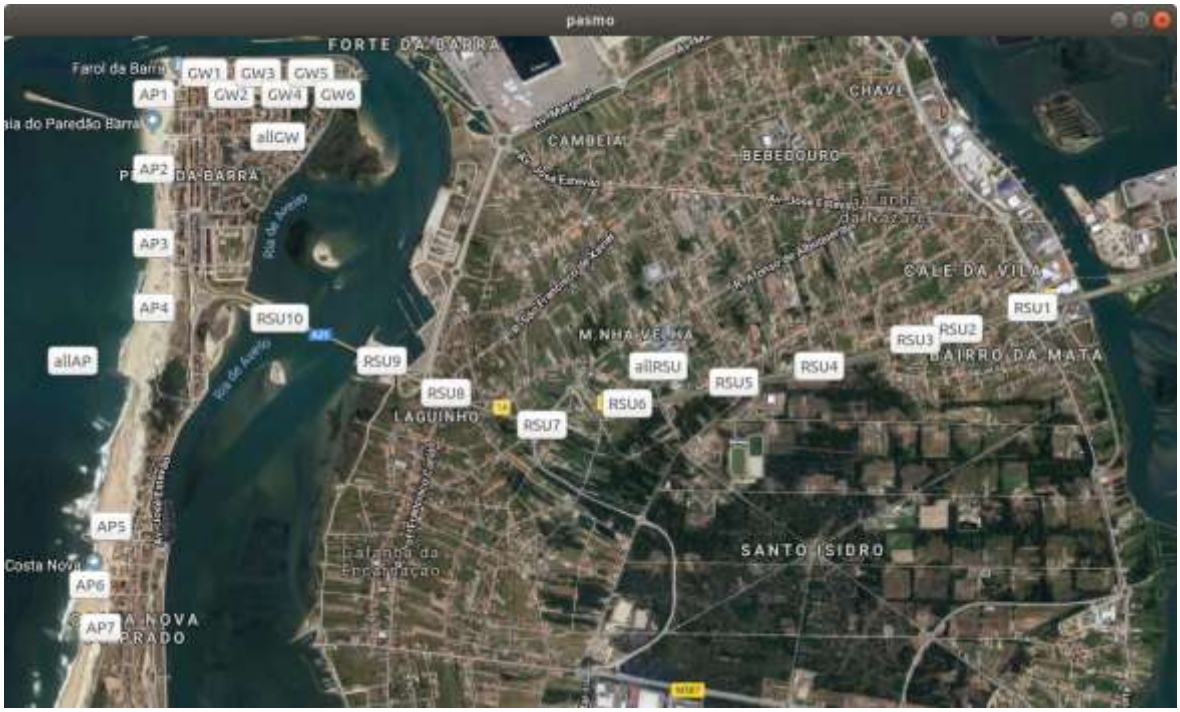


Figura 77 – Programa de controlo interface gráfica inicial

Na Figura 77 pode ver-se o aspeto do programa de controlo de watchdogs quando é aberto, em que dá para ver a localização de cada dispositivo no mapa e qual é o tipo de dispositivo. É possível selecionar o dispositivo que se quer sabendo apenas a sua localização. As identificações dos botões são as seguintes:

- AP – Access Point
- GW – Gateway LoRa
- RSU – Road Side Unit

Os números a seguir à identificação são uma forma de ajuda na identificação de cada um dos watchdogs, sendo usados para identificar os valores correspondentes a cada um, nos ficheiros que guardam informações cruciais para o programa, e como uma forma de identificar nos Emails enviados.

Para além dos botões relativos a cada um dos dispositivos, também estão presentes três botões chamados allRSU, allGW e allAP. Esses botões servem para controlar todos os watchdogs de dispositivos idênticos.

Quando se clica num botão que começa com “all” no nome será aberta a seguinte janela popUp:

Figura 78 – Janela PopUp dos botões iniciados em all

Na janela que abre podemos ver (Figura 78) que contém 5 botões, uma entrada de texto e um print de texto. Considerando que estamos a interagir com a interface allRSU, será a seguir explicado o que cada interação faz.

O primeiro botão chamado “Tempo Ativo”, serve para ver há quanto tempo estão ativos todos os watchdogs dos Road Side Units. Para isso o programa vai abrir um canal SSH com cada um dos watchdogs, correr o comando uptime e com o resultado imprimir no print de texto, obtendo-se a seguinte resposta:

Figura 79 – Janela PopUp dos botões iniciados em all resposta ao botão Tempo Ativo

Pelas impressões o RSUx sendo x um número, identifica qual é o watchdog e as linhas a seguir, é o que aconteceu quando se tentou executar o comando nesse watchdog. Dá para ver nos RSU4, RSU5 e RSU6 a resposta ao comando e, do RSU7 para a frente, o que acontece quando não consegue conectar ao watchdog.

O segundo botão chamado “Ficheiro memoria.txt” lê o ficheiro *memory.txt* do watchdog e imprime-o, obtendo-se o seguinte resultado:

Figura 80 – Janela PopUp dos botões iniciados em all resposta ao botão Tempo Ativo

Consegue-se ver (Figura 80) o que acontece quando não se consegue conectar no caso do RSU7 e RSU8, no caso do RSU6 de estarem a acontecer erros e um último caso que não aparece, se não houvesse nenhum erro a acontecer no momento. Nesse caso apenas aparecia a linha “ficheiro memoria.txt:” e nada na linha a seguir, continuando simplesmente para o próximo watchdog.

O terceiro botão chamado “Hard reset” serve para mandar todos os watchdogs executarem o hard reset. Para isso vai abrir o canal SSH e correr dois comandos em cada um dos watchdogs. Um comando para garantir que o pino de controlo do circuito vai ficar a zero depois do watchdog ser desligado, e outro comando manda o watchdog desligar. Ao executar o hard reset começa-se por desligar o watchdog e depois corta-se a energia, para proteger o watchdog de ficar danificado por se retirar a energia repentinamente. Assim, quando é premido o botão obtém-se a seguinte resposta:

Figura 81 – Janela PopUp dos botões iniciados em all resposta ao botão Tempo Ativo

Neste caso consegue-se observar que no RSU1 e no RSU2 foi executado o hard reset corretamente, enquanto os outros tiveram falhas de conexão.

O quarto botão é para ajudar no envio de ficheiros para o watchdog, podendo escolher o ficheiro numa interface gráfica quando se clica no botão. Sendo a seguinte interface gráfica:

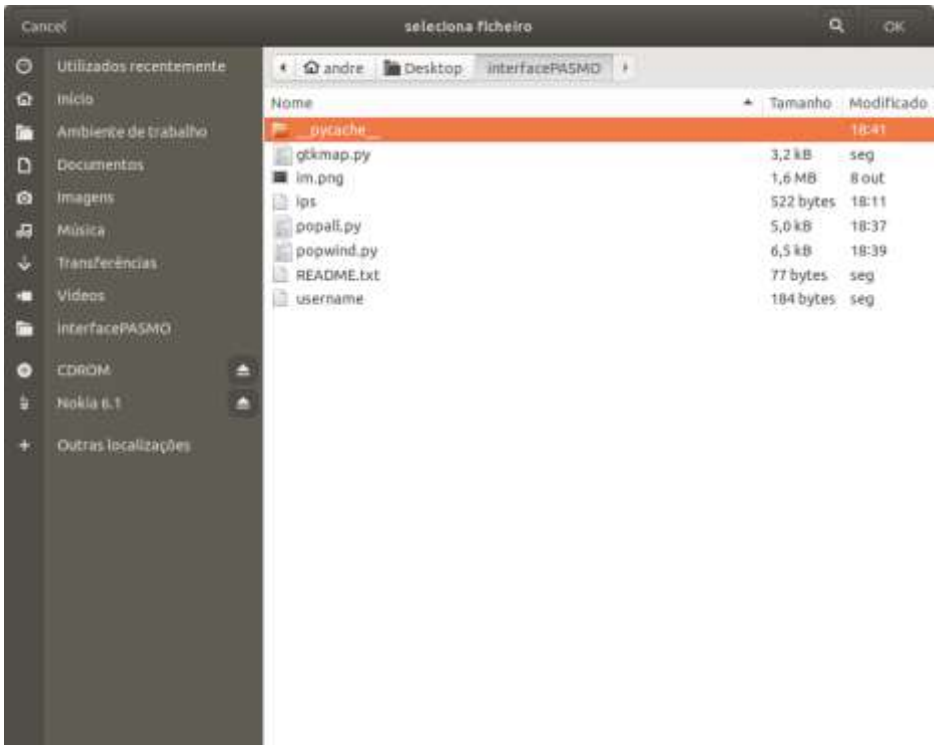


Figura 82 – Janela PopUp dos botões iniciados em all exemplo botão selecionar ficheiro

Nesta janela pode-se selecionar o ficheiro que se quer enviar para o watchdog. Ao selecionar o ficheiro, o seu fullpath será colocado na entrada de texto.

A entrada de texto serve para escrever o ficheiro que se quiser enviar para os watchdogs.

O botão “copiar ficheiro” irá executar o comando *scp* para cada um dos watchdogs. Esse comando também pode ser ativado se se clicar no enter quando interagindo com a entrada de texto. Em que envia o ficheiro indicado na entrada de texto para a pasta home do username no watchdog. Este comando também pode ser usado para enviar pasta, apenas se precisando escrever “-r fullpath da pasta”, sendo colocado o -r antes do caminho completo da pasta que se quer enviar. O resultado obtido, se foi enviado ou se falhou, o envio será imprimido no print de texto, e ficará com o seguinte aspeto:

Figura 83 – Janela PopUp dos botões iniciados em all exemplo botão Copiar ficheiro

Pode-se ver pela imagem acima que o comando foi corretamente executado e a pasta chegou aos watchdogs do RSU5 e RSU6, enquanto que o RSU7 e o RSU8 tiveram problemas no envio, e mostra o aviso de quando se tenta executar o comando *scp* para um IP que não se consegue conectar.

Por fim, o botão exit serve apenas para fechar a janela e, para esse efeito, também está presente o botão “x” que executa a mesma função.

No caso de quando se clica **num dos botões que identificam um watchdog específico**, já existem duas formas de conexão com o watchdog: pela rede de backup ou pela internet. Caso seja conectado pela internet, será aberta a seguinte janela popUp:

Figura 84 – Janela PopUp dos botões de watchdogs específicos

Como se pode ver, esta janela popUp apresenta um número maior de opções, que não mostrava na janela anterior. Esta apresenta a mais a opção de ver o "Log de erros" e aceder ao terminal.

Além disso, nesta janela, caso não se consiga conectar com o watchdog quer por internet, quer pela rede backup, vai ser apresentado um aviso quando a janela abre, ficando com o seguinte aspeto:

Figura 85 – Janela PopUp dos botões de watchdogs específicos sem conexão com o watchdog

Como existem alguns botões idênticos aos da janela que é aberta pelos botões "all", será apenas apresentada a aparência com que fica com cada botão que já foi falado antes. Visto já ter sido dada a sua explicação anteriormente.

Figura 86 – Janela PopUp dos botões de watchdogs específicos, resposta do botão Tempo Ativo

Figura 87 – Janela PopUp dos botões de watchdogs específicos, resposta do botão Ficheiro memory.txt

Figura 88– Janela PopUp dos botões de watchdogs específicos, resposta do botão Hard Reset

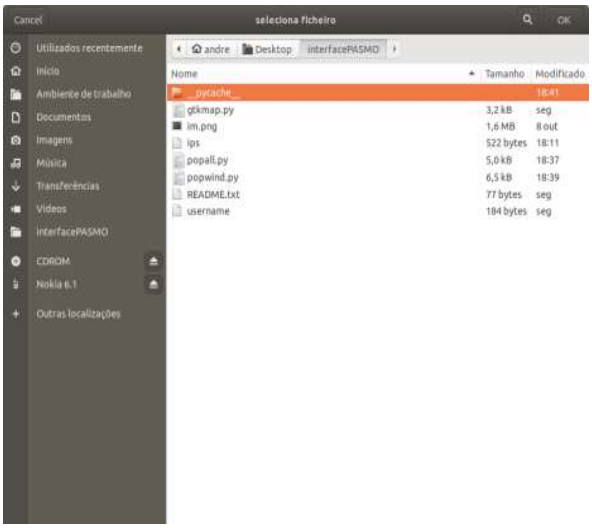


Figura 89 – Janela PopUp dos botões de watchdogs específicos, resposta do botão Selecionar ficheiro

Figura 90 – Janela PopUp dos botões de watchdogs específicos, resposta do botão Copiar ficheiro

Neste caso, na vez de ser enviado um ficheiro, está um exemplo de como se pode enviar uma pasta, que é colocar o -r e depois o caminho completo da pasta.

Como se pode ver pelas imagens acima, as respostas dos botões são idênticas às anteriores, apenas muda o fato que aqui apenas se controla um watchdog de cada vez.

Além destes botões também existem os outros dois que são o "Log de erros "nome do dispositivo controlado"", que quando clicado irá ler o ficheiro log criado pelo programa que controla o watchdog, obtendo-se um resultado assim:

*Figura 91 – Janela PopUp dos botões de watchdogs específicos, resposta do botão Log de erros ****

Neste botão podem se ver os vários erros que aconteceram e o momento em que aconteceram, tais como: avisos da falha de deteção do Wi-Fi, em que o watchdog não conseguia detetar o Wi-Fi; o aviso do reiniciar diário; avisos que o reiniciar terminou e avisos de quando os pings falham. Em todos os avisos pode-se ver a hora e o dia em que aconteceram, assim permitindo identificar problemas que tenham acontecido e o momento exato em que aconteceram.

Por último, o comando "Aceder terminal do watchdog", quando clicado esse botão, um terminal será aberto com o canal SSH já conectado, vindo com a seguinte aparência:

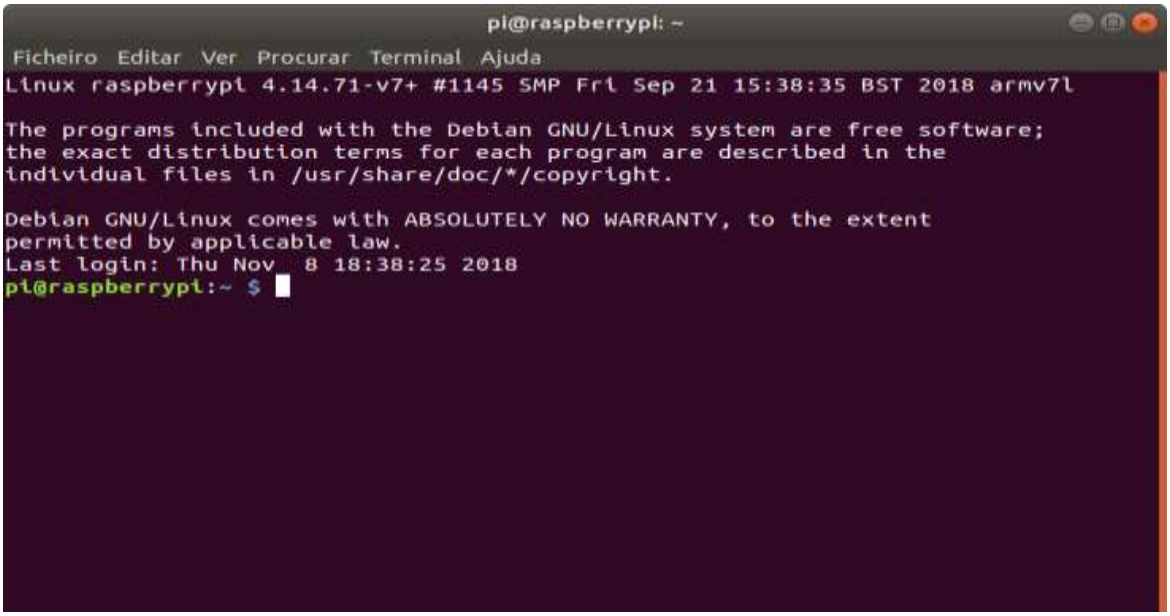


Figura 92 – Janela PopUp dos botões de watchdogs específicos, resposta do botão Aceder terminal do watchdog

Como não dá para prever todas as utilizações que serão precisas fazer, um programa que disponibiliza o terminal do watchdog é bastante importante. Isto providencia grande facilidade de alterar o que for necessário no watchdog e aumentar a liberdade do utilizador. Claro que os utilizadores de um programa com tanta liberdade, também têm de ter o cuidado de não danificar, eliminar ou parar programas cruciais para o funcionamento do watchdog.

Caso não exista conexão pela internet, mas a rede de backup esteja funcional, será aberta a seguinte janela popUp:

Figura 93 – Janela PopUp dos botões de rede de backup

Na Figura 93 está apresentada a janela que aparece quando a conexão é feita pela rede de backup, devido a não existir conexão pela internet. Como se pode ver, começa com um aviso que se está a utilizar a rede de backup, e pode-se ver que tem quatro botões, que já existiam antes, (as suas funcionalidades são iguais aos botões presentes nas outras janelas popUps). Além desses, também se conseguem ver dois botões diferentes e o texto editável também é diferente.

Figura 94 – Janela PopUp dos botões de rede de backup, resposta do botão Verificar quando a conexão volta

Este botão é para o caso se precise de fazer um backup, mas se considere que não se irá recuperar a conexão à internet. Como o tempo de estabelecimento da rede de backup pode demorar alguns minutos, este botão apenas entra num loop e avisa quando a rede de backup voltou a funcionar, apresentando a mensagem “Connected” e deixa outra vez interagir com a janela normalmente. Enquanto está a espera que a conexão volte, os botões de interação da janela ficam bloqueados.

O outro botão e a entrada de texto funcionam como um terminal. Este apenas corre o comando que estiver na entrada de texto e depois é fechado. Usar comandos de mudar de pasta ou abrir ficheiros, nesta forma de interação, é pouco útil, pois quando acaba de executar o comando o terminal é fechado. No caso de se enviar outro comando, será aberto um novo terminal que estará na mesma pasta. Mas, todos os outros comandos podem ser executados, por exemplo:

Figura 95 – Janela PopUp dos botões de rede de backup, resposta do botão Executar comando no terminal, exemplo 1

Pela Figura 95 pode-se ver como responde a um comando simples, em que corre o comando no watchdog e depois apresenta o resultado na janela.

Figura 96 – Janela PopUp dos botões de rede de backup, resposta do botão Executar comando no terminal, exemplo 2

Caso se tente executar um comando que dê erro, aparecerá o aviso de que ao correr o comando houve um erro e indicará qual foi a resposta ao erro.

Além destas opções, também dá para correr vários comandos seguidos como nos terminais normais:

Figura 97 – Janela PopUp dos botões de rede de backup, resposta do botão Executar comando no terminal, exemplo 3

Como se pode ver pela imagem acima, executa os vários comandos e apresenta as respostas e\ou os erros que aconteceram.

5.3.2 Rede Backup

De forma a programar as conexões da rede de backup, a primeira exigência que se teve foi arranjar uma extensão para o raspberry Pi que foi a seguinte:

Figura 98 – Extensão Raspberry Pi SIM900 GSM/GPRS Add-on v1

Esta extensão tem os pinos para ligar diretamente ao raspberry pi e funciona com 5V, mas nos pinos que ela tem livres apenas fornece tensões até os 3.3V. Ao ligar ao raspberry esta extensão liga-se a 26 pinos para o caso do raspberry pi 3: 8 deles são alimentação ou são ground; dos outros 18 pinos, existem apenas 4 que interagem diretamente com a placa, o resto controla os pinos GPIO que a placa apresenta.

Desses 4 pinos, há dois de UART do raspberry, que servem para comunicação (um pino é de transmissão para a placa, e o outro é de receção da placa). Os dois pinos restantes, um serve para fazer reset à placa e o outro serve para ligar e desligar a placa.

Esta placa tem integrado o SIM900 [43], que é um módulo para comunicações wireless, em que comunica com a tecnologia GSM e GPRS. Com este módulo é possível fazer telefonemas, mandar mensagens, enviar faxes e aceder á internet.

Quando se comunica com a extensão a partir do raspberry pi, a comunicação faz se com o módulo SIM900. Este módulo tem um terminal integrado com comandos específicos. Os comandos que se podem usar para comunicar com o módulo estão apresentados no documento [44].

Para estabelecer qualquer tipo de comunicação através da extensão GSM, é necessário comunicar com o módulo SIM900, usando os comandos AT.

Além disso, esta extensão usa um cartão SIM para fazer a comunicação com a rede. Esse cartão, a não ser que seja pago especificamente para ter um IP estático, irá ter um IP dinâmico. Ao ter um IP dinâmico faz com que sempre que o cartão SIM seja ligado á rede receba um IP diferente, o que torna complicado a partir do servidor conectar ao raspberry pi usando a rede de backup. Então para simplificar, em vez do servidor tentar ligar ao raspberry, foi feito com que o raspberry se conecte ao servidor, já que este tem um IP privado estático e a rede privada tem um IP público também estático, sendo assim mais fácil descobrir a qual IP é para se conectar.

Depois de tomar a decisão de como é feita a conexão entre o servidor e o raspberry por GSM, foram escritos dois programas. Um programa para o raspberry que controla a extensão de forma a criar uma conexão TCP/IP com o servidor, e para fazer essa conexão faz o uso de vários comandos AT, de forma a configurar o módulo SIM900 a estabelecer a ligação. O outro programa é para o servidor, e está escrito de forma a estar sempre a correr, e nesse programa é aberto um canal TCP/IP ao qual o raspberry se pode conectar.

Com estes dois programas simples, já existe uma conexão entre o raspberry e o servidor através de GSM. A partir daí foi necessário desenvolver o que se podia fazer com a comunicação.

Para isso desenvolveu-se o seguinte sistema de programas:

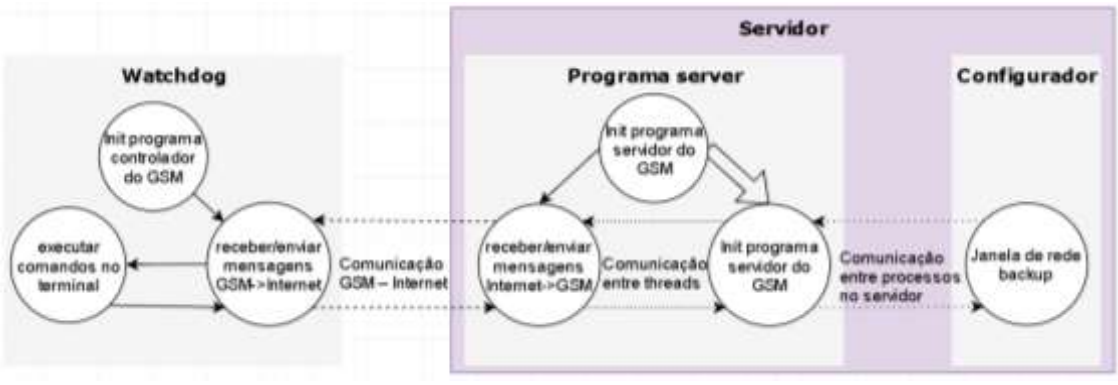


Figura 99 – Sistema para comunicação da rede backup

Este sistema (Figura 99) é dividido em três programas e em duas comunicações, sendo uma comunicação entre o raspberry pi e o servidor, usando GSM e internet. A outra comunicação é entre dois processos a correr no servidor, que é entre o programa que faz a conexão da rede backup e o configurador sendo, portanto, uma comunicação interna no servidor.

Assim sendo, irá ser explicado a seguir como funciona o programa de controlo da extensão GSM e o programa que está a correr no servidor.

Programa no raspberry

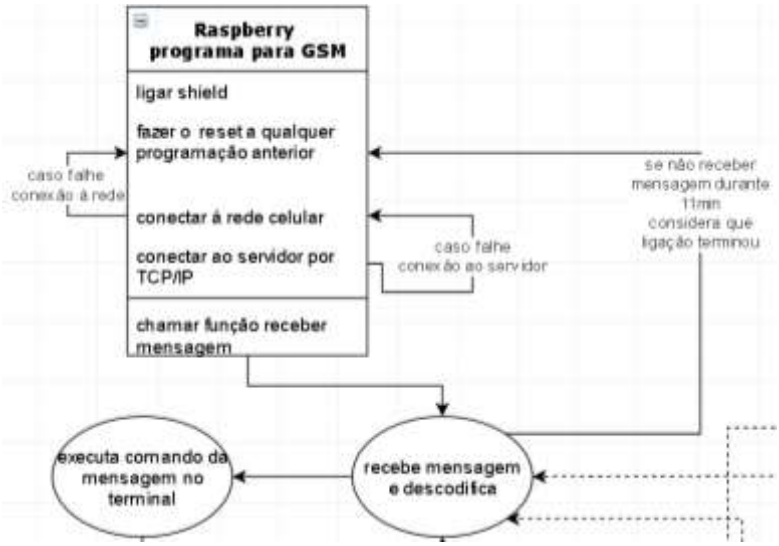


Figura 100 – Início programa de controlo de extensão para rede backup

O programa de controlo de extensão começa com a configuração da extensão GSM (Figura 100). Inicialmente muda a tensão do pino que liga a extensão para 5V, de forma a ligar a extensão. De seguida, faz um reset ao módulo, e logo a seguir começa a enviar os comandos AT necessários para verificar se a extensão está a funcionar corretamente.

Quando o SIM900 está sem nenhuma configuração, o programa começa a enviar os comandos AT que configuram a conexão à internet. No caso de um comando da configuração à internet falhar, o programa recomeça outra vez no reset das configurações. No caso de a extensão se conseguir conectar à internet por GSM, então irá ser iniciado o processo de conectar ao servidor por uma ligação TCP/IP e, caso essa conexão falhe, volta-se a configurar a conexão a internet, pois pode ter existido algum problema na conexão. Se a ligação ao servidor for bem-sucedida o programa irá chamar a função *receber mensagem*.

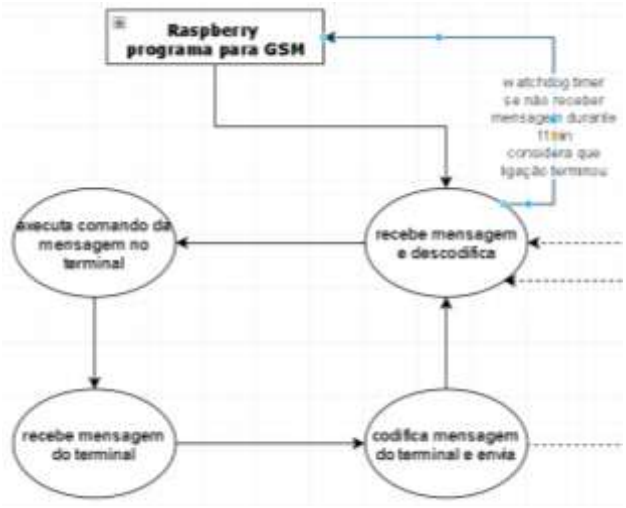


Figura 101 – Ciclo do programa de controlo de extensão para rede backup

Quando entra na função *receber mensagem* (Figura 101), entra num ciclo onde fica a verificar constantemente se recebeu alguma mensagem por GSM, e a verificar há quanto tempo não recebe uma mensagem. Quando não recebe uma mensagem há mais de 11 minutos, vai considerar que a ligação terminou e volta para a função anterior no momento em que faz o reset a todas as definições anteriormente feitas.

No caso de receber uma mensagem nova, o programa irá descodificá-la e executar o comando de terminal enviado na mesma. No final de executar o comando de terminal, vai ler a resposta ao comando e/ou o erro da resposta ao comando. De seguida, codifica essa resposta e envia-a para o servidor.

No fim de enviar a mensagem, volta ao estado inicial do ciclo, em que fica constantemente a verificar se recebeu alguma mensagem e a controlar há quanto tempo não recebe mensagens.

Programa no servidor

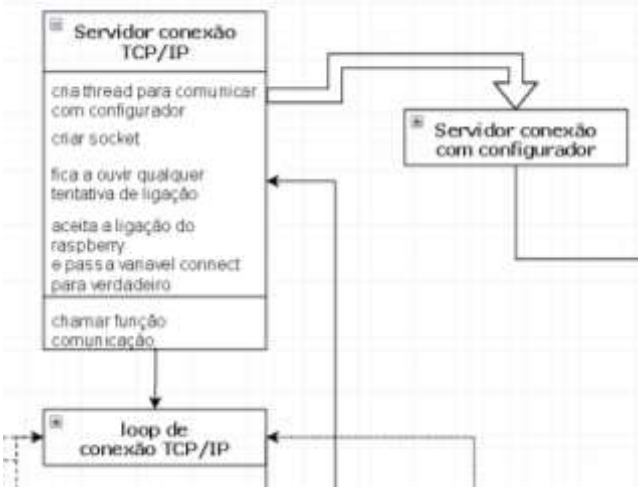


Figura 102 – Função inicial do programa no servidor para rede backup

No programa que está a correr no servidor (Figura 102) irá ser criado uma socket num porto específico, que irá estar aberto para o raspberry se poder ligar. Para isso o router da rede onde o servidor está precisa permitir a

conexão, e de fazer o encaminhamento dos pacotes de fora da rede privada para o servidor. Para o router fazer o encaminhamento dos pacotes é definido um porto específico no IP público, em que os pacotes enviados para esse porto serão encaminhados para o servidor. Permitindo o raspberry conectar com o servidor.

A seguir a criar o socket é iniciado uma thread. Essa thread irá para uma função que conectará este programa ao configurador. Depois de iniciar a thread, o programa ficará a ouvir o socket à espera de receber um pacote de uma máquina que se queira conectar ao servidor. No caso de existir alguma a querer-se conectar, ao servidor aceita a ligação e envia uma primeira mensagem a verificar se é o watchdog que se conectou ou não. Caso seja o watchdog, mete uma variável que indica que está conectado para verdadeiro, e chama a função *comunicação*. No caso de não ser o watchdog, fecha a ligação e fica outra vez à espera de algum dispositivo que esteja a tentar conectar.

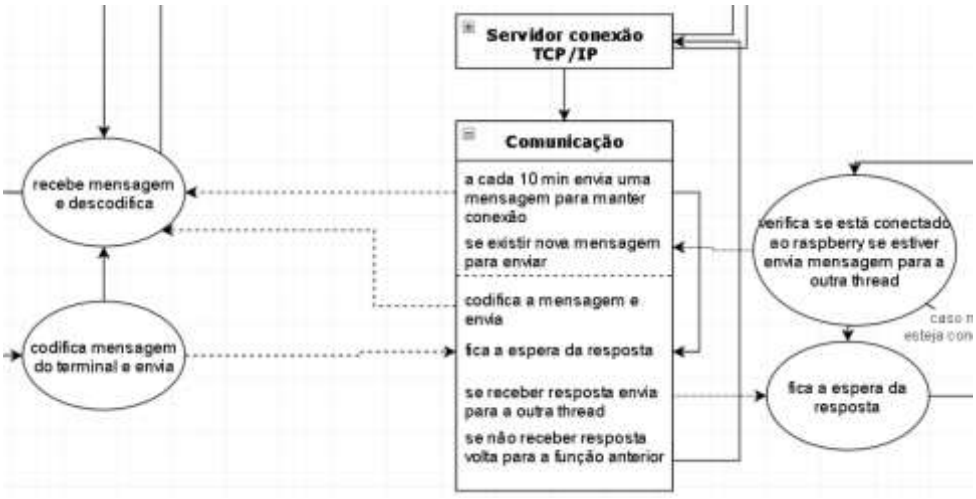


Figura 103 – Função comunicação do programa no servidor para rede backup

Na função *comunicação (*Figura 103*)* haverá um ciclo, que consiste em estar de 10 em 10 minutos a enviar uma mensagem para o raspberry pi. Esta mensagem serve como verificação se ainda existe conexão. Além da mensagem de verificação de conexão, irá estar constantemente a verificar se existe uma mensagem do configurador para enviar.

Quando existir uma nova mensagem do configurador para enviar, vai codificar a mensagem e enviá-la para o raspberry, ficando depois à espera de uma resposta; se receber resposta envia para a outra thread e volta para o ciclo de espera por uma nova mensagem para enviar. Se não receber resposta considera que a conexão acabou, colocando a variável que indica que está conectado a “falso” e volta para o código onde se estabelece a conexão.

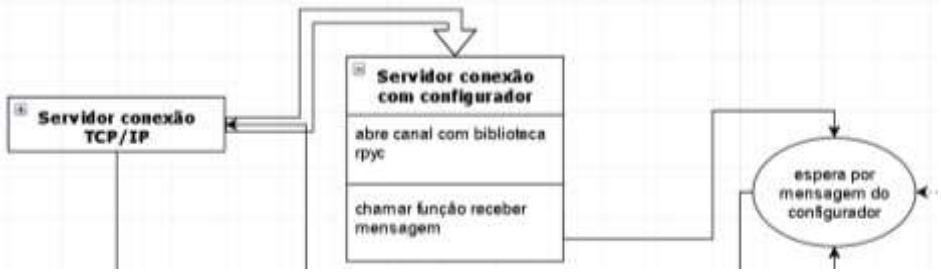


Figura 104 – Função que liga configurador à rede backup

Nesta função (Figura 104) vai fazer o uso da biblIoTeca rpyc, que serve para comunicação entre processos ou programas diferentes no mesmo dispositivo ou em dispositivos diferentes.

Com esta biblIoTeca a função irá abrir um canal de comunicação, para onde o configurador poderá enviar mensagens. No final de abrir o canal abre uma função que fica á espera que uma mensagem seja recebida.

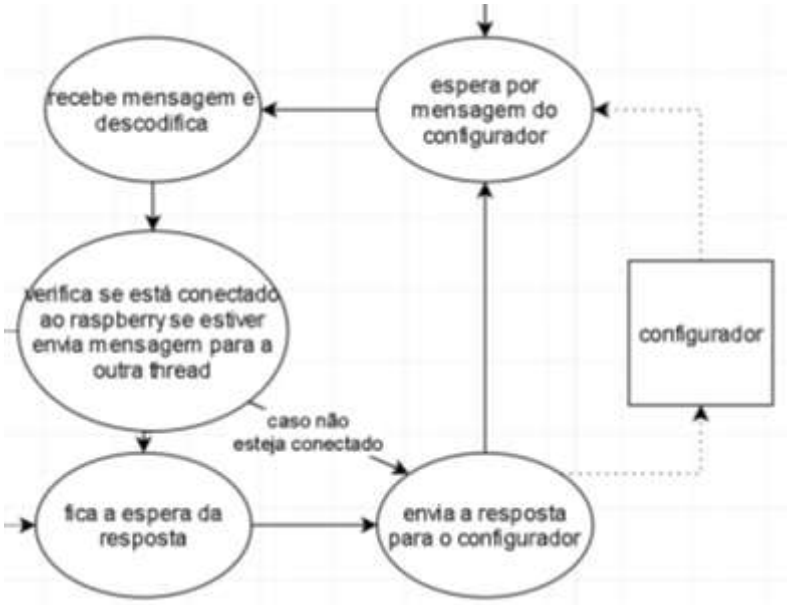


Figura 105 – Ciclo da função liga configurador à rede backup

Nesta função (Figura 105) fica à espera de receber uma mensagem. No momento em que a recebe irá descodificá-la, verificando posteriormente se a mensagem é a perguntar se está conectado ou é outra. Se a mensagem for a perguntar se está conectado, simplesmente envia a resposta de volta para o configurador com o valor da variável que indica se está conectado ou não. Caso seja outra mensagem, irá verificar se está conectado, e se não estiver informa o configurador que não há conexão. No caso de haver conexão, irá enviar a mensagem para a thread que envia as mensagens ao raspberry e espera por uma resposta.

No momento em que recebe a resposta, envia-a para o configurador e volta para o estado de ficar à espera de uma nova mensagem.

6. Conclusões

Nesta dissertação começou-se por fazer uma introdução geral ao projeto PASMO, e de seguida faz-se uma apresentação de vários projetos e plataformas com objetivos semelhantes (fornecer acesso às tecnologias recentemente desenvolvidas na investigação para todos poderem utilizar). O objetivo ao disponibilizar as tecnologias mais recentes para todos, é de se conseguir acelerar o desenvolvimento e a introdução das mesmas no dia a dia dos cidadãos. Devido ao aumento de interesse nestes projetos e em plataformas abertas ao público, na Europa foi criada a organização Enoll que apoia, acompanha e ajuda no desenvolvimento deste tipo de projetos e plataformas.

Foram então explicadas as tecnologias que se utilizam neste projeto (e tecnologias semelhantes), para se conseguir entender melhor o que o projeto fornece. É então explanado o que o projeto contém, onde é colocado e as áreas que cada uma das tecnologias utilizadas no projeto abrangem.

De seguida fez-se a apresentação do trabalho que foi desenvolvido, quais as restrições e objetivos, apresentam-se os testes feitos. Nos testes de Wi-Fi foi estudado quanto o alcance e a largura de banda são afetados pelas alterações climatéricas. O que se acabou por verificar foi que as variações do clima não afetam o alcance nos limites em que foi estudado, e quanto à largura de banda afeta pouco até aos 450 metros, já que apenas aos 500 metros se consegue notar alguma diferença mais significativa nos valores obtidos. Também se estudou o efeito de vários dispositivos na mesma rede, mas concluiu-se que o dispositivo específico é o que faz mais diferença nos resultados.

Nos testes de LoRa fez-se um estudo do local em que se devia colocar o sensor em relação ao carro. Verificou-se que o melhor lugar era num local mais distante do centro do carro, mas que possa ficar sempre por baixo, quaisquer que sejam as suas dimensões. Então, foi concluído que o melhor local para o sensor em estacionamentos de espinha é entre os 0,75 a 1,25 metros do passeio, enquanto que nos estacionamentos em paralelo já deveria ser colocado entre 0,4 a 0,7 metros do passeio. Estas medidas foram calculadas de forma a garantir que ficaria de baixo do veículo, mas não ficaria localizado no centro dele, para aumentar o alcance de comunicação.

Depois foi feito o estudo de alcance a várias condições temporais e verificou-se que o alcance é bastante afetado pela variação do clima, em que poderia variar de pouco mais de 75 metros até alcances superiores a 150 metros. Mas, ao analisar os resultados verificou-se que situações em que teríamos alcance inferior a 100 metros eram raras, por isso considerou-se que o alcance do sensor seria de 100 metros.

São então apresentados os resultados do trabalho. Usando resultados dos testes feitos criaram-se duas opções de localização para os APs, uma opção de localização para os gateways LoRa e a localizações dos RSUs.

De seguida, nos resultados, foi apresentado o sistema de heartbeat, em que se começa por apresentar o circuito eletrónico desenhado para o controlo do hard reset. Foram apresentadas duas opções (uma mais complexa que a outra). De seguida fez-se o estudo do circuito da solução mais simples.

A seguir são apresentadas três diferentes soluções para o watchdog e indicados os materiais, bem como as vantagens e as desvantagens de cada solução. É de seguida apresentado o programa desenvolvido para um watchdog com sistema operativo e com comunicação. Esse programa está desenhado para controlar um AP, e é explicado o seu funcionamento, como controla o AP e como está programado para atuar no caso de ocorrer erros no AP. É explicado porque o programa está feito de forma a que sempre que é necessário fazer um hard reset, é primeiro desligado o watchdog e de seguida cortada a energia. Isso está feito dessa maneira de forma a proteger o equipamento, pois pode danificar o sistema heartbeat se se remover a energia enquanto ele está em funcionamento, logo para reduzir o risco desse acontecimento, é desligado o watchdog antes do corte de energia.

Estão também apresentadas formas de aumentar a fiabilidade do sistema heartbeat (incluindo formas de proteger da chuva, poeira, temperatura, radiações eletromagnéticas, descargas elétricas e ruído na alimentação).

É então exposto como funciona o sistema de rede. Aí é apresentado o configurador que é um programa de interface gráfica, de onde se pode comunicar com os vários watchdogs. Esse programa já está feito de forma a comunicar com os watchdogs por internet sempre que possível, e para o caso de não haver conexão por internet, ele faz automaticamente a conexão pela rede de backup. Também permite a interação com vários watchdogs ao mesmo tempo, simplificando o controlo de cada um.

Por fim é apresentado como funciona a rede de backup, em que a conexão é feita através de TCP/IP entre o watchdog e o servidor, estando essa conexão circunscrita ao envio de mensagens simples.

Ao completar as várias componentes deste trabalho verificaram-se algumas partes que se poderiam melhorar ou escolher uma solução diferente.

- Nos testes realizados poder-se-ia aumentar o número de testes e estudar outras variáveis que pudessem afetar o resultado dos testes, para se conseguir perceber o que pode influenciar os resultados mais precisamente e o quanto influenciava cada variável.
- No watchdog poder-se-ia estudar qual é a eficácia da solução desenvolvida fazendo um estudo da sua fiabilidade, verificando quanto tempo a solução consegue manter o sistema a funcionar corretamente sem nenhuma interação de pessoas, e estudar mais e melhores formas de proteger o sistema.
- No configurador foi adotada a solução de criar um programa de interface gráfica para controlar os watchdogs. Pode ser alterado o sistema de controlo em vez de correr num programa correr num site, mas essa opção, dependendo dos objetivos, pode não ser considerada uma melhoria, mas simplesmente uma solução diferente.
- O sistema de rede de backup também poderia ser alterado para uma solução que não exigisse a conexão constante entre o watchdog e o servidor. Desenvolver uma solução em que o watchdog poderia ser acedido pelo servidor a qualquer momento, sem que se necessitasse de ter um canal de comunicação constantemente aberto, sendo o canal aberto apenas no momento em que fosse necessária a utilização da rede backup.

Esta solução teria o problema de que o watchdog estaria exposto para qualquer um aceder, se não fossem colocadas as seguranças devidas, o que iria criar uma falha na segurança no watchdog. Para isso uma solução seria o watchdog conectar-se na mesma VPN que o servidor.

E a solução de comunicação em vez da TCP/IP feita, podia usar uma conexão com SSH. Teria de ser visto se a quantidade de dados que se usava nessa conexão, porém como a rede backup é apenas usada para situações em que existe problemas com a internet (que não deverão ser muito frequentes).

Como deverá ser raro usar a rede backup não será necessário uma conexão com a liberdade que o SSH apresenta, e interessa que nesta conexão se limite a quantidade de dados transmitidos, devido a conexão ter restrições do contrato com a operadora. Por isso, a solução apresentada como tem alguma liberdade de interação, mas restringe a quantidade de dados que se usa na comunicação, é uma boa solução para esta conexão.

Bibliografia

[1] IoT, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7689a1081d09, Março 2018

[2] IoT, https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/, Março 2018

[3] sigfox, https://www.sigfox.com/en/sigfox-story, Março 2018

[4] sigfox, https://www.sigfox.com/en/sigfox-IoT-technology-overview, Março 2018

[5] LoRa, Konstantin Mikhaylov, Juha Petäjäjärvi, Tuomo Hänninen. "Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology". European Wireless 2016

[6] LoRa, Juha Petäjäjärvi, Konstantin Mikhaylov, Antti Roivainen, Tuomo Hänninen, Marko Pettissalo. "On the Coverage of LPWANs: Range Evaluation and Channel Attenuation Model for LoRa Technology". 2015 14th International Conference on ITS Telecommunications (ITST)

[7] IEEE 802.11p e IEEE 802.16e, Priyanka Tiwari, Rajendra Singh Kushwah. "Traffic Analysis for VANET using WAVE and WiMAX". 2015 International Conference on Communication Networks (ICCN)

[8] IEEE 802.11p e IEEE 802.16e, R. Bhakthavathsalam, Starakjeet Nayak. "Operational Inferences on VANETs in 802.16e and 802.11p with Improved Performance by Congestion Alert". The 8th Annual IEEE Consumer Communications and Networking Conference - Special Session Information Dissemination in Vehicular Networks

[9] IEEE 802.11ac e IEEE 802.11n, Cisco and/or its affiliates, "802.11ac: The Fifth Generation of Wi-Fi", Technical White Paper March 2014

[10] IEEE 802.11, Marcelo G. Rubinstein e José Ferreira de Rezende, "Qualidade de Serviço em Redes 802.11", Universidade Estadual do Rio de Janeiro

[11] IEEE 802.11ac, NETSCOUT, "White Paper: IEEE 802.11ac Migration Guide"

[12] LTE, https://www.frequencycheck.com/countries/portugal, Março 2018

[13] LTE, C. Gessner, A. Roessler, M. Kottkamp, "UMTS Long Term Evolution (LTE) - Technology Introduction", ROHDE&SCHWARZ July 2012.

[14] SC-FDMA, https://blog.3g4g.co.uk/2009/02/ofdm-and-sc-fdma.html, Março 2018

[15] Smartsantander, http://www.smartsantander.eu/index.php/testbeds, Abril 2018

[16] DRIVE-IN, http://www.cmuportugal.org/tiercontent.aspx?id=1552, Abril 2018

[17] Cidades futuras, http://3decide.com/pt-pt/showcases/futurecitiesproject/, Abril 2018

[18] Laboratório em Ann Arbor, https://www.mlive.com/news/ann-arbor/index.ssf/2014/04/transportation.html, Abril 2018

[19] PASMO, http://www.cm-ilhavo.pt/pages/2371?news_id=2825, Maio 2018

[20] Monoestável, http://pt.farnell.com/texas-instruments/cd74hc123e/multivibrator-reset-pdip16-7v/dp/1287430?st=monostable, Março 2018

[21] Relé, http://www.botnroll.com/pt/digital/455-modulo-rele-8-canais-5v-em-linha.html?search_query=rele+3v&results=87, Março 2018

[22] Alimentação Arduíno, http://www.botnroll.com/pt/alimentadores-acdc-12v/477-alimentador-ac-dc-12v-2a.html, Março 2018

[23] Ethernet extensão, http://www.botnroll.com/pt/shield-comunicacoes/758-arduino-ethernet-shield-w5100.html, Março 2018

[24] Extensão GSM/LTE, http://www.botnroll.com/pt/shield-comunicacoes/2846-sim7000c-arduino-nb-IoT-lte-gprs-gps-expansion-shield.html, Maio 2018

[25] Extensão RS232, http://www.botnroll.com/pt/shield-comunicacoes/2359-shield-rs232485-para-arduino-.html, Maio 2018

[26] Single board computer, https://pcengines.ch/apu3b4.htm, Maio 2018

[27] Cabo Ethernet, https://www.electrofun.pt/cabos-condutores/cabo-de-rede-ethernet-rj45-cat5-1m, Março 2018

[28] Cabo USB para RS232, https://www.electrofun.pt/cabos-condutores/cabo-adaptador-conversor-usb-para-ttl-rs232-pl2303hx, Março 2018

[29] Datasheet Banana Pi, http://www.produktinfo.conrad.com/datenblaetter/1500000-1599999/001573546-da-01-en-BANANA_PI_R2_ROUTER_BOARD.pdf, Setembro 2018

[30] Datasheet AIMB-215, http://downloadt.advantech.com/ProductFile/PIS/AIMB-215%20B1/Product%20-%20Datasheet/AIMB-215%20B1_DS(03.23.15)20150410141323.pdf, Setembro 2018

[31] Datasheet Mitac, http://client.mitac.com/pdf/PD10AI.pdf, Setembro 2018

[32] Outros SBCs, https://all3dp.com/1/single-board-computer-raspberry-pi-alternative/, Setembro 2018

[33] AV living lab, http://avlivinglab.com/, Outubro 2018

[34] Catalonia living lab, http://catalonialivinglab.com/, Outubro 2018

[35] IoT living lab, http://IoTlivinglab.com/, Outubro 2018

[36] Enoll, https://enoll.org/, Outubro 2018

[37] Extensão RPI3, https://www.botnroll.com/pt/gsm/2653-gsm-gprs-gnss-bluetooth-hat-para-raspberry-pi.html, Outubro 2018

[38] Alimentação RPI3, https://www.botnroll.com/pt/alimentadores-acdc-5v/2902-fonte-de-alimenta-o-5v-2-5a-p-raspberry-pi.html, Outubro 2018

[39] RPI3, https://www.botnroll.com/pt/raspberry-pi/1499-raspberry-pi-3-modelo-b-.html, Outubro 2018

[40] Controlo, https://en.wikipedia.org/wiki/Control_engineering, Novembro 2018

[41] Fiabilidade, https://en.wikipedia.org/wiki/Reliability_engineering#Basics_of_a_reliability_assessment, Novembro 2018

[42] Watchdog, https://en.wikipedia.org/wiki/Watchdog_timer, Novembro 2018

[43] SIM900, http://simcomm2m.com/En/module/detail.aspx?id=71, Novembro 2018

[44] SIM900 comandos, SIMCom, “SIM900_AT Command Manual_V1.03”, 24 de dezembro de 2010

[45] Synchonicity, https://synchronicity-IoT.eu/, Outubro 2018

[46] Enoll projects, https://enoll.org/projects/, Outubro 2018

[47] RPMA, https://www.ingenu.com/technology/rpma/, Março 2018

[48] Weightless, http://www.weightless.org/about/weightless-specification, Março 2018

[49] NB-FI, https://wavIoT.com/technology/what-is-nb-fi, Março 2018

[50] HyperLAN, https://en.wikipedia.org/wiki/HiperLAN, Dezembro 2018

[51] Gaiola de faraday, https://www.mundodaeletrica.com.br/gaiola-de-faraday-o-que-e-qual-a-sua-aplicacao/, Novembro 2018

[52] Índice de proteção IP, http://www.omegatrafo.com.br/ip.pdf, Novembro 2018

[53] Watchdog circuito, https://pt.farnell.com/w/search/prl/results?st=watchdog, Maio 2018

[54] WiReboot, https://www.cnx-software.com/2016/07/04/wireboot-is-a-watchdog-device-rebooting-your-router-if-the-wifi-connection-is-lost-crowdfunding/, Maio 2018

Anexo

1. *Componentes do circuito*

i. Componentes para contruir circuito inicial

Nome	Quantidade	Imagem
CD74HC123E - Monostable Multivibrator [20]	1	
Módulo Relé 1 canal 5V compatível com Arduíno [21]	1	

Tabela 13 – Componentes do circuito sem condensadores e resistências

As resistências e condensadores não foram adicionadas a lista de compra inicial devido á Universidade de Aveiro disponibilizar, e sem fazer testes com o circuito não se sabia os valores que se iria usar.

ii. Componentes para contruir circuito final (segunda solução)

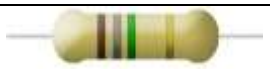
Nome	Quantidade	Imagem
Resistência 1M8Ω	1	
Resistência 10KΩ	1	
Condensador 100µF	1	
CD74HC123E - Monostable Multivibrator [20]	1	
Módulo Relé 1 canal 5V compatível com Arduíno [21]	1	

Tabela 14 – Componentes do circuito final segunda solução

2. *Componentes para Watchdog*

i. Watchdog opção 1

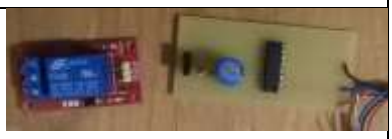
Nome	Quantidade	Imagem
Arduíno uno	1	
Circuito eletrónico	1	
Alimentador 12V 2A [22]	1	
Extensão de Ethernet para Arduíno [23]	1	
Cabo Ethernet [27]	1	

Tabela 15 – Componentes para watchdog opção 1

ii. Watchdog opção 2

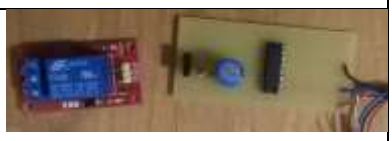
Nome	Quantidade	Imagem
Arduíno uno	1	
Circuito eletrónico	1	
Alimentador 12V 2A [22]	1	
Extensão de Ethernet para Arduíno [23]	1	
Cabo Ethernet [27]	1	
Extensão LTE/GSM [24]	1	
Cartão SIM	1	
Extensão RS485 [25]	1	

Tabela 16 – Componentes para watchdog opção 2

iii. Watchdog opção 3

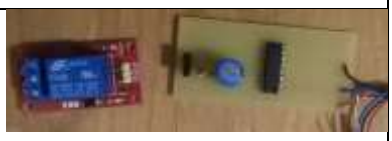
Nome	Quantidade	Imagem
Raspberry Pi 3 [39]	1	
Circuito eletrónico	1	
Extensão de GSM [37]	1	
Fonte de alimentação [38]	1	
Cartão SIM	1	
Cabo Ethernet [27]	1	
Cabo USB para RS232 [28]	1	

Tabela 17 – Componentes para watchdog opção 3