FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

FEUP

Avaliação da rede Homeplug para suporte de aplicações industriais

João Pedro Gonçalves Lemos

Mestrado Integrado em Engenharia Electrotécnica e de Computadores, Major Automação

Orientador: Paulo José Portugal (Prof. Doutor)

27 de Junho de 2011

Resumo

Esta dissertação apresenta um estudo sobre o desempenho da rede Homeplug para suporte de aplicações industriais, focado essencialmente em quatro parâmetros: a largura de banda, a taxa de perda de pacotes, a latência e o jitter.

Com esta dissertação pretende-se avaliar a capacidade da tecnologia Power Line Communications, para operar em ambientes industriais. A principal vantagem desta tecnologia é a utilização da rede eléctrica já existente para transporte de dados, eliminando assim os custos de instalação e manutenção de uma rede exclusiva para o transporte de informação.

Para a realização dos testes de desempenho da rede, e de forma a garantir a sua repetibilidade, e controlo das condições de execução, é apresentada uma *Test Bed* laboratorial. Esta *Test Bed* consiste num troço de rede eléctrica isolado de interferências electromagnéticas externas, onde são conectados os módulos de comunicação e as diferentes cargas eléctricas, consoante o cenário de teste.

Para obtenção das medidas das características apresentadas, são efectuados testes com tráfego TCP e UDP aperiódico, bem como tráfego UDP representativo de tráfego industrial isolado ou na presença de outros tipos de tráfegos, para duas ou três estações na rede.

Os resultados obtidos demonstram que a rede Homeplug poderá ser uma boa alternativa às soluções existentes, desde que as aplicações a executar na rede não possuam restrições temporais demasiado exigentes, como tempos de latência inferiores a 1 milisegundo, ou valores de jitter inferiores a 100 microsegundos.

Abstract

This thesis presents a study about the performance of a Homeplug based network to support industry applications, focused mainly on four parameters, which are the bandwidth, the rate of packet loss, the latency and the jitter associated with data transmission.

The main objective of this thesis is to evaluate the usability of the Power Line Communications technology in industrial environments. The main advantage of this technology is using the existing electrical network for transporting data, eliminating the costs of installing and maintaining a network exclusively for data transportation.

To accomplish the performance tests, and to ensure its repeatability, a Test Bed is implemented. This Test Bed consists of a section of the power line, isolated from external noise, where the communication modules and different electrical loads are connected, depending on the test scenario.

To obtain the values of the presented characteristics, the tests are divided into two groups. The first one consists of transmitting aperiodic TCP and UDP traffic, and the second one in transmitting only periodic UDP traffic or periodic UDP traffic in the presence of other types of traffic, for two or three stations connected to the network.

The obtained results show that the Homeplug network may be a good alternative to the existing solutions, as long as the applications running on the network do not have too tight time constraints, like needing a Delay less than 1 ms or a Jitter under 0.1 ms.

Agradecimentos

A si, Prof. Doutor Paulo José Portugal, pela competência com que orientou a minha Dissertação, pela partilha de conhecimento, críticas e sugestões, tanto atempadas como construtivas e, pelo profissionalismo demonstrado. Um muito obrigado!

Um sentido agradecimento ao Prof. Doutor António Pina Martins, pelas suas breves, mas doutas indicações na montagem da Test Bed.

Aos meus colegas, pela partilha do laboratório, pelas dores de cabeça conjuntas e pela divertida e descontraída convivência que tornaram as pequenas (e grandes) dificuldades mais fáceis de superar!

A ti, madrinha pela compreensão em todos os momentos, mas principalmente, neste último mês. Por seres sempre tão amiga e pelo teu voto de confiança!

A ti Li, pelos dias perdidos à volta do computador, pelo apoio incondicional, paciência (muita!) motivação e inspiração, e por acreditares em mim.

E a vocês, pai e mãe... por tudo!

A todos os demais... O meu sincero obrigado!

João Lemos

"Mudam-se os tempos, mudam-se as vontades,
Muda-se o ser, muda-se a confiança;
Todo o mundo é composto de mudança,
Tomando sempre novas qualidades."

Luís de Camões

Índice

Lista de Figuras

Lista de Tabelas

Abreviaturas e Símbolos

ACK	*Acknowledge*
ADSL	*Asymmetric Digital Subscriber Line*
AES	*Advanced Encryption Standard*
AFE	*Analog Front End*
AGC	*Automatic Gain Controller*
ARQ	*Automatic Repeat Request*
AVLN	*HomePlug AV Logic Network*
BMC	*Best Master Clock*
BPSK	*Binary Phase Shift Keying*
CA	*Collision Avoidance*
CB	*Contention Based*
CCo	*Central Coordinator*
CDCR	*Collision Detection and Collision Resolution*
CENELEC	*European Committee for Electrotechnical Standardization*
CF	*Contention Free*
CL	*Convergence Layer*
CM	*Connection Manager*
CRT	*Cathode Ray Tube*
CSMA	*Carrier Sense Multiple Access*
CSPEC	*Connection Specification*
DBPSK	*Differential Binary Phase Shift Keying*
DC	*Deferral Counter*
DEEC	Departamento de Engenharia Electrotécnica e de Computadores
DES	*Data Encryption Standard*
DNL	*Discovered Networks List*
DQPSK	*Differential Quadrature Phase Shift Keying*
DSL	*Discovered Station List*
EIA	*Electronic Industries Alliance*
EOF	*End-of-File*
EOP	*End-of-Packet*
ETSI	*European Telecommunications Standards Institute*
FEC	*Forward Error Correction*
FEUP	Faculdade de Engenharia da Universidade do Porto
FIFO	*First In, First Out*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
IP	*Internet Protocol*
HLE	*High Layer Entity*
HPAV	*Homeplug AV*
LAN	*Local Area Network*

MAC	*Media Access Control*
MII	*Media Independent Interface*
MPDU	*MAC Protocol Data Unit*
MSDU	*MAC Sevice Data Unit*
MTU	*Maximum Transmission Unit*
NACK	*Negative Acknowledgement*
NEK	*Network Encryption Key*
NMK	*Network Membership Key*
NPW	*Network Password*
OFDM	*Orthogonal Frequency-Division Multiplexing*
OPERA	*Open PLC European Research Alliance*
OSI	*Open Systems Interconnection*
PB	*PHY Block*
PCF	*Persistent Contention Free*
PCS	*Physical Carrier Sense*
PDI	Preparação para a Dissertação
PHY	*Physical Layer*
PLC	*Power Line Communications*
PTP	*Precision Time Protocol*
PUA	*PLC Utilities Alliance*
QAM	*Quadrature Amplitude Modulation*
QoS	*Quality of Service*
rMII	*Reduced Media Independent Interface*
RTT	*Round Trip Time*
ROBO	*Robust Orthogonal Frequency-Division Multiplexing*
SACK	*Selective Acknowledge*
SAP	*Service Access Point*
SOF	*Start-of-Frame*
TCP	*Transmission Control Protocol*
TDMA	*Time Division Multiple Access*
TXOP	*Transmit Opportunity*
UC	Unidade Curricular
UDP	*User Datagram Protocol*
UPA	*Universal Powerline Association*
USB	*Universal Serial Bus*
VCS	*Virtual Carrier Sense*
VLAN	*Virtual Local Area Network*

Capítulo 1

Introdução

As comunicações industriais atingiram, na actualidade, um patamar de grande importância. Actualmente são raros os equipamentos industriais que operam individualmente e sem comunicação com unidades de controlo, sensores de aquisição, actuadores ou outros tipos de equipamentos.

Com o aparecimento de novas tecnologias, e devido ao elevado custo da instalação de novas cablagens numa estrutura empresarial, opta-se cada vez mais por tecnologias que não necessitem de uma reestruturação da camada física da rede de comunicações existente, sempre que se adicione ou retire um equipamento à rede já existente.

Uma das opções disponíveis para tentar reduzir os custos com instalações de redes de cabos e proporcionar uma rede mais flexível, é a utilização das linhas de distribuição de energia eléctrica para o transporte de dados.

Esta tecnologia, denominada de *Power Line Communications*, já está largamente implementada a nível de comunicações domésticas, não acontecendo o mesmo a nível industrial devido a várias limitações nas soluções disponíveis no mercado, tais como os elevados tempos de latência e de jitter.

Das soluções existentes, optou-se por estudar o Homeplug, pelo facto de ser uma tecnologia relativamente recente, em expansão e com poucos estudos sobre o seu desempenho a nível industrial. Além disso, o aprofundamento dos conhecimentos nesta área, torna-se aliciante pela sua utilidade, podendo ser uma forma de revolucionar as comunicações a nível industrial.

No desenvolvimento desta dissertação pretende-se avaliar o desempenho de uma rede *Homeplug* para suporte de aplicações industriais.

1.1 Objectivos

Com esta dissertação pretende-se avaliar o desempenho de uma rede *Homeplug* para suporte de aplicações industriais.

Este objectivo principal pode ser dividido em duas vertentes. a primeira prende-se com a implementação e realização de vários testes e medições numa rede *Homeplug* implementada na rede eléctrica do Laboratório, onde não existe controlo sobre os equipamentos conectados à rede. A segunda, está relacionada com a realização dos testes num ambiente controlado, onde são conectadas diferentes cargas na rede eléctrica com o intuito de testar a imunidade às interferências eléctricas provocadas por diferentes equipamentos.

Para além dos diferentes cenários, pretende-se ainda verificar o desempenho da rede para diferentes tipos de tráfego, tendo sido utilizado tráfego TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*) aperiódico para a avaliação dum desempenho geral da rede. Seguidamente é utilizado tráfego UDP periódico, de modo a simular o tráfego utilizado por aplicações industriais.

Com esta divisão, pretende-se que o primeiro objectivo tenha um carácter mais prático, acompanhado da configuração da rede, realização de medições, injecção de interferências na rede, etc.

A segunda parte do trabalho tem um objectivo mais teórico, onde são tratados os resultados obtidos e calculados os parâmetros verificados na transferência de dados na rede, como a largura de banda, a taxa de perda de pacotes, a latência e o *Jitter*.

1.2 Estrutura da Dissertação

Esta dissertação está estruturada em 6 capítulos, sendo este o primeiro, no qual é feita uma breve introdução ao tema da mesma e são apresentados os seus objectivos.

O capítulo 2 introduz a tecnologia PLC (*Power Line Communications*) referindo algumas das soluções existentes actualmente no mercado. São também apresentados os principais aspectos desta tecnologia e são abordados alguns dos *standards* que a regulamentam.

No capítulo 3 é apresentada a tecnologia a utilizar no decorrer desta dissertação, o *Homeplug*. São indicados os principais aspectos de funcionamento da mesma e quais as vantagens e dificuldades da sua utilização. Como a utilização da tecnologia *Homeplug* vais ser a parte fulcral deste trabalho, este capítulo apresenta ainda uma análise comparativa entre os protocolos *Homeplug 1.0* e *Homeplug AV*.

No capítulo 4 serão apresentadas as principais ferramentas utilizadas, bem como toda a metodologia utilizada para a realização dos testes.

Seguidamente, no capítulo 5 serão exibidos os resultados obtidos e discutidos os principais aspectos de cada um.

Por último, no capítulo 6, procede-se às principais conclusões retiradas do trabalho efectuado, bem como sugestões de possíveis trabalhos futuros.

Capítulo 2

Power Line Communications

Neste capítulo será apresentada a tecnologia PLC, para tal, é efectuada uma breve contextualização histórica desta tecnologia, são apresentados alguns dos *standards* existentes e entidades responsáveis pelo seu desenvolvimento.

Por fim apresenta-se uma brevemente descrição de algumas das soluções existentes no mercado para implementação desta tecnologia, à excepção da tecnologia *Homeplug*, que será discutido no capítulo 3.

2.1 Power Line Communications

A tecnologia *Power Line Communications* começou a ser desenvolvida com o intuito de rentabilizar a rede eléctrica já existente em edifícios e em redes de distribuição de energia.

O grande motivo impulsionador do desenvolvimento e aposta nesta tecnologia é a facilidade de implementação de uma nova rede, utilizando para isso a rede eléctrica já existente, ou seja, não é necessário instalar novos cabos, o que por vezes, devido a vários factores é uma tarefa bastante complicada, demorada e altamente dispendiosa, senão mesmo impossível em situações extremas, como a impossibilidade de alterar fisicamente a estrutura do edifício.

Com o desenvolvimento desta tecnologia pretende-se utilizar a rede eléctrica que, para além do seu objectivo primordial, que é o transporte de energia, transportar sinais de dados, o que permite monitorizar e até controlar todos os equipamentos que estejam ligados à rede eléctrica.

A implementação desta tecnologia teve início na década de 1910, com os sistemas de *Power Line Carrier*, devido à necessidade das empresas distribuidoras de energia em controlar e monitorizar as suas linhas. Esta tecnologia foi inicialmente desenvolvida linhas de alta e muito alta tensão, pois estas atravessam zonas tipicamente pouco povoadas e de difícil acesso. Esta tecnologia consistia em incorporar os dados a serem transmitidos, numa portadora que funcionava com frequências entre os 50 kHz e os 500 kHz. A modulação era efectuada recorrendo a técnicas de

modulação de amplitude e eram incluídos nesta modulação os sinais de áudio, protecção e frequência piloto, para a detecção de falhas na transmissão. Esta solução foi então adoptada por várias empresas para comunicação entre as suas subestações, mas que foi posteriormente abandonada devido ao desenvolvimento tecnológico e principalmente à diminuição do preço da fibra óptica.

Por volta de 1930, começaram a surgir os primeiros sistemas PLC, com comunicação bidireccional e funcionando numa gama de frequências dos 3 kHz aos 148.5 kHz. Estes sistemas funcionavam predominantemente a baixa tensão, com intuito de possibilitar leituras remotas, bem como integrarem aplicações relacionadas com a domótica.

Outro factor que impulsionou em grande escala o desenvolvimento da tecnologia PLC foi o fim da Segunda Guerra Mundial, em 1945, pois nesta altura grande parte das linhas telefónicas tinham sido destruídas existindo assim muito mais infra-estruturas da rede eléctrica disponíveis.

Em 1950 surgiu o primeiro sistema PLC, designado de *Ripple Control*, desenhado e implementado em linhas de média e baixa tensão. A onda portadora destes sistemas funcionava a frequências entre os 100 Hz e 1 kHz e era necessário definir o sentido da comunicação através de sinais de controlo. Uma década depois, apareceu em França, o primeiro sistema PLC industrial, que foi apelidado de *Pulsadis* [1].

Tal como qualquer tipo de tecnologia, o PLC tem vantagens e desvantagens decorrentes da sua utilização. No campo das desvantagens podemos destacar como principais as interferências electromagnéticas, sobretudo quando se pretende uma grande largura de banda e a dificuldade em garantir uma boa qualidade do serviço. Estes aspectos têm vindo a ser gradualmente colmatados com a optimização das técnicas utilizadas para modulação de sinais.

Por outro lado a tecnologia PLC apresenta grandes vantagens, nomeadamente: a utilização da rede eléctrica já existente, a sua rápida implementação, pois não necessita de instalação de novos cabos e permite uma encriptação de dados bastante robusta, assegurando assim a confidencialidade e segurança nos dados transmitidos.

Este tipo de tecnologia pode ser dividido segundo a sua aplicação, em dois grandes campos, sendo estes: a utilização da rede de distribuição de energia para interligação de edifícios e fornecimento de internet. E a aplicação em redes dentro do mesmo edifício, com especial ênfase no controlo centralizado e a automatização de equipamentos, como sistemas de controlo de temperatura, sistemas de iluminação, monitorização de equipamentos e controlo de processos industriais. Durante o decorrer deste trabalho apenas serão focados os aspectos das redes dentro do mesmo edifício.

2.2 Regulamentação

Com o aparecimento dos vários sistemas PLC, apareceu também a necessidade de criar *standards* de modo a assegurar a segurança dos utilizadores, a interoperabilidade entre equipamentos de diferentes fabricantes e minimizar o impacto da utilização desta tecnologia nas tecnologias já existentes e implementadas no mercado.

Apesar desta tecnologia já não ser nova, ainda não existem no mercado *standards* globais para redes PLC, contudo existem várias entidades envolvidas neste processo e foram já criadas algumas normas que estão a ser estudadas de modo a que se encontre um *standard* global.

Também a nível geográfico, dependendo do local onde é implementada a tecnologia existem divergências, pois a regulamentação existente na Europa não é a mesma que a existe noutras zonas, como a América ou a Ásia. A nível Europeu o CENELEC (*European Committee for Electrotechnical Standardization*) criou o *standard* EN50065 [2], que define a banda de frequências para comunicações na rede eléctrica, a amplitude máxima do sinal e os limites de interferências com as bandas de frequência adjacentes, como pode ser visto na Tabela 5.1. Estas indicações diferem significativamente das apresentadas nas normas aplicadas na América ou na Ásia, que permitem um espectro de frequências até 500 kHz, principalmente devido à não utilização destas frequências para rádio transmissões [3].

Tabela 2.1: Distribuição das bandas de frequências para redes PLC Europeias [3]

Banda	Frequência	Utilização
	3 KHz – 9 kHz	Disponível apenas para empresas de distribuição de energia eléctrica
A	9 KHz – 95 kHz	Disponível para empresas de distribuição de energia eléctrica e entidades autorizadas
B	95 KHz – 125 kHz	Disponível para consumidores, sem restrições
C	125 KHz – 140 kHz	Disponível para consumidores, desde que possuam MAC (*Media Access Control*)
D	140 KHz – 148.5 kHz	Disponível para consumidores, sem restrições

Como se pode verificar, a norma do CENELEC restringe bastante a largura de banda para transferência de dados através da rede eléctrica, que, apesar de ser suficiente para alguns tipos de aplicações, como leituras remotas e controlo da carga numa rede eléctrica, não o é para outros tipos de aplicações, como redes de telecomunicações. Para solucionar este problema, surgiram várias associações e instituições na tentativa criar *standards* para a utilização de redes PLC a frequências superiores. Dentro destas instituições podemos destacar as seguintes: IEEE (*Institute of Electrical and Electronics Engineers*), OPERA (*Open PLC European Research Alliance*), PLCForum (*PowerLine Communications Forum*), PUA (*PLC Utilities Alliance*), UPA (*Universal Powerline Association*) e a *HomePlug Alliance*.

2.2.1 IEEE (*Institute of Electrical and Electronics Engineers*)

O IEEE [4] é a maior associação profissional internacional e uma das maiores autoridades nos sectores da computação e telecomunicações, energia eléctrica, robótica, aeronáutica e tecnologias biomédicas.

A principal missão do IEEE é fomentar a inovação tecnológica para o benefício da humanidade. Como tal, e sendo o PLC uma tecnologia com elevado potencial, foi criado um Comité Internacional para regulamentação das comunicações sobre a rede eléctrica. Este comité publicou

em 31 de Dezembro de 2010 o *standard* IEEE Std 1901-2010 [5], que regulamenta a implementação das camadas MAC (*Media Access Control*) e PHY (*Physical Layer*), para comunicações de banda larga em redes eléctricas.

2.2.2 OPERA (*Open PLC European Research Alliance*)

OPERA é um consorcio constituído por 26 participantes, que integram todos os tipos de organizações no desenvolvimento da tecnologia PLC, sendo estes, Indústria Eléctrica, Investigadores e Produtores, Universidades, Operadores PLC e Empresas de Engenharia e Consultadoria.

Munindo-se dos conhecimentos nas diversas áreas, este consorcio foi criado segundo o objectivo "*Becoming a real alternative to existing broadband technologies, PLC will enhance safety of communications and supply a real alternative to the customers, increasing competitiveness*" [6].

Este projecto teve a duração de 4 anos, e foi dividido em duas fases, decorrendo a primeira entre 2004 e 2006 e a segunda entre 2007 e 2008 e culminou com a distribuição pública dos resultados obtidos no documento *D54 - Final plan for using and disseminating knowledge* [7].

2.2.3 PLCForum (*PowerLine Communications Forum*)

PLCforum é uma associação internacional, criada no ano de 2000 e constituída, à semelhança do OPERA, por elementos dos vários sectores associados à tecnologia PLC. Esta associação tem como principais objectivos, para além da troca de conhecimento entre os diversos membros, a criação de regulamentação, o desenvolvimento de nova tecnologia, a criação de oportunidades de negócio e o marketing e publicidade do potencial da tecnologia PLC [8].

2.2.4 PUA (*PLC Utilities Alliance*)

PUA é uma aliança Europeia, criada no ano de 2002, com o objectivo de aumentar a cooperação entre as empresas provedoras de serviços energéticos a nível europeu, de modo a promover e influenciar a implementação da indústria PLC na Europa.

Actualmente esta associação é constituída por 8 membros, sendo estes: EDP (Portugal), Iberdrola (Espanha), Endesa (Espanha), Enel (Itália), EnBw (Alemanha), EDF (França), Union Fenosa (Espanha) e EEF (Suíça) [9].

2.2.5 UPA (*Universal Powerline Association*)

UPA foi criada no ano de 2005, e tinha como principal objectivo promover o crescimento da tecnologia PLC, criando *standards* que permitissem a interoperabilidade entre equipamentos. Esta associação cessou as suas funções em Novembro de 2010 e alguns dos seus trabalhos foram adoptados pelo projecto OPERA [10].

2.2.6 *Homeplug Alliance*

Homeplug é uma aliança constituída por parceiros que integram todos os níveis da cadeia de valor da tecnologia PLC, integrando assim os sectores do desenvolvimento da tecnologia, mercado e serviços. O principal objectivo desta aliança é promover o desenvolvimento da tecnologia PLC a preços competitivos e o desenvolvimento de *standards* que facilitem a sua implementação no mercado [11].

Até ao momento já foram publicados os *standards Homeplug 1.0* [12], que foi posteriormente incluído no TIA-1113 [13] e foi o primeiro *standard* aprovado pela norma ANSI; o *Homeplug Turbo*; o *Homeplug AV* [14] que foi incluído no IEEE 1901 [5]; e o standard *Homeplug Green PHY* [15]. Encontra-se também em desenvolvimento o standard *Homeplug AV2* para comunicações de alta velocidade e grande largura de banda.

Para além dos meios já descritos, também o CENELEC [16], o IEC (International Electrotechnical Commission) [17] e o ETSI (European Telecommunications Standards Institute) [18] continuam a trabalhar na criação de um *standard* Europeu para a tecnologia PLC.

2.3 Protocolos PLC

Os diferentes protocolos e formas de implementar a tecnologia PLC, como em qualquer outra tecnologia, foram evoluindo ao longo do tempo, aumentando cada vez mais a velocidade e largura de banda disponíveis para transmissão de dados. Esta evolução encontra-se representada na Fig 2.1.

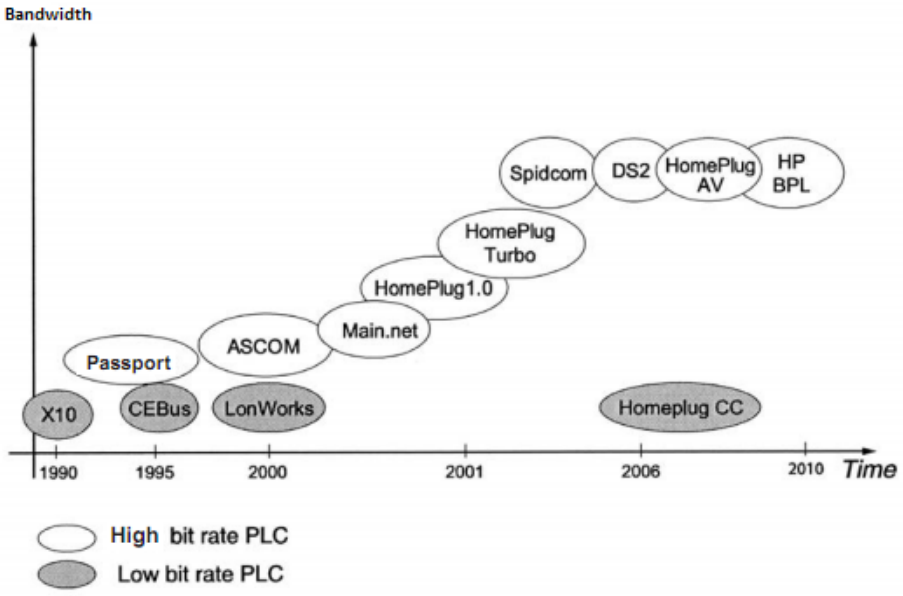

Figura 2.1: Evolução da tecnologia PLC [1]

Dos vários protocolos que foram surgindo ao longo dos anos, podem ser destacados o *X10*, o *CEBus*, o *LonWorks* e o *Homeplug*, devido à relevância que atingiram no mercado mundial.

Em seguida serão apresentadas as principais características de cada um destes protocolos.

2.3.1 X10

O protocolo *X10* foi o primeiro protocolo PLC a surgir no mercado, por volta de 1975, e foi desenvolvido pela *Pico Electronics*. Este protocolo tem como objectivo facilitar a implementação de aplicações de domótica e automação. Este protocolo permite a transmissão de dados em *broadcast* com uma largura de banda bastante reduzia (cerca de um comando por segundo), quer na linha eléctrica quer em comunicações rádio. É da responsabilidade de cada um dos módulos decidir se deve ou não responder perante o comando recebido [19].

Apesar da existência de alternativas que proporcionam uma largura de banda mais alargada existem actualmente milhões de módulos *X10* implementados a nível mundial, devido principalmente ao reduzido custo dos equipamentos [20].

Para a transmissão de dados é utilizada uma onda portadora à frequência de 120 kHz, que é transmitida a cada passagem pelo zero da frequência da rede, 50 kHz, como se pode ver na Figura 2.2.

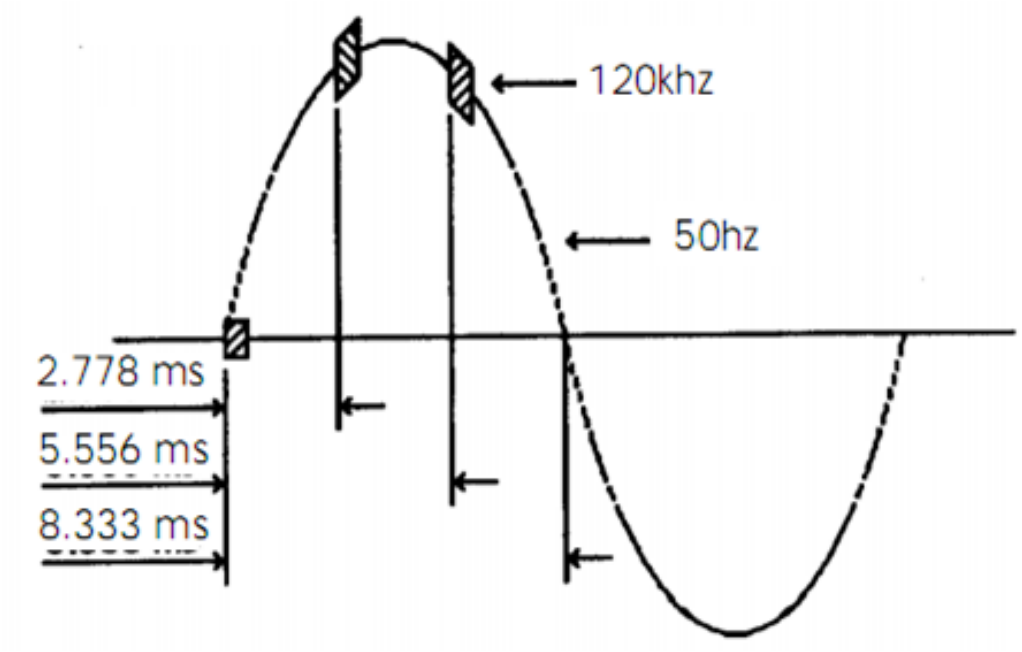

Figura 2.2: Onda portadora do protocolo X10 [21]

Uma transmissão completa de dados do módulo emissor para o módulo receptor deste protocolo, engloba 11 ciclos da rede eléctrica. Esta consiste em 2 ciclos para o *Start Code*, 4 ciclos para o endereço que contém 4 bits que identificam o edifício e mais 5 ciclos para os 4 bits que

identificam módulo e o comando. Estes comandos são, geralmente, simples como um "on" ou "off", intensidade da iluminação, temperatura, etc.

Este protocolo tem algumas limitações conhecidas, como a sua susceptibilidade à atenuação do sinal, e consequente perda de instruções, desencadeamento de acções erradas ou em tempos errados e a sua baixa velocidade e susceptibilidade a interferências de comunicações externas, principalmente devido à falta de encriptação dos dados [21].

2.3.2 CEBus

O protocolo *CEBus*, também conhecido pelo nome de *EIA-600*, foi desenvolvido pela *EIA* (*Electronic Industries Association*), por volta de 1992, com o objectivo da criação de um standard para comunicações não só sobre a rede eléctrica, mas também utilizando como meio físico o cabo coaxial, rádio frequência, infravermelhos, e fibra óptica, para automação doméstica [22].

Este protocolo é baseado no modelo de OSI (*Open Systems Interconnection*) [2] e implementa as camadas 1, 2, 3 e 7 do mesmo. O protocolo de comunicações utilizado é o peer to peer, ou seja, cada módulo pode transmitir para qualquer outro módulo pertencente à rede.

As comunicações entre módulos são efectuadas realizando conexões temporárias entre os intervenientes das mesmas, garantido a exclusividade do acesso ao meio entre estas por um período de tempo suficientemente grande que permita enviar um comando ou uma requisição. Depois de terminada a comunicação as estações voltam libertar o meio.

Para controlo dos módulos, o *CEBus* permite o controlo distribuído, permitindo a um módulo controlar qualquer outro. Este tipo de controlo possibilita um crescimento do número de nós de uma rede, sem que haja alterações na sua configuração, indo de encontro ao conceito *Plug & Play*. Outro tipo de controlo previsto por este protocolo é modo *Cluster Control*, que é baseado no controlo centralizado, ou seja um módulo pode controlar vários outros módulos, este tipo de controlo é útil quando empregado em sistemas de controlo, como por exemplo a temperatura ou luminosidade. Os dois tipos de controlo encontra-se esquematizados na figura 2.3, para o caso de um sistema trifásico.

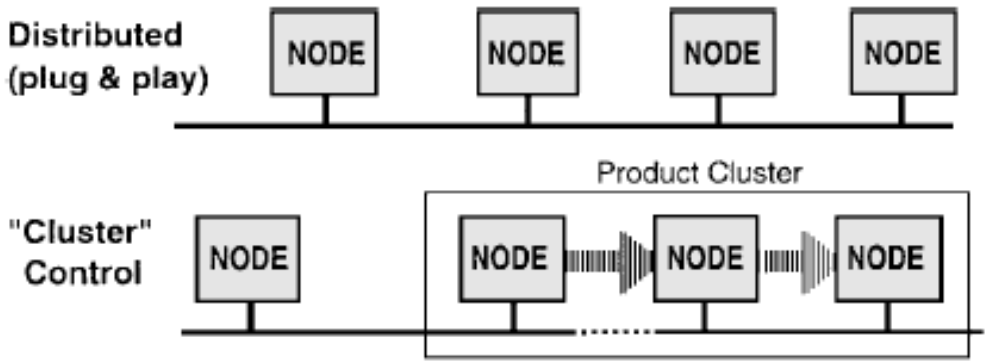

Figura 2.3: Tipos de controlo dos módulos CEBus [22]

A transmissão de dados é efectuada utilizando quatro símbolos, 1,0, EOF e EOP, que se distinguem pelo tempo duração, em que o 1 tem a duração de 100 µs e os restantes 2, 3 e 4 vezes mais, respectivamente. Para a modulação destes sinais são utilizados dois estados do meio físico: o estado Superior e o Inferior, a modulação dos sinais inicia-se sempre numa transição entre estados e o tipo sinal distingue-se pela duração de cada estado até à transição seguinte, tal como representado na Figura 2.4.

Para solucionar o problema das colisões entre mensagens, é utilizado o protocolo CSMA/CDCR (*Carrier Sense, Multiple Access/Collision Detection and Collision Resolution*).

A grande vantagem do *CEBus* pode ser vista como a simplicidade de interligação entre meios de comunicação, mas por outro lado, a taxa de transmissão de dados é reduzida e não permite a sua encriptação [22].

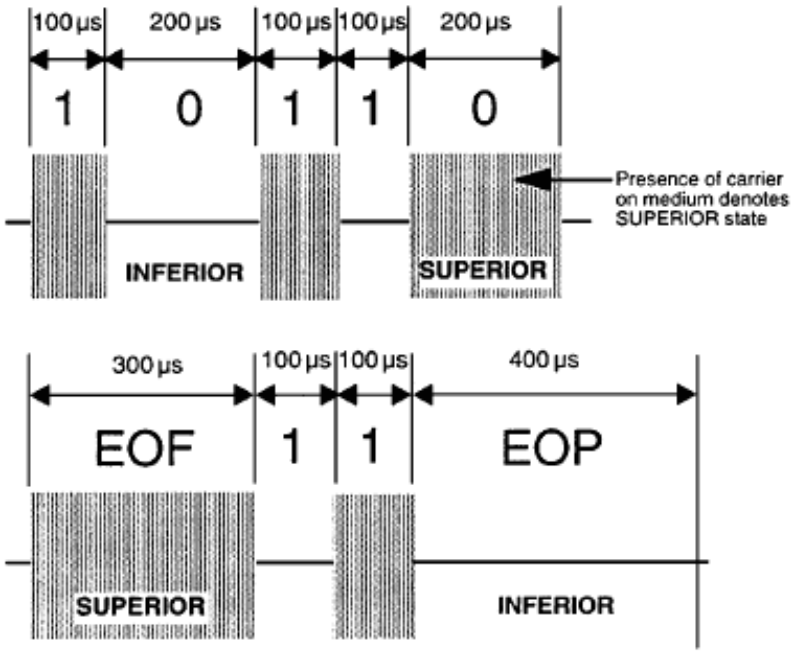

Figura 2.4: Duração dos símbolos CEBus [22]

2.3.3 Lonworks

O desenvolvimento do protocolo *Lonworks*, propriedade da *Echelon*, teve início há cerca de duas décadas e encontra-se actualmente na versão 2.0. Este protocolo permite comunicações entre vários meios, como a rede eléctrica, rádio frequência, cabo coaxial, infravermelhos e fibra óptica [23].

Este protocolo implementa todas as camadas do modelo de OSI, através da utilização de um processador denominado de *Neuron* (Figura 2.5), o que proporciona um grande leque de serviços prestados por esta tecnologia.

As mensagens são transmitidas no formato de pacotes, que por sua vez são analisados por todas as estações constituintes da rede. Caso o pacote contenha um endereço, cada uma das estações verifica se este contém informação para a sua aplicação ou se contém uma mensagem de administração da rede, tomando as medidas necessárias consoante o conteúdo do pacote.

Para eliminar ou pelo menos minimizar as colisões entre transferências é utilizado um mecanismo de acesso ao meio de transmissão denominado de *Predictive p-persistent CSMA protocol*. Este mecanismo permite obter excelentes desempenhos, mesmo em condição de sobrecarga da rede, pois ajusta dinamicamente o número de *packet time slots*, baseado na previsão do tráfego na rede. No protocolo *Lonworks* são utilizados no mínimo 16 níveis de diferentes prioridades de acesso ao meio e no máximo 1008, este valor é ajustado dinamicamente, consoante a estimativa de carga na rede.

Para o endereçamento dos pacotes podem ser usados três tipo de endereços, *Device Address*, *Group Address* e *Broadcast Address*, consoante se queira transmitir para um único módulo, para um grupo de módulos ou para todos os módulos, respectivamente.

Este protocolo prevê ainda a utilização de quatro tipos de mensagens para optimização da qualidade do serviço, a designar, *Acknowledged Messaging*, *Repeated Messaging*, *Unacknowledged Messaging* e *Authenticated Messaging* [23].

A principal desvantagem desta tecnologia é o facto de que utilizando a rede eléctrica como meio físico de comunicação, apenas podem ser atingidas taxas de transmissão até 5.4 Kbps, o que limita bastante a sua utilização.

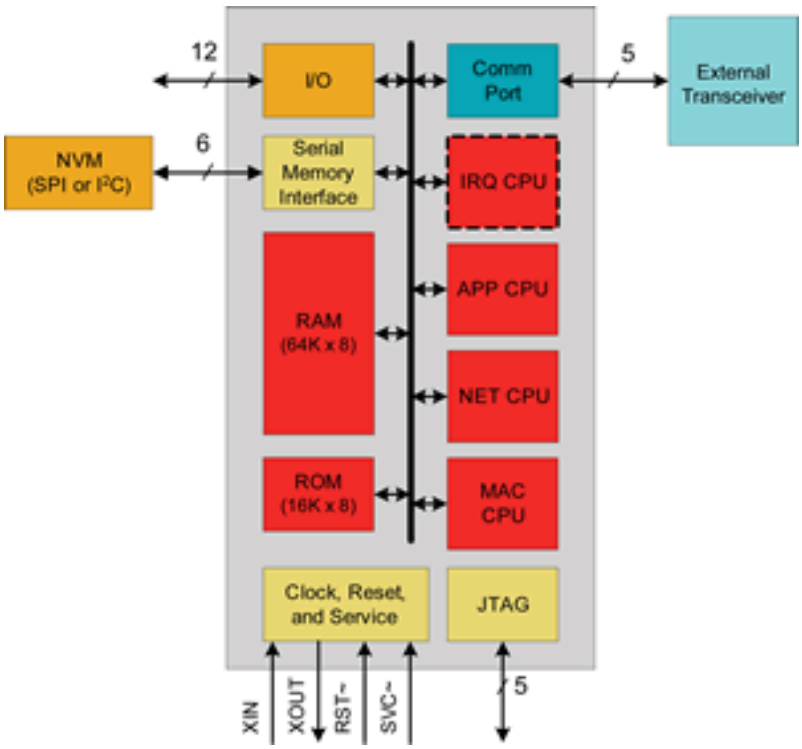

Figura 2.5: Processador Neuron [23]

2.3.4 Homeplug

O *Homeplug* foi a tecnologia escolhida para o desenvolvimento desta dissertação, e como tal vai ser alvo de um capítulo específico para descrição do seu funcionamento.

Capítulo 3

Homeplug

Este capítulo pretende descrever o funcionamento do protocolo *Homeplug*, para tal, será efectuado uma breve descrição do mesmo, seguida da descrição das camadas PHY e MAC e por fim, será explicada a construção das tramas para transmissão de mensagens. Na primeira secção será abordado o protocolo *Homeplug 1.0* e na segunda o *Homeplug AV*.

3.1 Homeplug 1.0

Homeplug é uma tecnologia criada pela aliança empresarial do mesmo nome. Esta tecnologia foca-se tanto na camada física do meio de transmissão, e respectivas técnicas de modulação dos sinais de dados sobre a rede eléctrica, como na camada de ligação de dados. É nesta última camada que são implementadas técnicas que permitem definir o tipo de controlo sobre os dados a serem transmitidos, o que condiciona directamente a velocidade e a quantidade de dados a transmitir.

O primeiro produto a ser lançado para o mercado foi o *Homeplug 1.0* [12], que permite uma velocidade de transmissão de dados de até 14 Mbit/s. Após o lançamento deste primeiro produto, e devido ao seu grande sucesso a nível mundial, surgiram mais três versões, o *Homeplug Turbo*, com taxas de transmissão máximas de 85 Mbit/s; o *Homeplug AV* [14], mais vocacionado para a transmissão de voz e vídeo, com taxas de 200 Mbit/s e o *Homeplug GreenPHY* [15]. Este último foi especificamente desenvolvido para aplicações de *SmartGrids*, e tem uma taxa de transmissão máxima de 10 Mbit/s, contudo é caracterizado pelo baixo consumo dos seus equipamentos. Actualmente encontra-se ainda em desenvolvimento o *Homeplug AV2*, que promete possibilitar a implementação de redes *Gigabit* sobre a rede eléctrica.

Apesar da existência de quatro tipos de equipamentos *Homeplug*, a sua interoperabilidade é totalmente garantida.

Para possibilitar elevadas taxas de transmissão de dados, associadas a uma boa qualidade do serviço, a tecnologia *Homeplug* recorre à implementação de técnicas avançadas de controlo de

acesso ao meio, através de protocolos CSMA (*Carrier Sense Multiple Access*) e OFDM (*Orthogonal Frequency-Division Multiplexing*) associados à organização hierárquica da camada de dados.

Este tipo de tecnologia garante ainda uma elevada segurança na transmissão de dados, possibilitando a encriptação dos dados através dos protocolos DES (*Data Encryption Standard*) e AES (*Advanced encryption Standard*).

Como a rede eléctrica não foi inicialmente pensada para a transmissão de dados, mas sim para o transporte de energia, as comunicações neste meio sofrem a influência de vários factores, tais como a interferência electromagnética dos aparelhos ligados à rede, motores, interruptores, entre outros; atenuação dos sinais transmitidos; e interferências de sinais externos, como por exemplo transmissões de rádio. Para ultrapassar estas dificuldades, o protocolo *Homeplug* utiliza uma abordagem adaptativa, com técnicas de comunicação bastante robustas, associada a técnicas avançadas de detecção e correcção de erros e pedidos automáticos de retransmissão.

Do ponto de vista do modelo de OSI, as duas camadas relevantes para a transmissão de dados através da rede eléctrica, utilizando o protocolo *Homeplug*, são a camada física e a camada de ligação de dados (Figura 3.1).

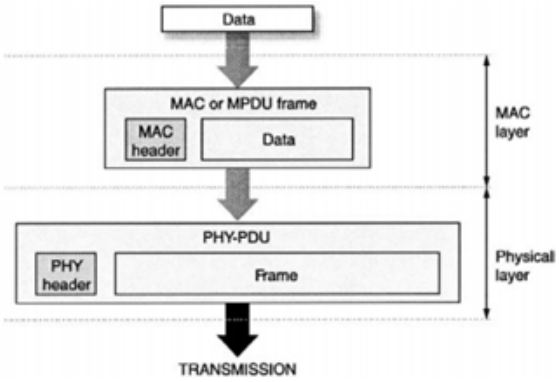

Figura 3.1: Camadas OSI utilizadas pelo Homeplug [1]

3.1.1 Camada Física

A técnica utilizada pelo *Homeplug* para modulação na camada física é a utilização de símbolos OFDM, combinados em blocos, para formarem a trama a ser transmitida. Esta é uma técnica já largamente utilizada por outros tipos de redes, como o Wi-Fi e transmissão de TV através de cabo ou ADSL (*Asymmetric Digital Subscriber Line*).

A OFDM consiste em dividir o espectro de frequências disponível em várias bandas estreitas de subportadoras e cada uma dessas subportadoras transporta parte da informação binária a ser transmitida. As respostas em frequência de cada sub-banda são ortogonais e ligeiramente em sobreposição por forma a obter uma boa eficiência espectral.

No *Homeplug 1.0*, o espectro de frequências é dividido em 84 sub-bandas com frequências compreendidas entre os 5.4 MHz e os 21 MHz, mas apenas 74 dessas sub-bandas são utilizadas, devido a restrições regulamentares, principalmente relacionadas com redes de rádio amadores.

Para eliminar a necessidade de equalização nas transmissões, cada sub-banda é composta por duas partes, sendo a primeira um *Cyclic Prefix*, que é utilizado para delimitação temporal do bloco que transporta os dados e a segunda o bloco de dados, que consiste nos símbolos OFDM com os dados a serem transmitidos. O mecanismo utilizado para a modulação dos sinais é o DQPSK (*Differential Quadrature Phase Shift Keying*), onde os dados são modulados como a diferença em fase, entre o símbolo actual e o símbolo anterior.

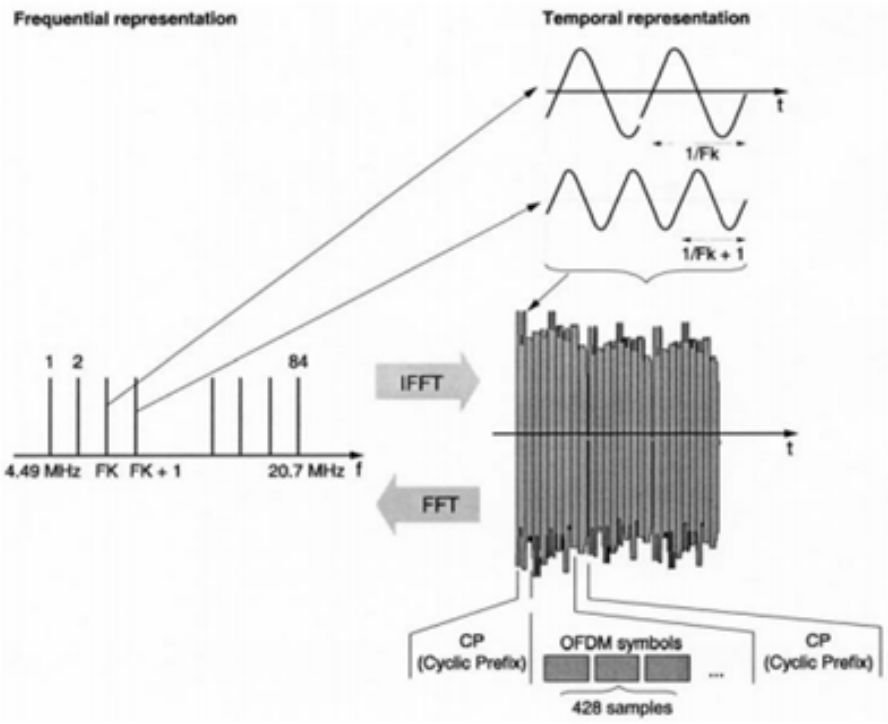

Figura 3.2: Sub-bandas portadoras [1]

Os efeitos do ruído impulsivo presente na linha, são ultrapassados recorrendo à utilização da técnica FEC (*Forward Error Correction*) baseada numa junção dos métodos de *Viterbi* e *Reed-Solomon*. Com esta técnica de correcção de erros e modulação OFDM , associadas à monitorização constante das interferências presentes em cada subportadora, permite ao *Homeplug* distribuir os sinais pelas várias subportadoras, de acordo com as interferências presentes nas mesmas, podendo mesmo ocorrer a inactividade de algumas das subportadoras (*blacklist*).

Conforme as interferências se propagam pelas diversas frequências, os sinais são modulados em várias frequências em simultâneo, aproveitando as melhores condições possíveis da ligação, garantindo assim altas taxas de transmissão, bom desempenho e fiabilidade.

Para modulação dos sinais nas subportadoras, o *Homeplug* suporta DBPSK 1/2, DQPSK 1/2 e DQPSK 3/4, em todas as subportadoras, com a excepção para comunicações *broadcast*. Nestas últimas, os sinais não podem ser alocados nas subportadoras de uma forma dinâmica. Para resolver esta situação o *Homeplug* utiliza o protocolo de modulação ROBO, que utiliza uma DBPSK com

uma forte correcção de erros e repetição de bits no tempo e em frequência, proporcionando assim uma comunicação bastante fiável e eficaz.

3.1.2 Camada de ligação de dados

É nesta camada que são implementadas a técnicas de encapsulamento dos dados e de controlo de acesso ao meio (MAC), por esta razão, esta camada é também apelidada de *MAC Protocol Data Unit*.

Nesta camada também se efectua a interligação entre a camada física e as camadas superiores de transmissão de dados.

O MAC do *Homeplug 1.0* foi criado de forma a ser completamente compatível com o formato utilizado pelo IEEE 802.3, o que permite, de uma forma facilitada a interligação com as redes *Ethernet* já existentes. Os blocos *Ethernet* provenientes de redes superiores passam por processos de fragmentação e reassemblagem sequenciais, aquando da transmissão e recepção de dados.

Para controlo de acesso ao meio, o *Homeplug* utiliza uma variante do protocolo CSMA/CA [2]. No protocolo original, cada nó deve ser capaz de analisar o meio e verificar se este se encontra ocupado. Caso o meio se encontre ocupado a transmissão não se inicia e o nó fica a aguardar até que o meio esteja livre para transmissão. O nó só transmite assim que detecta que o meio se encontra livre para transmissão, durante um determinado tempo de contenção fixo (DIFS), acrescido de um tempo aleatório (*BackOff*), como apresentado na Figura 3.3.

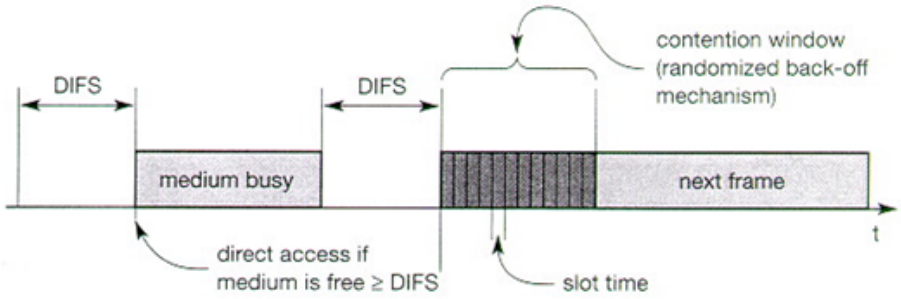

Figura 3.3: Protocolo CSMA/CA [1]

A versão utilizada no *Homeplug* acrescenta ao protocolo original, a utilização de um mecanismo de resolução de prioridades, um algoritmo de *backoff* e um valor que indica o número de vezes que uma estação não conseguiu transmitir, em comparação com estações com a mesma prioridade. Este valor é designado de DC (*Deferral Counter*) e é incrementado sempre que uma estação não consegue transmitir, o que permite utilizar o protocolo já descrito em conjunto com este indicador, como se mostra na Figura 3.4.

O mecanismo de resolução de prioridades do *Homeplug* prevê ainda a utilização de até quatro níveis de prioridades diferentes (Tabela 3.1), que são transmitidos em dois *slots* de resolução de prioridades (PSR0 e PSR1), estes *slots* são utilizados para determinar qual a mensagem com maior prioridade. Após determinado qual o nível de maior prioridade das mensagens a ser transmitidas,

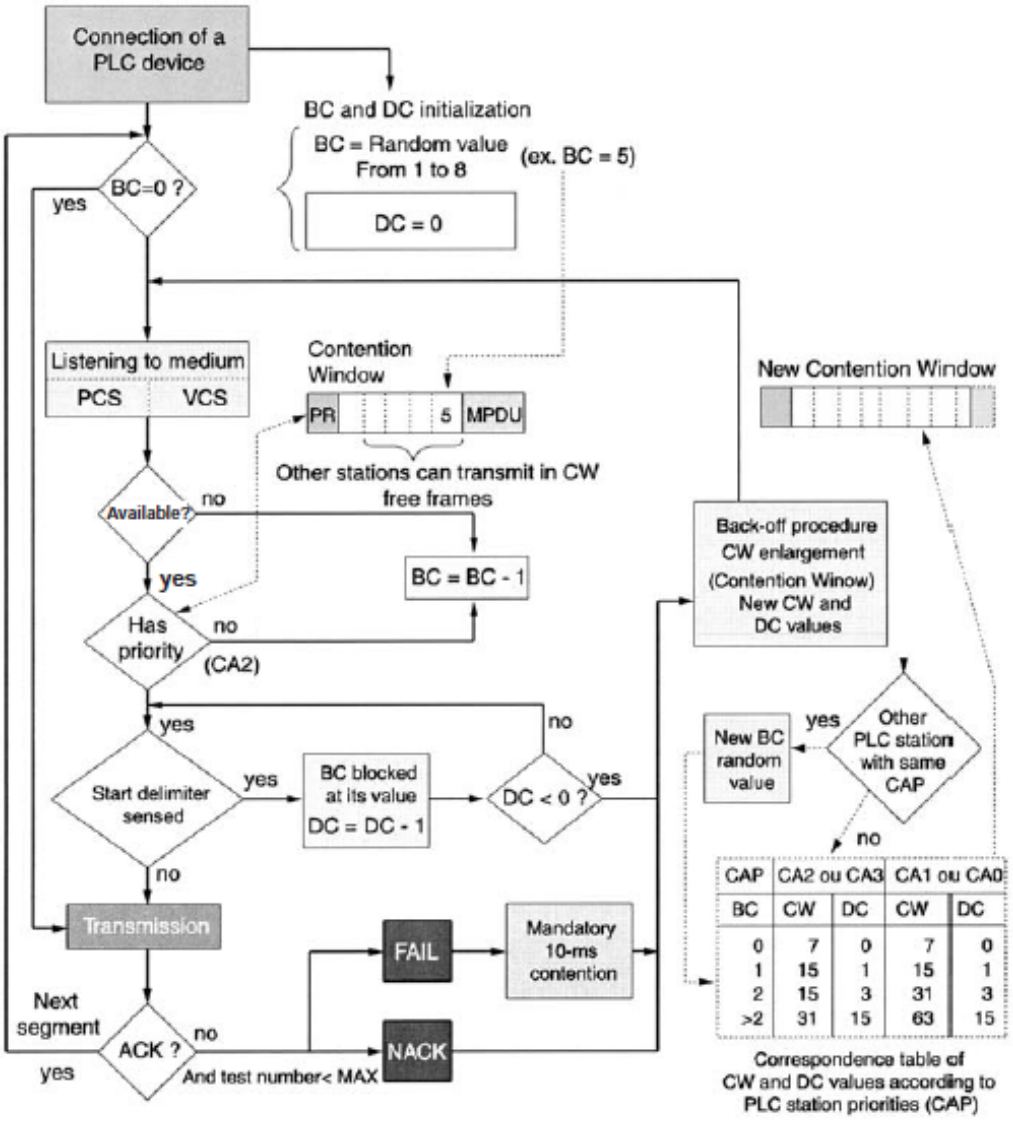

Figura 3.4: Protocolo CSMA/CA no Homeplug 1.0 [1]

apenas estas entram no período de contenção, ficando as restantes a aguardar por uma nova transmissão. Por exemplo, quando existem os quatro níveis de prioridades numa rede a tentar transmitir ao mesmo tempo, Os nós com prioridade 3 e 2 transmitem um sinal de resolução de prioridades no *slot* PSR0. Por sua vez, os nós com prioridades 1 e 0 detectam este sinal, o que provoca o abandono da tentativa de transmissão. Seguidamente o nó com prioridade 3 transmite um sinal em PSR1, que será detectado pelo nó com prioridade 2, provocando a desistência deste último. Posto isto, apenas o nó com prioridade 3 entra no período de contenção.

Esta técnica de resolução de prioridades permite assim melhorar largamente a qualidade do serviço, diminuindo o tempo de espera de transmissão de mensagens com elevada prioridade. O método de resolução de prioridades é efectuado sempre que uma nova mensagem é transmitida,

como se pode ver na Figura 3.5.

Tabela 3.1: Níveis de prioridade do *Homeplug* [12]

Prioridade	VLAN tag	Tipo de Aplicação
3	7.6	Voz – menos de 10 ms de atraso e jitter
2	4.5	Vídeo ou Audio – menos de 100 ms de atraso
1	0.3	Transferências em massa ou tráfego secundário
0	1.2	Tráfego menos prioritário

Para além de eliminar a ocorrência de colisões, o mecanismo de sensorização do meio utilizado no *Homeplug* permite ainda uma melhoria na sincronização entre os diferentes nós da rede. Este mecanismo pode ser divido em duas partes, o PCS (*Physical Carrier Sense*) e a outra VCS (*Virtual Carrier Sense*). A primeira está implementada na camada física e indica quando um segmento de preâmbulo é detectado. A segunda é implementada na camada MAC e é actualizada pela informação contida nos delimitadores de cada trama.

Como acréscimo aos mecanismos já descritos, o *Homeplug* permite ainda a integração de prioridades com camadas de rede superiores, através da utilização de *tags* VLAN (*Virtual Local Area Network*).

Figura 3.5: Resolução de prioridades [12]

3.1.3 Formato das Tramas

A tecnologia *Homeplug* utiliza dois tipos básicos de tramas. A trama longa (Figura 3.6), que é constituída por um limitador SOF (*Start of Frame*), pelos dados e por um limitador de EOF (*End of Frame*), e a trama curta (Figura 3.7), que é constituída por um limitador de resposta *Response Delimiter*. Esta última é utilizada no processo de paragem e espera para pedidos automáticos de repetição ARQ (*Automatic Repeat Request*), o que permite a retransmissão de pacotes corrompidos.

Todos os delimitadores utilizados nas tramas têm a mesma estrutura e são constituídos por um campo de *Preamble*, que contém um sinal utilizado para sinalizar o início de um delimitador, e um campo de *Frame Control*, que, além dos dados apresentados na Tabela 3.2, contém informação que permite a sincronização entre módulos, reduzindo assim o número de colisões entre mensagens.

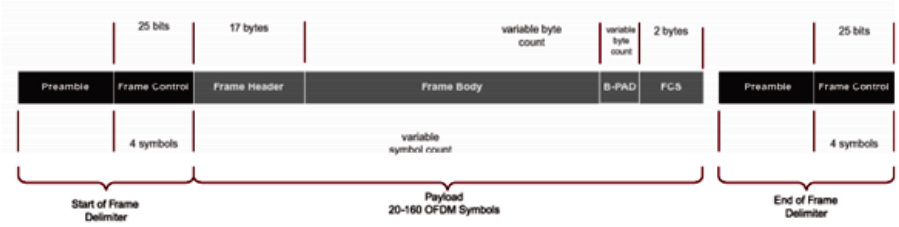

Figura 3.6: Trama Longa [12]

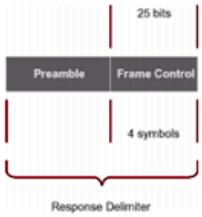

Figura 3.7: Trama curta [12]

Tabela 3.2: Campos do Frame Control

Tipo de Delimitador	Campos	Significado
Start of Frame (SOF)	Type	Indica se espera, ou não, por resposta, consoante se pretenda uma trama curta depois da trama longa
	Contention Control	Quando activo, previne todos os nós com prioridade igual ou inferior à actual de acederem ao meio, contudo, se existir uma mensagem com prioridade superior a transmissão actual pode ser interrompida
	Frame Length	Comprimento dos dados em múltiplos de símbolos OFDM
	Tone Map Index	Índice para a informação de adaptação de canal, armazenada no receptor
End of Frame (EOF)	Type	Indica se é esperada ou não a resposta
	Contention Control	O mesmo que o do SOF, esta redundância permite melhorar a sincronização
	Channel Access Priority (CAP)	Indica a prioridade da mensagem actual
Response (Resp)	Type	Contém a informação de ACK, confirmação positiva, NACK, confirmação negativa devido a falha na recepção ou FAIL, confirmação negativa devido a falta de recursos
	Channel Access Priority (CAP)	Indica a prioridade da mensagem anterior

A trama longa, para além dos delimitadores é constituída por:

- *Frame Header* (Figura 3.8), que contém a informação de segmentação (Tabela 3.3), endereço de destino e endereço de origem;
- *Frame data body* (Figura 3.9), que contém os dados a serem transmitidos;
- *Possíveis bits* de preenchimento;
- *Frame check sequence*, que permite a detecção de erros não corrigidos.

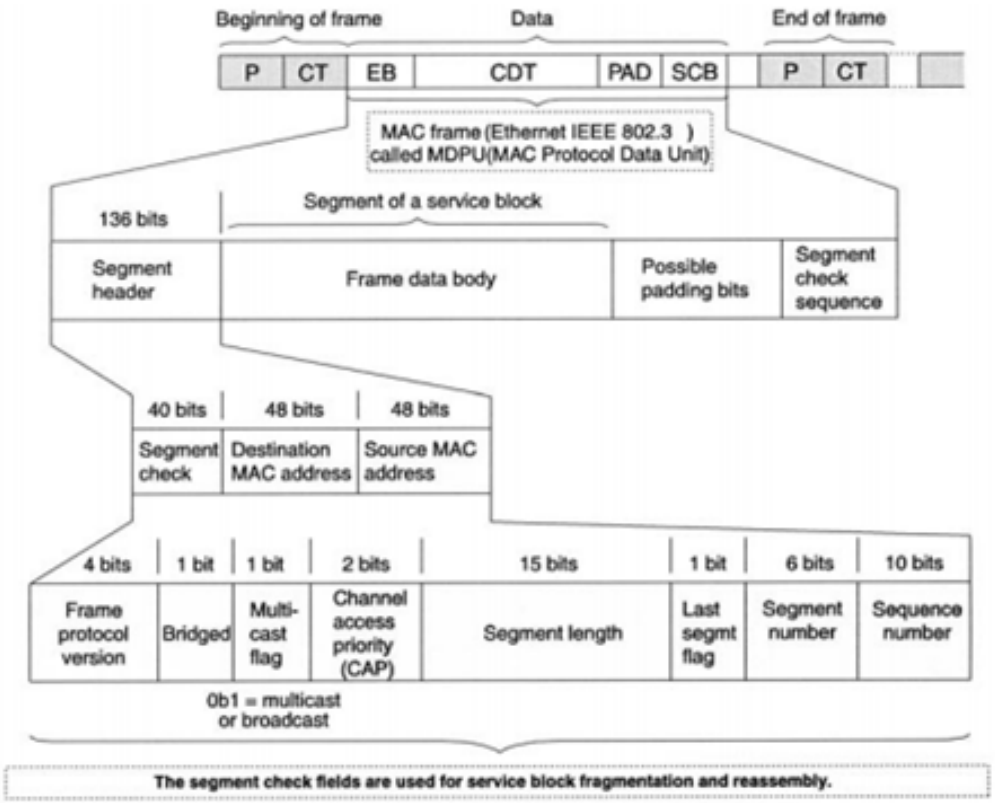

Figura 3.8: Header da trama longa [1]

Os dados a serem transmitidos estão limitados a um máximo de 160 símbolos OFDM, o que corresponde no máximo a 1600 bits, dependendo do tipo de modulação utilizada. De modo a garantir a qualidade de serviço, quando a mensagem ultrapassa este limite são utilizadas técnicas de segmentação e remontagem e os dados são transmitidos em várias tramas. Estas tramas podem ser transmitidas de forma sequencial, mas passam igualmente pelo processo de avaliação de prioridades de transferência, o que permite que esta sequência seja interrompida por mensagens de alta prioridade, diminuindo assim o tempo de latência de mensagens prioritárias.

Este conjunto de técnicas permite ao sistema adaptar-se facilmente às mudanças das condições de transmissão da rede eléctrica, garantindo permanentemente uma boa qualidade de serviço.

Tabela 3.3: Campos do Header

Campo	Função
Protocol Version	Define o valor do protocolo utilizado. Este valor apenas é usado quando há upgrade do standard
Bridged	Indica se a estação transmissora se encontra no modo bridge, ou seja com capacidade de repetir as mensagens recebidas
MCF (multicast flag)	Indica se a transmissão é efectuada em multicast ou broadcast
CAP (channel access priority)	Indica o nível de prioridade da estação de origem, em comparação com outras estações
Segment length	Comprimento do segmento transmitido
LSF (last flag segment)	Colocada a 1, caso este seja o último segmento da transmissão
Segment number	Indica a ordem de fragmentação e remontagem de mensagens
Segment sequence number	Este número é único para cada mensagem, e incrementado a cada nova mensagem, mesmo que uma mensagem seja segmentada, os seus segmentos terão todos o mesmo número.

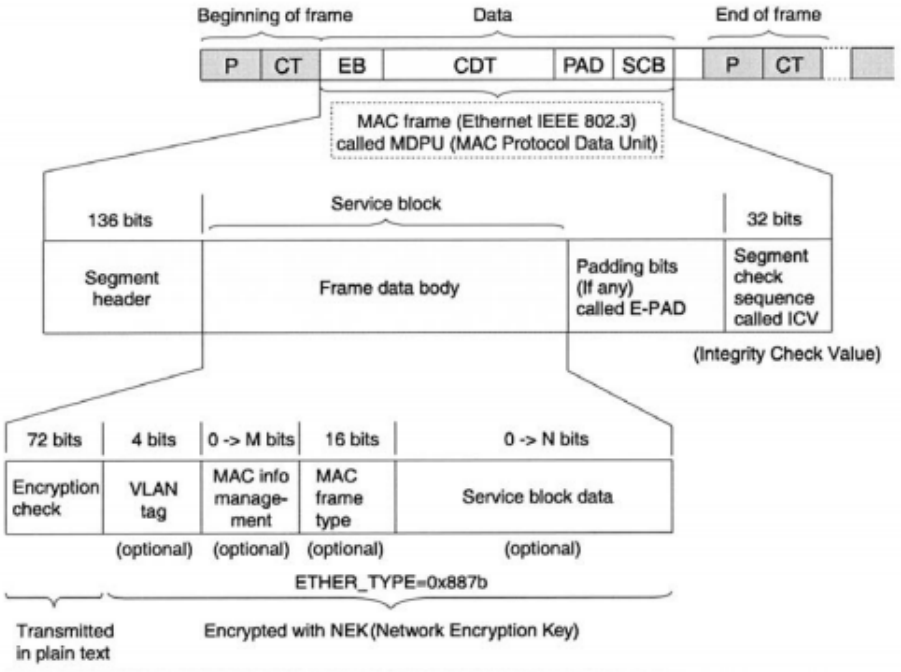

Figura 3.9: Frame data body [1]

3.2 Homeplug AV

O protocolo *Homeplug AV* foi desenvolvido com intuito de fornecer uma conexão de alta qualidade, mantendo a interoperabilidade com o *Homeplug 1.0*. Este utiliza técnicas avançadas de implementação da camada PHY e MAC, proporcionado uma ligação de 200 Mbps ao nível da cama PHY, o que se traduz numa capacidade de transmissão de informação máxima de 150 Mbps [14].

A camada MAC do *Homeplug AV* suporta tanto o acesso ao meio através de mecanismos CSMA como TDMA, baseados em sincronização com o ciclo AC da linha. O mecanismo TDMA permite assim garantir os parâmetros QoS (*Quality of Service*), como a largura de banda garantida, baixa perda de dados e um apertado controlo da latência e do *jitter*. Por outro lado, o mecanismo CSMA proporciona quatro níveis de prioridades para a transmissão de pacotes.

Todas as actividades na rede e mais concretamente a alocação do tempo para os mecanismos TDMA e CSMA são controladas por um dos módulos HPAV (*Homeplug AV*) que assume o papel de *Central Coordinator* (CCo) [14].

3.2.1 Arquitectura do sistema

A arquitectura do sistema HPAV encontra-se representada na Figura 3.10. Esta arquitectura pode ser dividida em 3 grandes planos, nomeadamente:

- As *High Layer Entities* (HLE) podem ser aplicações, *bridges* ou servidores que fornecem serviços externos ao módulo HPAV. Estas, em conjunto com o *Data Service Access Point* (SAP), que está desenhado para receber pacotes no formato *Ethernet*, permitem que todos os protocolos baseado na tecnologia IP (*Internet Protocol*) possam ser facilmente tratados;

- O plano de controlo, que possui uma camada MAC única, designada de CM (*Connection Manager*), o que permite uma maior eficiência no tratamento dos pedidos, em conjunto com uma maior flexibilidade no desenvolvimento desta tecnologia. Em conjunto com a CM, está também prevista a existência de mais uma camada paralela, o CCo, que apenas está activo numa das estações da rede HPAV.

- O plano de dados, que proporciona o tradicional modelo em camadas, com interface M1 entre a camada CL (*Convergence Layer*) e a camada MAC, e a PHY interface entre as camadas MAC e PHY;

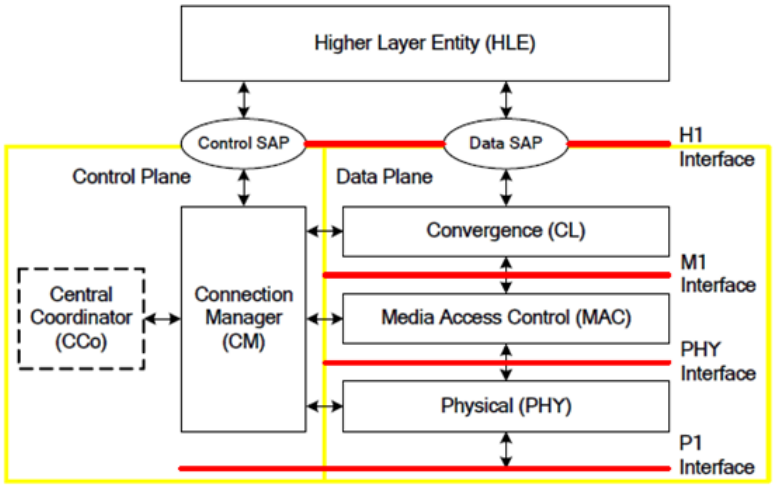

Figura 3.10: Arquitectura HPAV [14]

3.2.2 Camada física PHY

A camada física do HPAV opera na gama de frequências entre os 2 e 28 MHz, mas ao contrário do protocolo *Homeplug 1.0*, no HPAV este espectro de frequências está dividido em 917 sub-bandas. A modulação pode variar desde BPSK (*Binary Phase Shift Keying*), que transporta 1 bit de informação por portadora por símbolo, até 1024 QAM (*Quadrature Amplitude Modulation*), que transporta 10 bits de informação por portadora, por símbolo. Estas modulações podem ser aplicadas independentemente a cada uma das portadoras, dependendo das características do canal de transmissão.

Do lado do transmissor, a camada PHY recebe os dados vindos da camada MAC , que podem ser do tipo *Homeplug 1.0*, *Homeplug AV* ou informação de controlo *Homeplug AV* (Figura 3.11). A saída destas três *streams* de dados é posteriormente alvo de uma modulação OFDM comum, sendo esta última acoplada à rede eléctrica através de um módulo AFE (*Analog Front End*).

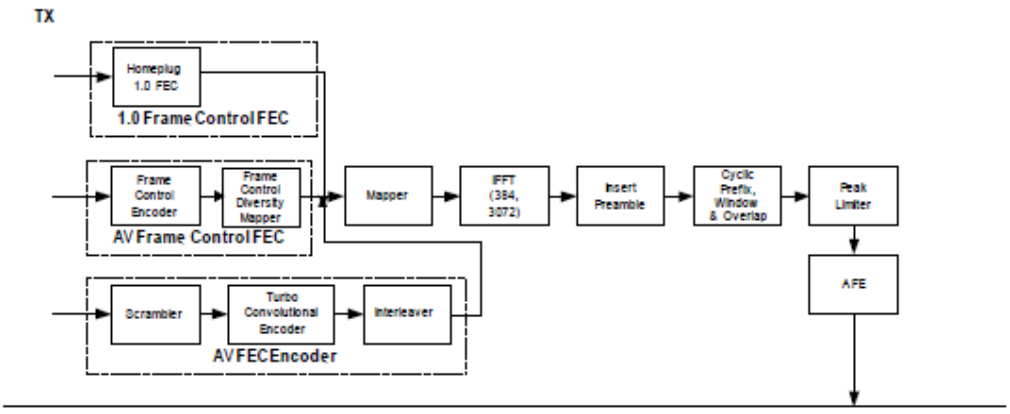

Figura 3.11: HPAV OFDM Transciever - Emissor [14]

Do lado do receptor o módulo AFE funciona em conjunto com um módulo de AGC (*Automatic Gain Controller*) e com um módulo de sincronização temporal, para alimentar dois circuitos separados de recuperação de informação, consoante o protocolo utilizado (Figura 3.12).
Na camada PHY do HPAV está ainda prevista a alteração, através de *software*, das sub-bandas de frequência a utilizar, permitindo assim uma adaptação às regulações regionais das frequências a utilizar.

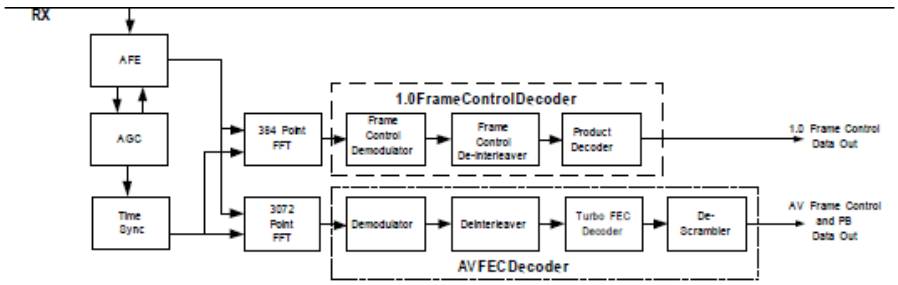

Figura 3.12: HPAV OFDM Transciever - Receptor [14]

3.2.3 Camada MAC – Serviços

O protocolo HPAV fornece serviços orientados à conexão e livres de contenção, permitindo assim garantir os parâmetros QoS definidos pelas aplicações, bem como serviços sem conexão baseados na contenção priorizada, de modo a suportar aplicações baseadas na priorização dos parâmetros QoS.

Estes dois tipos de serviços possibilitam a existência de dois períodos de transmissão. O primeiro período é designado de CB (*Contention Based*) e é implementado através da tecnologia CSMA/CA. Este é partilhado por todas as estações, existindo concorrência pelo meio. É também nesta fase que decorre o período de *Priority Resolution*, onde as estações com tráfego com prioridade inferior entram nos períodos de contenção, libertando assim o meio para as estações com tráfego de prioridade superior poderem transmitir. O segundo período de transmissão designa-se de CF (*Contention Free*) e é implementado recorrendo a alocações TDMA persistentes, de duração adequada, consoante os parâmetros QoS. Esta técnica de alocação do tempo de transmissão garante que não exista concorrência pelo meio entre estações e que cada uma transmite no período para si alocado.

A implementação destas duas tecnologias é efectuada pelo CCo, aquando da definição do *Beacon Period* (Figura 3.13). Este período está dividido em 3 regiões, a região do *Beacon*, a região CSMA e a região CF. O CCo transmite um *beacon* para todas as estações no início de cada *Beacon Period*, que contém o agendamento de cada uma das regiões dentro do período total de transmissão. Os *beacons* são sinais extremamente robustos, e a alocação do tempo para transmissão de cada uma das estações é persistente, ou seja uma estação pode transmitir no tempo alocado para si, mesmo que não tenha recebido um sinal de *beacon*, pois o CCo garante que não existe alteração dos agendamentos para cada uma das estações, durante um número de *beacons* conhecido.

Para especificação dos parâmetros QoS, as HLE (*High Layer Entities*) utilizam o CSPEC (*Connection Specification*), que por sua vez é avaliado por cada um dos CM, que quando apropriado transmitem ao CCo os requisitos necessários e solicitam a alocação de uma região CF de modo a garantir estes requisitos.

Caso o CCo consiga acomodar o pedido de conexão, é solicitado às estações que analisem o meio e efectuem uma estimação inicial do canal, ou seja, criem um *Tone Map* que especifique as melhores condições para a modulação dos sinais OFDM. Este *Tone Map* é depois transmitido do receptor para o emissor e também ao CCo, o que permite optimizar o processo de cálculo do tempo a alocar a cada conexão.

Para além das alocações persistentes durante o *Beacon Period*, existem ainda regiões não persistentes, que podem ser utilizadas para proporcionar largura de banda adicional, apenas durante o *Beacon Period* actual, de forma a garantir os QoS em situações de ocorrência de erros ou alterações do canal de transmissão.

Caso estes períodos não persistentes não sejam utilizados para alocações CF, são utilizados pelas estações para transmissão de tráfego CSMA/CA.

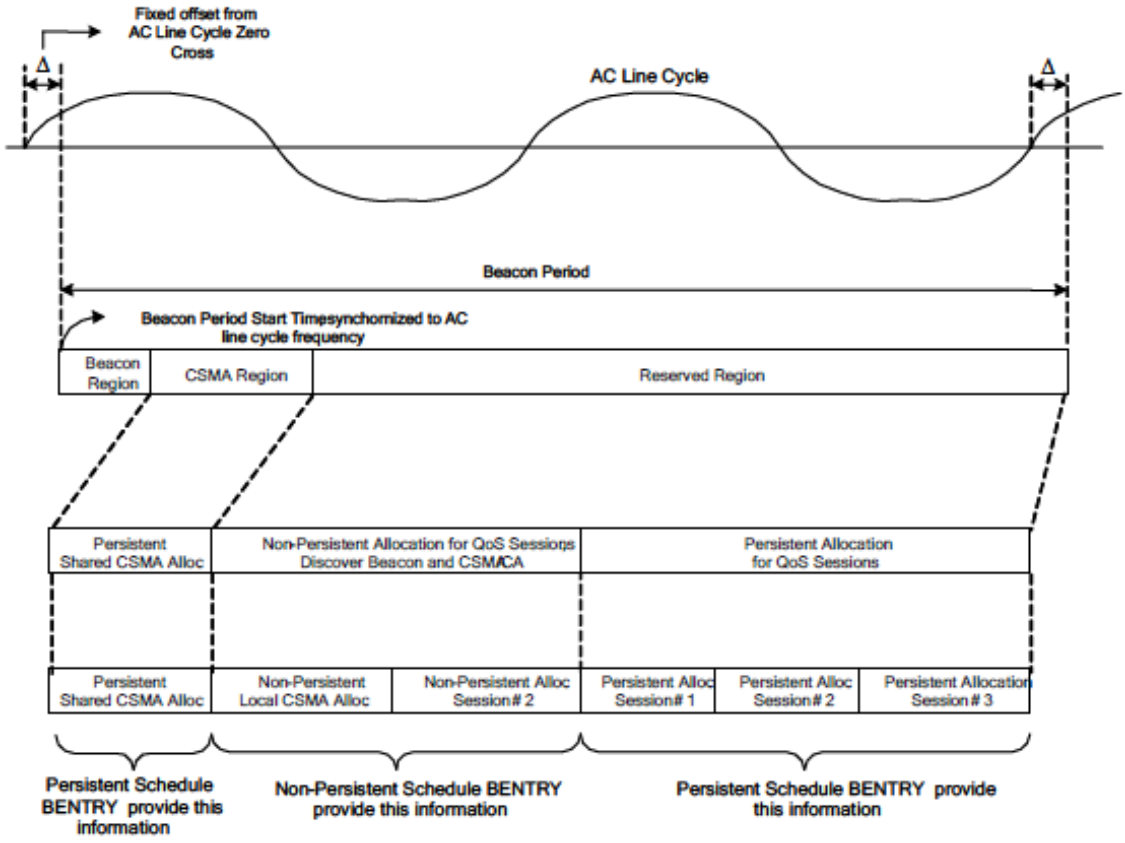

Figura 3.13: Estrutura do Beacon Period [14]

3.2.4 Camada MAC – Plano de controlo

A camada CM (*Connection Manager*) é a responsável por avaliar os parâmetros CSPEC e, em conjunto com o CM da estação para a qual se pretende transmitir e com o CCo, proporcionar a uma conexão que satisfaça estes mesmos requisitos. É a camada CM que garante a largura de banda necessária para satisfazer determinados requisitos QoS, e em caso de falha, é da responsabilidade desta tomar medidas de correcção para que os parâmetros QoS sejam garantidos.

3.2.5 Camada MAC – Plano de dados

No plano de dados da camada MAC são recebidos pacotes MSDU's (*MAC Service Data Unit*), normalmente pacotes *Ethernet*, para posteriormente serem encapsulados. Aquando do encapsulamento é lhes adicionando um *header*, um *Check Sum* e opcionalmente um *Time Stamp*. Este encapsulamento forma os *MAC Frames*, que são posteriormente encaminhados para a respectiva *stream* de dados. Como demonstrado na Figura 3.14, estas *MAC streams* são de seguida divididas em 512 octetos, sendo encriptadas e encapsuladas em *PHY Block's* (PB). Por último, os PB são empacotados em MPDU's (*MAC Protocol Data Unit*) que são passados para a camada física e transmitidos como descrito na subsecção 3.2.2.

Do lado do receptor, à medida que são reconstruídos os MSDU's, é efectuado o SACK (*Selective Acknowledge*) dos PB, os que não forem positivamente recepcionados são retransmitidos na TXOP (*Transmit Opportunity*) seguinte.

Uma vez que as tecnologias FEC (*Forward Error Correction*) e SACK são aplicadas a pacotes relativamente pequenos, o FEC é mais robusto, reduzindo o número de retransmissões, o que permite ao HPAV funcionar quase à capacidade máxima do canal.

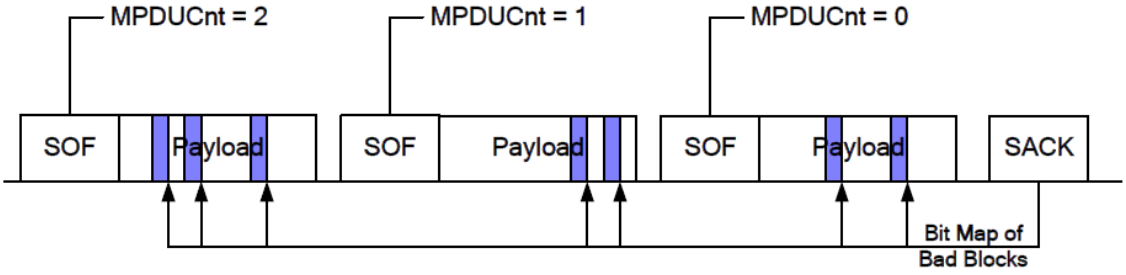

Figura 3.14: Segmentação MAC e geração de MPDU [14]

3.2.6 Central Coordinator

Em cada rede AVLN (*Homeplug AV Logical Network*) existe apenas um CCo, esta rede é constituída por várias estações que partilham a mesma NMK (*Network Membership Key*) , e que são comandadas por um único CCo. Quando um novo módulo é conectado à rede eléctrica, este

escuta o meio para verificar a existência de alguma AVLN a que ele se possa tentar conectar, caso nenhuma AVLN seja detectada, este novo módulo passa a desempenhar o papel de CCo e inicia a transmissão do *beacon* a cada passagem pelo zero da rede, criando deste modo uma nova AVLN. Aquando da eventual conexão de um outro módulo, este detectará as AVLN's existentes e conecta-se a uma delas, ou seja, no caso anterior passa a existir uma nova rede, constituída por duas estações.

Para uma monitorização contínua, quer da sua rede, quer de redes vizinhas, o CCo envia periodicamente um *Discover Beacon*, e cada estação que receba este *Discover Beacon* adiciona a informação contida neste à sua DSL (*Discovered Station List*), caso a estação receba um *Discover Beacon* de outra AVLN, adiciona também a informação contida neste, à sua DNL (*Discovered Networks List*). Estas listas são posteriormente enviadas ao CCo, permitindo-lhe criar um mapa actualizado de toda a rede.

Este mapa da rede criado pelo CCo, é posteriormente utilizado para analisar a existência de um possível CCo melhor que o actual. Esta escolha é efectuada segundo os seguintes critérios, por esta ordem de prioridade:

1. Selecção do utilizador;
2. Capacidade do CCo;
3. Número de estações na *Discovered Station List*;
4. Número de AVLN's na *Discovered Network List*;

Caso seja detectado um CCo melhor, ambas as estações negoceiam essa tarefa e são transferidas as funções. Pode ainda ser seleccionada uma estação para o CCo de *backup*, que apenas monitoriza a rede, não tomando qualquer tipo de acção de controlo, caso esta estação deixe de receber o sinal de *Beacon* por um número de períodos especificado, inicia automaticamente as funções de CCo.

3.2.7 Segurança dos dados

A segurança e confidencialidade dos dados transmitidos numa rede HPAV é assegurada através da encriptação de dados segundo o mecanismo 128-bit AES. Esta encriptação utiliza a NEK e é efectuada em segmentos individuais aquando da formação das MPDU's. Esta chave pode ser alterada de uma forma automática e dinâmica, e cada uma das estações pode conter mais que uma chave, permitindo-lhe assim participar activamente em múltiplas AVLN's.

Quando uma estação é conectada à rede, esta tem obrigatoriamente de receber a NMK da respectiva rede, caso contrário não poderá transmitir nessa AVLN. A nova estação pode obter esta NMK das seguintes formas:

- Utilizando a NMK que vem pré programada em todos os equipamentos HPAV, o que proporciona uma solução *plug and play*, mas não fornece qualquer tipo de segurança na transmissão de dados;

- O utilizador pode definir e introduzir uma NPW (*Network Password*) directamente numa nova estação da rede. Esta NPW é utilizada para criar a NMK, através de uma encriptação 128-bit AES;
- Utilizando o pré programado DAK (*Device Access Key*), este é um valor único a cada módulo HPAV, que pode ser introduzido num outro módulo já pertencente à rede. Este, por sua vez utiliza este DAK para encriptar a NMK e transmite-a em *broadcast*. Como apenas a nova estação possui o valor do DAK, apenas esta consegue desencriptar a NMK, ligando-se assim à AVLN;
- A estação pode ser introduzida na rede, directamente pelo utilizador através do simples pressionar de um botão, quer no novo módulo, quer num dos já pertencentes à rede.

Assim que uma estação possua a NMK de uma rede e se junte a esta, é-lhe fornecida a NEK a ser usada para encriptar os dados a serem transferidos.

3.2.8 Coexistência e redes múltiplas

O protocolo HPAV, incorpora mecanismos que permitem a existência de várias AVLN, sem existirem interferências entre elas, nestes casos os CCo's negoceiam entre si o período para transmissão do seu *Beacon* e o período para transmissão na região PCF (*Persistent Contention Free*). Aquando desta negociação, cada uma das redes transmite o seu *beacon* e o tráfego persistente nos períodos previamente definidos, sendo o período para tráfego CSMA partilhado entre as várias redes, como se verifica na Figura 3.15.

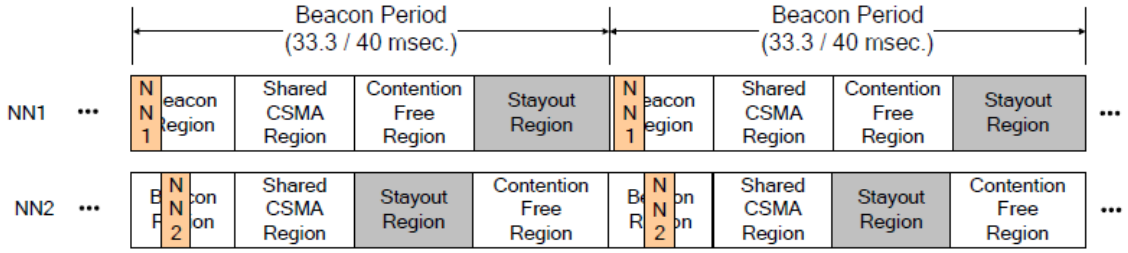

Figura 3.15: Coordenação entre redes AVLN [14]

Para além da existência de várias AVLN, é também possível a coexistência de redes HPAV e *Homeplug 1.0* no mesmo meio existindo apenas uma troca mínima de informações de controlo entre as duas redes. Opcionalmente, e caso o utilizador assim o pretenda, podem ser implementados dispositivos capazes de comunicar e operar entre os dois protocolos, permitindo assim a troca de dados entre redes.

Capítulo 4

Metodologia

Por forma a quantificar os principais parâmetros, fundamentais ao correcto funcionamento de uma rede de dados, foram realizadas várias experiências em diferentes cenários, com o objecto de avaliar o desempenho de uma rede *Homeplug* para suporte de aplicações industriais.

Ao longo deste capítulo serão apresentados os parâmetros a serem avaliados, as metodologias, as ferramentas adoptadas para as medições e os diferentes cenários de análise.

Este conjunto de experiências foi dividido em duas grandes etapas, consistindo a primeira numa análise baseada numa rede com dois computadores comunicando entre si, onde um deles desempenha o papel de cliente e outro o papel de servidor e a segunda etapa baseada na transferência de tráfego periódico entre um cliente e um servidor, mas com outro interveniente na rede que gerará tráfego adicional ao periódico a ser medido.

O primeiro grupo de testes e experiências teve como objectivo a medição da largura de banda, a perda de pacotes, a latência e o jitter de tráfego TCP e UDP, com diferentes características. O segundo grupo de testes tem como principal objectivo a avaliação do desempenho da rede Homeplug quando sujeita a tráfego UDP periódico, tráfego este representativo do tráfego industrial.

4.1 Principais medidas a serem efectuadas

A importância e o significado dos diferentes parâmetros a serem medidos numa rede de dados, varia consoante o tipo destas e das aplicações a utilizarem a mesma. Por exemplo, numa rede de distribuição de conteúdos do tipo cliente - servidor uma das medidas mais importantes a ter em conta é a latência entre a aplicação servidor e a aplicação cliente. Por outro lado, numa rede com múltiplos servidores, a largura de banda disponível pode ser dos critérios mais importantes para gerir a carga em cada um dos servidores.

Tendo em conta o principal objectivo deste trabalho, foram escolhidos quatro parâmetros essenciais para caracterizar a rede, sendo estes a latência, a largura de banda, o jitter e o número de pacotes perdidos.

4.1.1 Largura de banda

A largura de banda está definida como sendo a medida da capacidade de um meio transmitir dados ao longo do tempo, esta deve ser medida em bits por segundo (bps). Aplicações de multimédia ou transferência elevada de dados precisam geralmente de uma grande largura de banda, ao contrário da maioria de aplicações de controlo que estão mais dependentes de características temporais [24].

4.1.2 Pacotes perdidos

Sempre que o número de pacotes recebidos é inferior ao número de pacotes enviados, existe perda de pacotes ao longo do meio de transmissão. A taxa de pacotes perdidos ao longo da transmissão é normalmente apresentada em percentagem. A perda de pacotes afecta o desempenho da aplicação porque os pacotes perdidos têm de ser retransmitidos ou no caso de não existir retransmissão podem provocar o funcionamento incorrecto das aplicações. Esta medida será apenas analisada para tráfego de pacotes UDP, pois no tráfego TCP existem mecanismos de retransmissão, de modo a tentar eliminar as perda de pacotes [24].

4.1.3 Latência

A latência é definida como sendo o tempo que decorre desde o momento da criação de um pacote, até à sua recepção, por parte da aplicação de destino. Geralmente a latência é medida em milisegundos (ms). Esta é um dos factores mais importantes, geralmente para aplicações em tempo real, pois um elevado atraso na recepção das mensagens pode provocar um mau funcionamento da aplicação. Este tempo, também denominado de *end-to-end delay*, engloba os tempos de processamento, transmissão e propagação na rede [24].

Durante o estudo realizado foram ignorados os tempos de propagação do sinal, pois são bastante reduzidos e só dependem da velocidade de propagação dos sinais nos cabos físicos e da sua distância, sendo a velocidade de propagação num cabo de pares cruzados de aproximadamente:

$$Velocidade: \quad v = 0.59 \times c = 0.59 \times 299792458 = 176877550(m/s) \tag{4.1}$$

Tendo sido utilizados durante as experiências, cabos com um comprimento de aproximadamente 10 metros, obtém-se então um tempo de propagação de aproximadamente 50 nano segundos, que, devido ao seu reduzido valor, pode ser desprezado.

O tempo de processamento dos dados está directamente relacionado com o tempo que os equipamentos de uma rede demoram a processar os cabeçalhos dos pacotes para depois os encaminharem, como nos testes os únicos equipamentos constituintes da rede de dados foram as cartas de rede e os módulos HPAV, este tempo foi também ignorado [25].

O tempo de transmissão pode ser definido como o tempo necessário para colocar todos os bits de um segmento de dados, na camada física da rede, este é o tempo que se pretende analisar, pois engloba tanto os tempos das cartas de rede como o tempo de modulação dos módulos *Homeplug*.

Podemos então esquematizar os principais tempos a serem medidos como se apresenta na Figura 4.1.

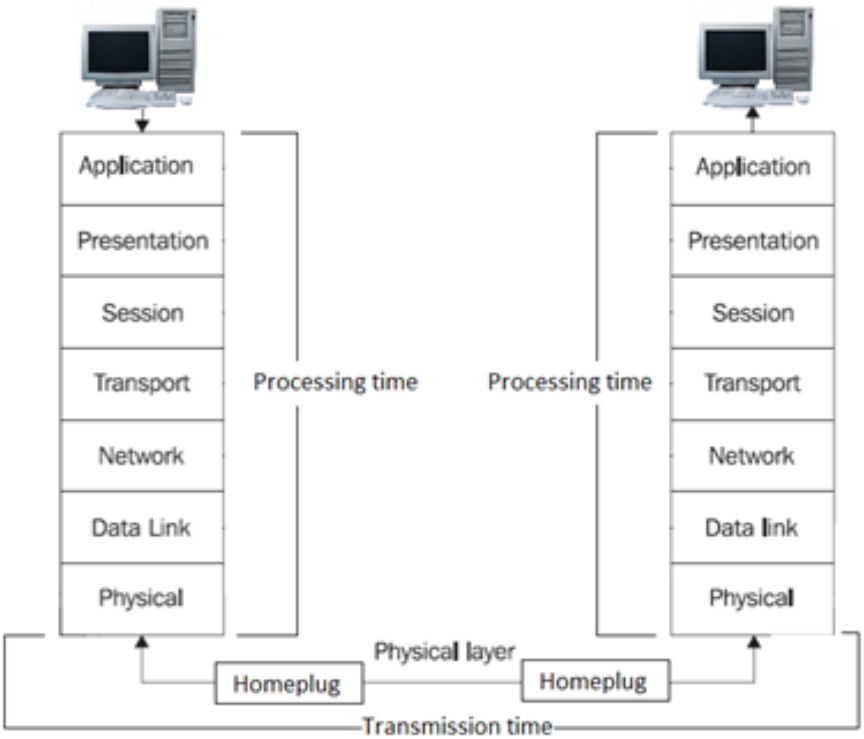

Figura 4.1: Tempo de transmissão

4.1.4 Jitter

O Jitter pode ser definido como uma variação do atraso na recepção de pacotes consecutivos numa rede de dados. Este valor pode ser obtido medindo a diferença entre o tempo decorrido entre a saída de 2 pacotes sucessivos (t3-t1) e o tempo decorrido entre a recepção do 1º e do 2º pacote transmitidos (t4-t2), tal como apresentado na Figura 4.2. A diferença entre estes dois tempos é o valor do jitter. Um valor elevado de jitter corresponde a uma recepção inconstante dos dados, o que pode influenciar a qualidade do serviço da aplicação, como é o caso das chamadas VoIP.

$$jitter(ms) = (t_3 - t_1) - (t_4 - t_2) \tag{4.2}$$

Figura 4.2: Jitter

4.2 Equipamentos e topologias da rede

Todos os testes realizados foram efectuados em ambiente laboratorial, no laboratório I005 do Departamento de Engenharia Electrotécnica e de Computadores da Universidade do Porto. Os recursos utilizados estavam maioritariamente disponíveis no laboratório, tendo existido contudo a necessidade de aquisição de algum hardware, nomeadamente 3 módulos *Homeplug AV dLan® 200AVmini* [26] e um filtro de linha [27]. Todo o restante material foi escolhido de modo a permitir criar uma rede de baixo custo, controlada e totalmente replicável.

4.2.1 Equipamentos

Nesta subsecção serão apresentados os principais equipamentos utilizados ao longo do trabalho desenvolvido nesta dissertação. Equipamentos específicos a cada cenário de análise serão apresentados aquando da apresentação do respectivo cenário.

- PC1

Este computador foi utilizado em todos os testes, desempenhando o papel de emissor dos dados.

Processador: Intel® Pentium® Dual CPU T2330 @ 1.60GHz
Memória: 2.00 GB
Sistema Operativo: Ubuntu 10.10 – 32 bit
Placa de rede: 1 Gbps

- PC2

Este computador foi utilizado em todos os testes, desempenhando o papel de receptor dos dados.

Processador: Intel® Pentium® 4 CPU @ 2.8GHz
Memória: 1.00 GB

Sistema Operativo: Ubuntu 10.04 – 32 bit
Placa de rede: 100 Mbps

- PC3

Este computador foi utilizado nos testes de tráfego tempo real, tal como descrito na subsecção 4.4.2. O papel desempenhado foi o de emissor de tráfego adicional ao tráfego de teste.
Processador: Intel® Pentium® 4 CPU @ 2.8GHz
Memória: 1.00 GB
Sistema Operativo: Windows XP - 32 bit – SP 3
Placa de rede: 1 Gbps
Alimentação: 230 Volts 4 A
Potência Fonte: 300 W Max.

- Módulos HPAV

Modelo: dLan® 200AVmini
Quantidade: 3
Standards: *Ethernet specifications IEEE 802.3, IEEE 802.3x, IEEE 802.3u, Auto MDI / X HomePlug AV*
Protocolos: CSMA/CA
Velocidade Máxima: 200 Mbps
Modulação: OFDM – 1155 carriers, 1024/256/64-QAM, QPSK, BPSK
Interfaces: *Ethernet* RJ45 <-> Conector eléctrico *EuroPlug*
Datasheet: [28]

4.2.2 Cenários de teste

Com intuito de simular o mais possível uma rede eléctrica industrial e respectivas cargas existentes numa planta industrial, tendo em conta o tipo de equipamentos disponíveis para a realização dos trabalhos, foram montados um conjunto de 8 cenários distintos. Destes 8 cenários, 6 proporcionam um ambiente controlável e facilmente replicável em ambiente laboratorial, o que confere uma elevada repetibilidade aos testes realizados.

- Cenário 1

O primeiro cenário utilizado serviu para testar e comprovar o desempenho de uma rede *Ethernet* ponto a ponto. Este cenário serviu também para se obter os valores base para as medidas a recolher, uma vez que os módulos utilizados possuem interface *Ethernet*. Os valores da rede ponto a ponto, nomeadamente o valor da latência e do jitter, foram recolhidos para posteriormente serem comparados e subtraídos aos valores obtidos com a rede *Homeplug*, obtendo-se assim os valores e as alterações provocadas unicamente pela tecnologia *Homeplug*.

O primeiro cenário consiste numa ligação *Ethernet* ponto a ponto entre o PC1 e o PC2, como representado na Figura 4.3.

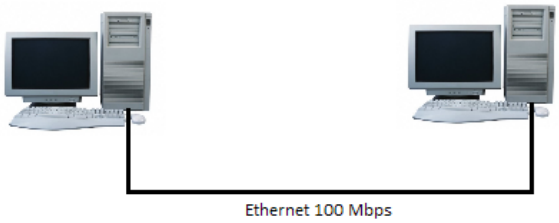

Figura 4.3: Cenário 1

- Cenário 2

O cenário 2 foi criado com o intuito de verificar e avaliar o funcionamento de uma rede *Homeplug* num ambiente real, não controlado, e com diversos equipamentos ligados simultaneamente à rede eléctrica. Para o efeito os módulos *Homeplug* foram conectados directamente na rede eléctrica do laboratório I005 a uma distância de aproximadamente 10 metros entre si, tal como apresentado na Figura 4.4.

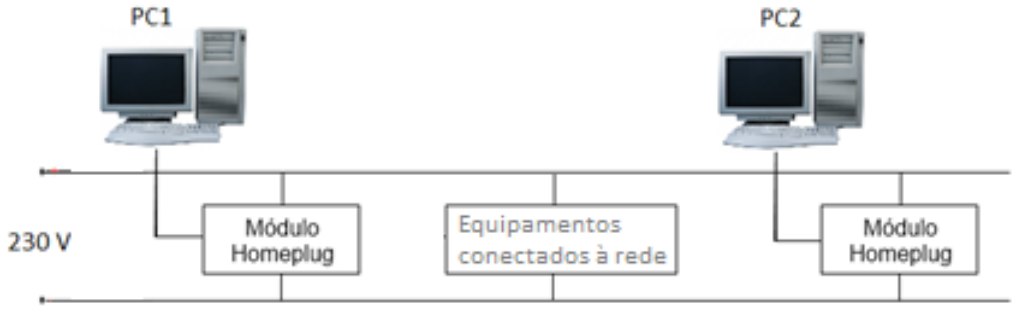

Figura 4.4: Cenário 2

- Cenário 3

O cenário 3 tem como objecto verificar e avaliar o desempenho da rede *Homeplug* quando os módulos são conectados numa rede eléctrica isolada e filtrada de interferências electromagnéticas externos. Esta rede permite assim realizar os testes num ambiente controlado e facilmente replicável.

Para a criação da rede isolada foram utilizados dois transformadores, T1 e T2, ligados em *back-to-back*, de modo a obter-se uma razão de transformação de 1:1, ou seja funcionarem apenas como transformador de isolamento. Os dois transformadores permitem assim isolar o troço de rede eléctrica, no qual decorrerão os testes, da rede eléctrica do laboratório. Este isolamento tem como principal objectivo eliminar as interferências electromagnéticas provenientes dos vários equipamentos conectados à rede eléctrica.

Características dos transformadores:

Dois transformadores trifásicos T1 e T2 de características idealmente iguais.
Potência: 750 kVA
Rácio de transformação: 0.22
Tensão primário: 230 Volts
Tensão secundário: 50 Volts
Esquema de ligação: Y-Δ

A jusante dos transformadores foi ainda introduzido um filtro de linha [26] com o objectivo de eliminar as interferências provenientes da rede eléctrica, que não tenha sido previamente eliminado pelos transformadores. Este filtro é um filtro constituído por dois estágios, dimensionado para eliminar as interferências a altas frequências, pois são estas usadas para modulação dos sinais da rede HPAV.

Características do filtro:

Alimentação: 230 Volts 6 A
Modelo: CORCOM 6VW1
Tipo: Filtro de altas frequências
Datasheet: [26]
Esquemático:

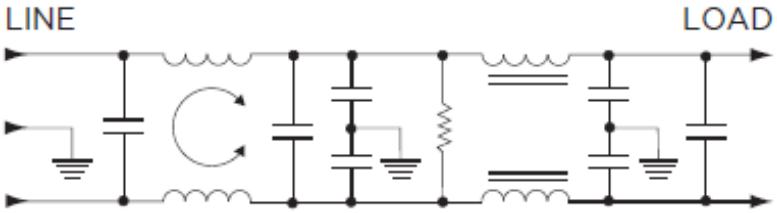

Figura 4.5: Esquemático do filtro [26]

Este tipo de configuração permite assim obter um troço da rede eléctrica filtrado de interferências electromagnéticas externas.

A este troço foram seguidamente conectados os módulos HPAV, a uma distância de aproximadamente 4 metros, como indicado na Figura 4.6.

Os cenários 4, 5 , 6 ,7 e 8 consistem em acrescentar cargas eléctricas ao cenário 3, com o intuito de injectar interferências na rede, as cargas utilizadas foram um Monitor CRT (CRT1), um computador (PC3) e um motor (M1). Estas cargas foram escolhidas por existirem frequentemente em ambientes industriais.

O principal objectivo destes testes é verificar que efeito das interferências electromagnéticas, introduzidas pelas mesmas na rede eléctrica, tem sobre as transmissões de dados na rede HPAV.

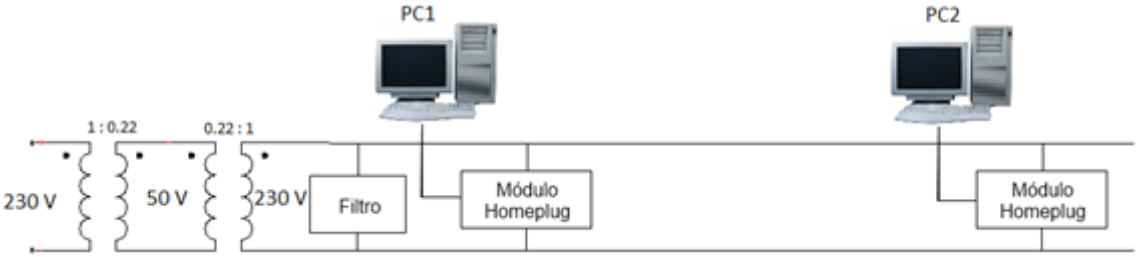

Figura 4.6: Cenário 3

- Cenário 4

Introdução de um monitor CRT conectado à rede eléctrica isolada, como representado na Figura 4.7.

Características do monitor:

Tipo: CRT

Modelo: Compaq S710

Alimentação: 230 Volts 50 Hz 1.4 A

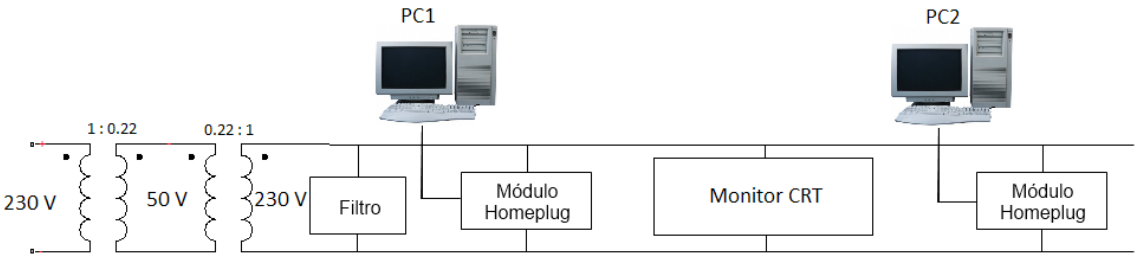

Figura 4.7: Cenário 4

- Cenário 5

No cenário 5 desligou-se o monitor CRT1 e ligou-se um computador PC3, tal como na Figura 4.8.

A introdução deste tipo de equipamento na rede permitiu verificar o impacto das fontes de alimentação deste tipos de equipamento na transmissão de dados, através da rede eléctrica. Estes equipamentos possuem fontes de tensão comutadas, as quais são potencias fontes geradoras de interferências electromagnéticas.

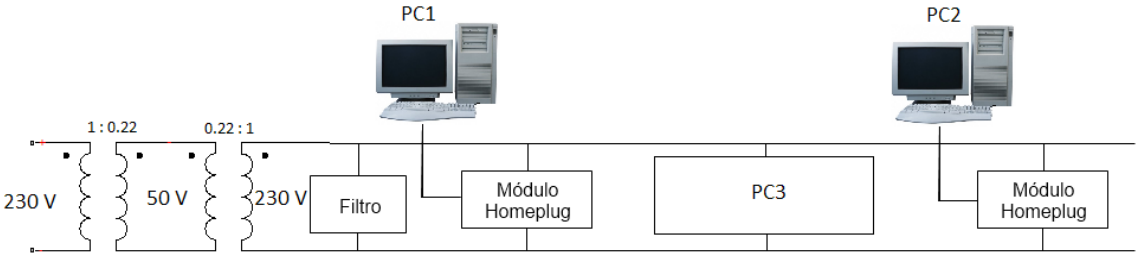

Figura 4.8: Cenário 5

- Cenário 6

Neste cenário foi novamente introduzido o monitor CRT1, em conjunto com o PC3 (Figura 4.9).

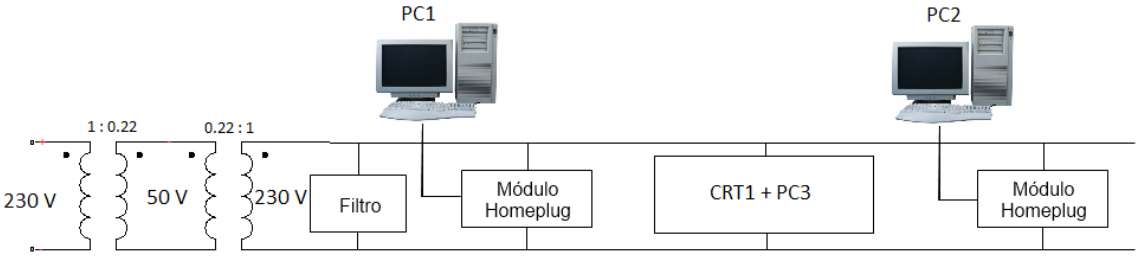

Figura 4.9: Cenário 6

- Cenário 7

Para realização de testes com outro tipo de equipamentos, alimentou-se o motor M1 através do troço de rede isolada previamente criado (Figura 4.10). O motor foi colocado em funcionamento, recorrendo a um variador de velocidade, até à sua velocidade nominal de 1410 rpm. O motor utilizado foi um motor de escovas, o que poderá ser uma fonte de interferências electromagnéticas, aquando dos contactos das escovas com os diferentes enrolamentos.

Características do motor:

Modelo: IEME VN6364
RPM: 1410
Potência: 0.18 Kw
Cos (phi): 0.67
Alimentação: 220 Volts Δ 0.85 A

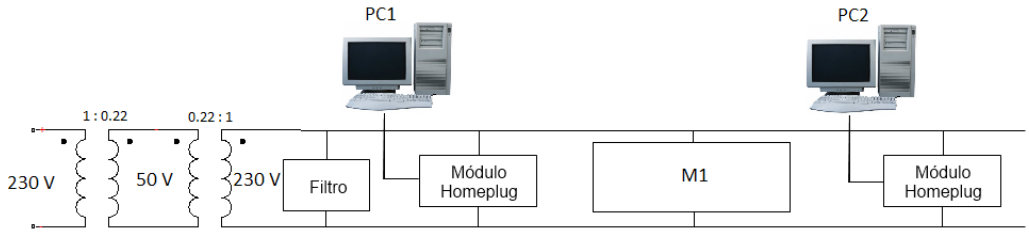

Figura 4.10: Cenário 7

- Cenário 8

Por último foram conectadas à rede eléctrica todas as cargas anteriormente utilizadas, em simultâneo (Figura 4.11).

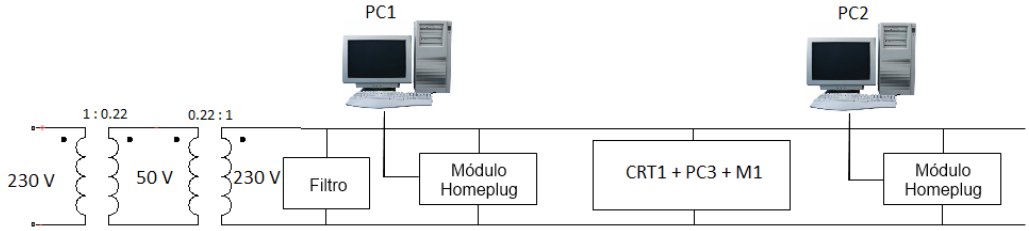

Figura 4.11: Cenário 8

4.3 Ferramentas

Nesta secção serão apresentadas a principais ferramentas utilizadas no decorrer dos testes.

Estas ferramentas podem ser divididas consoante a sua funcionalidade e podem ser agrupadas em três grupos, sendo estes a geração de tráfego, a análise do tráfego na rede e a sincronização de relógios entre computadores.

4.3.1 Geração de Tráfego

Iperf / Jperf

O Iperf é uma ferramenta desenvolvida pela NLANR/DAST, com o intuito de possibilitar a medição da máxima largura de banda quer em tráfego TCP, quer em tráfego UDP, de uma forma simples e intuitiva ao utilizador. O Iperf permite a configuração de vários parâmetros e reporta a largura de banda, jitter e pacotes perdidos [29].

O Jperf é uma *framework* escrita em Java, que permite executar e escrever testes de desempenho de rede automáticos. Esta aplicação é frequentemente descrita como sendo uma interface gráfica para o Iperf, pois a sua função é apenas criar uma classe *PerfTest* e de seguida criar uma instância *PerfTestRunner* para executar os testes, o que não é mais que o Ipef a executar os comandos enviados pelo utilizador, mas de uma forma automática [30].

O software Iperf funciona numa topologia cliente – servidor (Figura 4.12), ou seja deve ser instalado em ambas as máquinas. Seguidamente um dos equipamentos deve ser configurado como servidor, onde apenas é necessário configurar a porta à escuta, o tipo de tráfego a ser recebido e o intervalo para reportar os resultados. Na outra máquina, é necessário configurar a aplicação como cliente, e aqui sim, já é possível configurar diversos parâmetros adicionais, dependendo do tipo de tráfego a ser gerado.

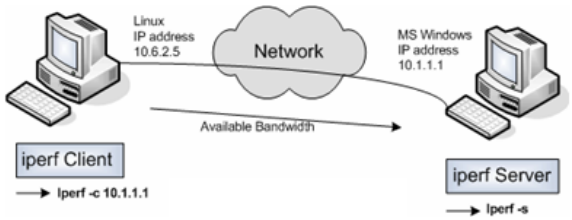

Figura 4.12: Transmissões Iperf [31]

Para tráfego TCP, os principais parâmetros configuráveis são o tamanho do *buffer*, TCP *window size* e *max segment size*, apesar de alguns destes parâmetros se encontrarem limitados pelo sistema operativo. Durante os testes TCP a aplicação cliente gera tráfego TCP com as especificações indicadas à maior taxa possível e os valores de *bandwidth* são apresentados quer numericamente quer graficamente em intervalos previamente definidos pelo utilizador. Os intervalos utilizados neste trabalho foram intervalos de 1 segundo entre actualizações e testes de duração de 60 segundos. No final do teste é também apresentado o valor médio obtido (Figura 4.13).

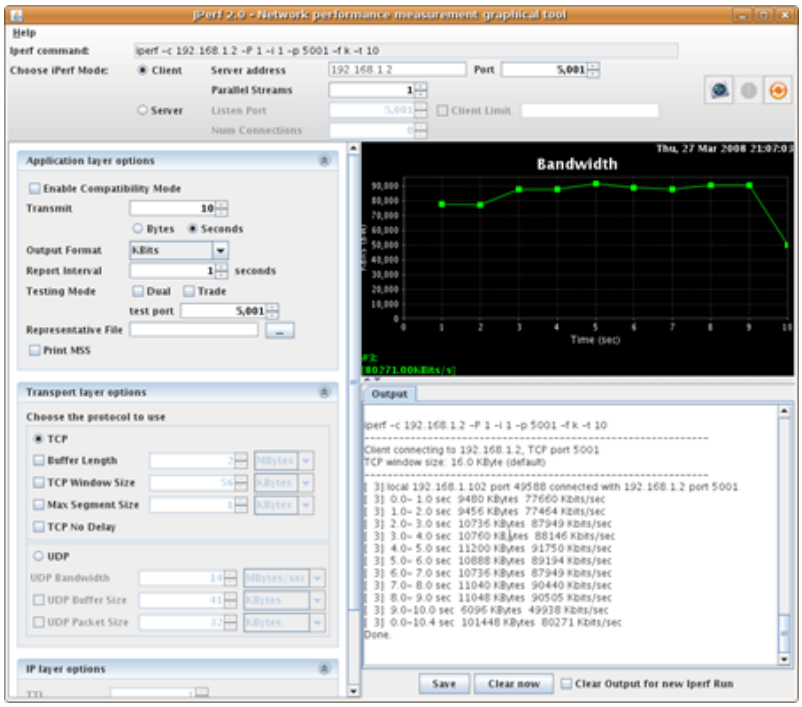

Figura 4.13: Interface TCP [31]

Para testes realizados com tráfego UDP, os pacotes já não são gerados à taxa máxima, mas sim à taxa previamente definida pelo utilizador. Caso esta taxa seja superior à capacidade do meio de transmissão, os pacotes são transmitidos à taxa máxima permitida pelo meio. No caso da rede *Homeplug* a velocidade máxima utilizada foi 100 Mbps, pois este é também o limite da interface *Ethernet* utilizada, para comunicações unidireccionais. Por este facto os resultados dos testes UDP são apresentados do lado do servidor e não do lado do cliente, ao contrário dos testes TCP. Para este tipo de tráfego os parâmetros configuráveis são o tamanho do buffer e o tamanho dos pacotes a serem gerados. Com pacotes UDP, e à semelhança dos testes TCP, é apresentado em intervalos predefinidos os valores da largura de banda, do jitter e dos pacotes perdidos, Figura 4.14.

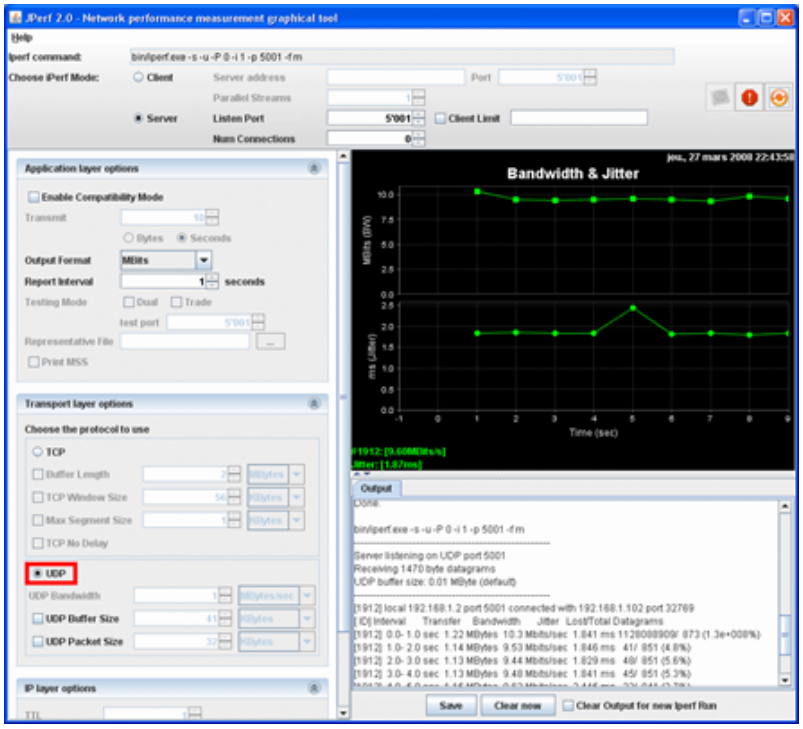

Figura 4.14: Interface UDP [31]

packETH

O *packETH* é um software que permite gerar todos os tipos de pacotes existentes para *Ethernet*, este software é de uso e alteração livre, segundo os termos da versão 2 da *GNU General Public License*. Este software foi inicialmente desenvolvido para *Linux*, mas existe actualmente, na sua versão 1.6, uma versão para *Windows* [32].

O *packETH* permite configurar vários parâmetros dos pacotes a serem gerados, consoante o seu tipo. Para este trabalho apenas foi utilizado para gerar pacotes UDP, tendo sido configuradas as seguintes opções: *MAC Adress*, *IP* e portas de partida e de destino, e o *payload*, que define o tamanho do pacote. O interface para a configuração dos pacotes pode ser visto na Figura 4.15.

Esta ferramenta foi utilizada para geração de pacotes, em substituição do Iperf, devido a esta permitir uma maior configuração do tipo de tráfego a gerar, não só da taxa de transmissão , mas

também do intervalo de tempo decorrido entre cada pacote transmitido. Esta última funcionalidade foi essencial para a geração de tráfego tempo real periódico.

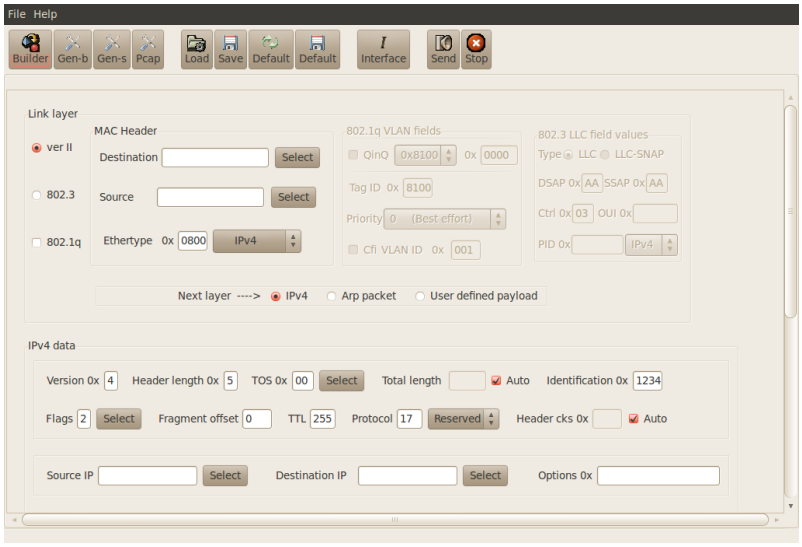

Figura 4.15: Interface criação pacotes

Para além da possibilidade da criação dos mais variados tipos de pacotes, esta aplicação permite ainda criar *streams* de pacotes, onde se pode configurar a taxa de transmissão dos pacotes em Mbps, ou caso assim se pretenda, pode-se definir um intervalo de tempo entre cada pacote a ser transmitido, em microsegundos, o que permite assim gerar tráfego periódico. Estas duas funcionalidades foram utilizadas para a realização dos testes desta Dissertação. O ambiente gráfico para a configuração destas *streams* de pacotes encontra-se apresentado na Figura 4.16.

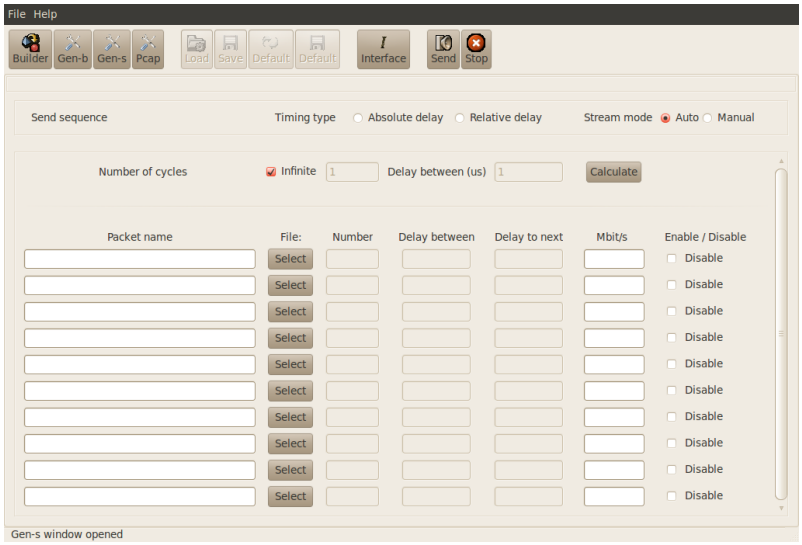

Figura 4.16: Interface criação streams

4.3.2 Análise do tráfego na rede

Wireshark

O *Wireshark* é um analisador de protocolos de comunicação, que permite capturar e analisar os pacotes transmitidos na rede. Esta é uma ferramenta largamente utilizada para análise de tráfego de redes, pois está disponível tanto para *Windows*, como para *Linux*, *Unix* e *OS X*, Esta aplicação é gratuita, contudo é licenciada pela versão 2 da *GNU General Public License*. Esta aplicação está em constante actualização e possui já uma extensa capacidade de lidar com vários tipos de protocolos de dados transmitidos na rede [33].

Com esta aplicação pretendeu-se medir os valores do latência e do jitter, sofridos pelos pacotes. O valor do jitter pode também ser obtido através do *Iperf*, contudo este não reporta os valores da latência, pelo que se torna necessária a utilização desta aplicação. Como o *Wireshark* aplicação não depende da aplicação que gera os pacotes, pode ser utilizado tanto para tráfego gerado pelo *Iperf*, como para tráfego gerado pelo *packETH*.

Para a realização dos trabalhos, o *Wireshark* deve ser configurado tanto no PC1, como no PC2, para capturar pacotes do protocolo a utilizar (UDP ou ICMP), e também na Porta, para a qual se está a transmitir os dados. Esta configuração é essencial, pois permite que sejam capturados apenas os pacotes relevantes aos testes a realizar, sendo descartado o restante tráfego existente na rede. O filtro de captura utilizado para capturar tráfego UDP foi o seguinte:

```
UDP port 5001
```

Este filtro permite assim capturar todos o pacotes UDP recebidos ou enviados pela porta 5001. O filtro é o mesmo para os dois computadores, pois no PC1 apenas existe tráfego de saída e no PC2 tráfego de chegada na porta 5001. Todo o restante tráfego na rede é descartado.

Em alternativa poderia ser capturado todo o tráfego e posteriormente ser aplicado um filtro de visualização, contudo esta é uma solução mais desvantajosa, uma vez que ao fim de pouco tempo o número de pacotes capturados pode ser tão elevado que se torna complicado tratar os resultados.

Aquando da captura de cada pacote, o *Wireshark* insere no relatório de captura um *timestamp*, ou seja, o número de segundos passados desde o *Epoch* (01-01-1970) [33], com uma resolução de microsegundos. Este valor é por sua vez obtido através da livraria *Libpacap* que gera os *timestamps* a partir do relógio interno do computador, estando a sua qualidade dependente do sistema operativo.

Para obter os valores da latência e do jitter terão de ser directamente comparados os *timestamps* inseridos tanto pelo emissor, como pelo receptor, existindo a necessidade de ambos os relógios estarem sincronizados. Esta sincronização é efectuada recorrendo ao software PTPd2, tal como apresentado na subsecção 4.3.3. Como esta sincronização não é imediata, é necessário sincronizar previamente os relógios dos dois computadores e só depois iniciar o *Wireshark*. Durante a realização dos testes foi adoptado um tempo mínimo de 30 minutos para sincronização, e só depois foi iniciado o *Wireshark*.

Antes de cada teste deve ser dada a ordem para o início de uma nova captura de dados (Figura 4.17). No final de cada teste os resultados obtidos devem ser exportados para um ficheiro CSV, permitindo assim o seu posterior tratamento.

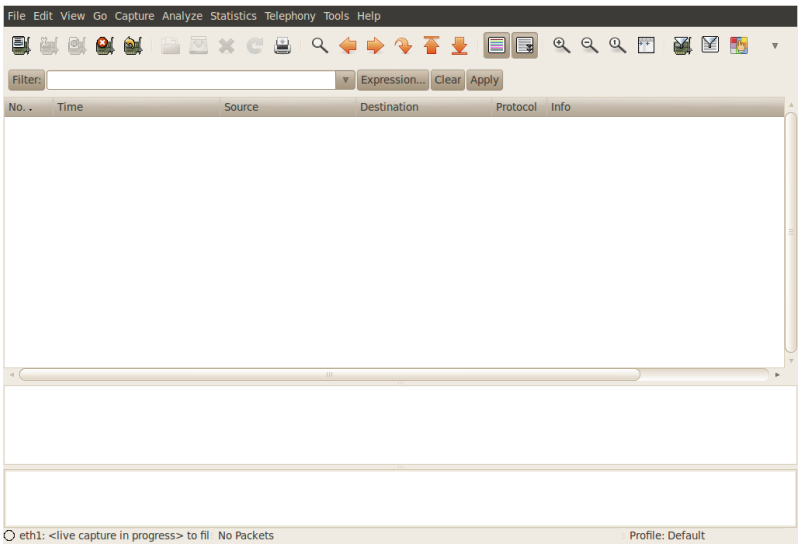

Figura 4.17: Interface Wireshark

4.3.3 Sincronização dos relógios

PTPd2

Para a sincronização dos relógios entre os computadores foi utilizada a ferramenta *PTPd2* [34]. Este software implementa o *Precision Time Protocol*, tal como definido no *Standard IEEE 1588-2008 (versão 2)* [35].

O PTP (*Precision Time Protocol*) é um protocolo de sincronização de relógios de alta precisão, que permite a sincronização entre vários computadores conectados na mesma LAN. O PTP foi originalmente definido pelo *standard IEEE 1588-2002* [36] tendo sido posteriormente revisto pelo *standard IEEE 1588-2008* [35]. Esta última revisão permite uma maior exactidão, precisão e robustez na sincronização dos relógios, mas não é compatível com a versão anterior. A versão 2 do protocolo PTP baseia-se numa arquitectura mestre - escravo, onde o mestre é escolhido através do algorítmo BMC (*Best Master Clock*), e segundo as propriedades previamente anunciadas por cada um dos relógios.

Nesta versão estão definidos três tipos de relógios: o *ordinary clock* que é um relógio com uma única conexão à rede e pode funcionar como mestre ou escravo, o *boundary clock* que é um relógio com múltiplas conexão a diferentes redes e actua como sincronizador entre redes, e por último, o *transparent clock* que altera as mensagens PTP, à medida que elas passam através dos diferentes equipamentos das rede, corrigindo os *timestamps* à media que as mensagens passam através dos equipamentos.

Na rede utilizada durante os testes apenas foram utilizados os *ordinary clocks* dos computadores PC1 e PC2

A sincronização entre os relógios é efectuada utilizando mensagens *multicast* como se apresenta na figura 4.18, esta troca de mensagens permite que os escravos determinem a sua diferença temporal em relação ao mestre, para posteriormente tomarem medidas por forma a minimizar esta diferença.

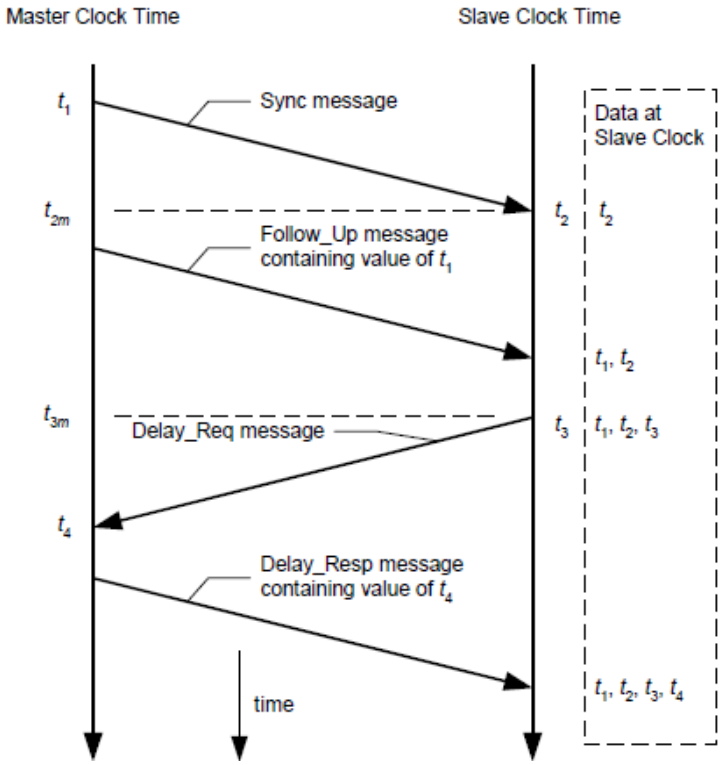

Figura 4.18: Mensagens transmitidas [37]

Todas as mensagens PTP são enviadas em *multicast*, apesar do *standard* prever também a utilização de mensagens *unicast*. As mensagens são enviadas utilizando o protocolo de transporte IP e contidas em pacotes UDP [37].

Método de Sincronização

Para efectuar a sincronização entre relógios, são trocadas várias mensagens, como apresentado anteriormente. Esta troca de mensagens inicia-se, a cada 2 segundos (Tms), aquando da transmissão, por parte do mestre de uma mensagem *Sync*. Nesta altura o mestre guarda no pacote da mensagem o tempo de envio da mesma (t1) e o escravo grava o tempo da sua recepção (t2). Existem ainda mestres que não têm a possibilidade de enviar o valor de t1 na mensagem de Sync e utilizam a mensagem de *Follow_Up*, que é enviada logo de seguida à mensagem *Sync*, e que contém o tempo de envio da primeira.

Calculando a diferença entre estes dois valores pode ser obtido o valor do *delay master-slave* (dms).

$$d_{ms} = t_2 - t_1 \tag{4.3}$$

$$T_{ms} = T_{syn} = 2seg \tag{4.4}$$

Após ter recebido uma mensagem *Sync*, ou uma mensagem Sync e uma *Follow_Up*, o escravo envia uma mensagem *Delay_Req*. Esta mensagem contém o valor do tempo de envio por parte do escravo (t3). Por sua vez, o mestre, aquando da recepção desta mensagem grava também o tempo da sua recepção, enviando-o de seguida através da mensagem *Delay_Resp*.

Calculando a diferença entre estes tempos obtém-se o valor do *Delay slave-master* (dsm).

$$d_{sm} = t_3 - t_4 \tag{4.5}$$

Estas mensagens são enviadas em intervalos uniformemente distribuídos entre 2 e 30 intervalos de *Sync*. Obtendo então o período de amostragem do *delay slave-master* segundo a seguinte fórmula:

$$T_{sm} = T_{sync} \times U[2,30] \tag{4.6}$$

Para o cálculo do tempo de uma viagem, *one-way delay*, assume-se que o tempo de propagação das mensagens é simétrico, de tal forma que a média dos tempos de *delay master-slave* e *delay slave-master* anulam o *offset* dos dois relógios. Com esta aproximação consegue-se então calcular o *one-way delay* (dow), segundo a seguinte fórmula:

$$d_{ow} = \frac{d_{ms} - d_{sm}}{2} \tag{4.7}$$

Obtido este valor, podemos então calcular o valor de *offset* entre os dois relógios (Δt), como se segue:

$$\Delta t = |d_{ms} - d_{ow}| \tag{4.8}$$

Calculado o *offset* entre os relógios, o *software PTPd2* ajusta o valor do relógio do escravo, efectuando um *reset* deste, caso o *offset* seja superior a 1 segundo, ou ajustando gradualmente até

atingir o valor pretendido. Este é um processo demorado, mas bastante preciso [38].

4.4 Descrição dos testes

Os testes efectuados, tal como referido previamente foram divididos em dois grandes grupos. O primeiro grupo teve como objectivo a medição da largura de banda, a perda de pacotes, a latência e o jitter do e tráfego TCP e UDP com diferentes características. O segundo grupo, tem como principal objectivo a avaliação do desempenho de uma rede Homeplug quando sujeita a tráfego UDP periódico.

Seguidamente serão descritas as metodologias utilizadas para medir cada um dos parâmetros já descritos.

4.4.1 Tráfego não periódico

Largura de banda

Para medição da largura de banda foi utilizada uma ferramenta *Iperf*, em conjunto com o seu ambiente gráfico, denominado de *Jperf*.

A largura de banda foi medida tanto para tráfego UDP como para tráfego TCP, sendo utilizada a mesma metodologia para a sua medição. Esta metodologia consiste em gerar tráfego do cliente para o servidor, à velocidade máxima permitida pela rede, durante um período fixo de tempo. Durante os vários testes foram adoptados 60 segundos como sendo a duração dos testes, pois é considerado um intervalo de tempo razoavelmente alargado, o que permite eliminar algumas variações indesejadas enquanto tende para um estado de regime permanente onde a variação da largura de banda é mínima. Ao mesmo tempo, este é um intervalo de tempo razoavelmente curto, o que permite um rápido tratamento dos dados e não alarga em demasia a duração dos testes.

Os dados são gerados pela aplicação *Iperf* cliente, a executar no PC 1 e recebidos pela aplicação *Iperf* servidor, a executar no PC 2.

Durante o decorrer do teste, o valor da largura de banda é actualizado de segundo a segundo. No final o valor médio da largura de banda é calculado através do cálculo da média dos valores reportados pela ferramenta, excluindo os 5 segundos iniciais da experiência, pois estes podem ser vistos como um período de *warm-up*, como se comprova no Capítulo 5.

Para o tráfego TCP, o teste foi repetido para diferentes valores do *TCP Window Size*, foram utilizados os seguintes valores: 10KBytes, 50KBytes, 100KBytes e 256KBytes, sendo este último o valor máximo permitido pelo sistema operativo adoptado. A variação deste parâmetro influência significativamente a quantidade de dados que podem ser transmitidos, sem a existência de uma mensagem *ACK*, tal como se verifica na Figura 4.19.

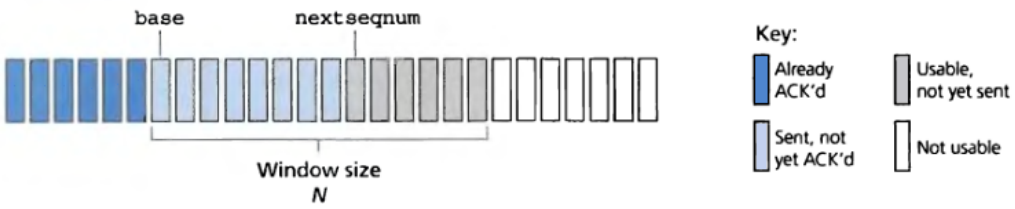

Figura 4.19: TCP Window Size [25]

Se definirmos a *base* como sendo o número do último pacote transmitido, mas ainda não reconhecido. E *nextseqnum* como o número do próximo pacote a ser enviado, as 4 divisões na Figura 4.19 têm os seguintes valores [25]:

- Pacotes com número contido em [0, base-1] - Pacotes transmitido e reconhecidos;
- Pacotes com número contido em [base, nextseqnum-1] - Pacotes transmitido mas ainda não reconhecidos;
- Pacotes com número contido em [nextseqnum, base+N] - Pacotes que podem ser enviados imediatamente;
- Pacotes com número superior a base+N - Pacotes que têm que esperar até que haja o reconhecimento de pelo menos um do pacotes enviados anteriormente.

Com esta divisão percebe-se que o valor de N, ou seja do *TCP Window Size*, influencia directamente o número de pacotes na rede sem terem sido reconhecidos, influenciando consecutivamente o número de pacotes a serem transmitidos em caso de não reconhecimento dos mesmos.

Estes testes foram repetidos para vários valores do *TCP Window Size* nos cenários 1, 2 e 3.Nos restantes cenários apenas se utilizou o valor de TCP Window Size igual a 256 KBytes, permitindo assim inferir sobre a influência das diferentes topologias da rede na largura de banda máxima.

Para o tráfego UDP, o teste foi efectuado com pacotes de diferentes tamanhos, 750 Bytes, 1472 Bytes e 2000 Bytes, a escolha destes valores permite visualizar o comportamento da rede aquando da existência ou não de fragmentação de pacotes. Neste caso, para redes *Ethernet* com MTU de 1500 bytes, poderemos ter um pacote UDP com o máximo de 1472 bytes de dados + 8 bytes do cabeçalho UDP + 20 bytes do cabeçalho IP, o que corresponde aos 1500 bytes de MTU da rede *Ethernet*.

Tal como nos testes TCP, nestes foram descartados os primeiros 5 segundos da experiência, eliminando assim o regime transitório, e foi calculada a média dos resultados reportados pela ferramenta para os 55 segundos seguintes.

Os testes foram realizados nos mesmo cenários que os testes de largura de banda TCP.

Perda de pacotes

A medição do número de pacotes perdidos foi realizada em conjunto com os testes da largura de banda, exclusivamente para tráfego UDP, pois esta medida não é relevante para tráfego TCP devido à retransmissão dos pacotes perdidos.

O número de pacotes perdidos é actualizado na aplicação Jperf do lado do receptor a cada segundo, no final do teste o número de pacotes perdidos é calculado através da média dos valores reportados pela aplicação, descartando novamente os 5 segundos iniciais.

Para cada tamanho de pacotes, foram criadas *streams* de dados de 60 segundos e às seguintes velocidades de transmissão: 10 Mbps, 50 Mbps e 100 Mbps do lado do emissor. Como apenas se verificaram perdas de pacotes para as velocidades máximas, apenas estes testes foram efectuados em todos os cenários.

Todos os testes foram repetidos até se alcançar um intervalo de confiança mínimo de 95 %. Para tal, os resultados foram divididos por intervalos de 5 segundos e calculou-se a média dos pacotes perdidos para cada um desses intervalos segundo a seguinte equação [39]:

$$\bar{X} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{4.9}$$

Obtida a média, podemos calcular o desvio quadrado como se segue [39]:

$$\sigma^2\left[\bar{X}(n)\right] = \sum_{i=1}^{n} \frac{(x_i - \bar{X}(n))^2}{n(n-1)} \tag{4.10}$$

Obtidos a média e o desvio quadrado, pode ser calculado o erro relativo, que deve ser majorado em 0,05, ou seja, 5% [39].

$$\varepsilon = \frac{1.96 \times \sigma\left[\bar{X}(n)\right]}{\bar{X}(n)} \tag{4.11}$$

As experiências foram repetidas até se obter valores de erro relativo inferiores a 5%, o que significa que se pode afirmar com 95% de certeza que os resultados apresentados nos estudos são válidos.

Latência

Para a medição da latência utilizou-se apenas tráfego UDP. Este tráfego é gerado no emissor recorrendo à ferramenta *packETH*, que permite definir o tamanho dos pacotes a gerar, o endereço e a porta de recepção e a taxa de transmissão de dados. Os pacotes foram gerados com três tamanhos diferentes: 45 bytes, 750 bytes e 1472 bytes, permitindo assim uma análise do comportamento da

rede com pacotes do tamanho máximo de um pacote sem fragmentação, tamanho médio e tamanho baixo, exemplificativo do tráfego tipicamente industrial.

Para além da variação do tamanho dos pacotes, os testes foram realizados a diferentes taxas de transmissão, 10 Mbps, 50 Mbps e 100 Mbps, permitindo assim analisar o comportamento da rede para taxas de transmissão próximas do máximo, bem como taxas mais baixas. Estes testes foram repetidos em todos os cenários.

Durante os testes de latência foram gerados 10000 pacotes por teste, o que permite uma análise de um número considerável de pacotes, bem como determinar se existem perdas de pacotes.

Para a análise de pacotes na rede foi utilizado o software *Wireshark* (Figura 4.20). Sempre que é enviado ou recebido um pacote na carta de rede, o *Wireshark* captura esse pacote e insere um *timestamp* no relatório de captura.

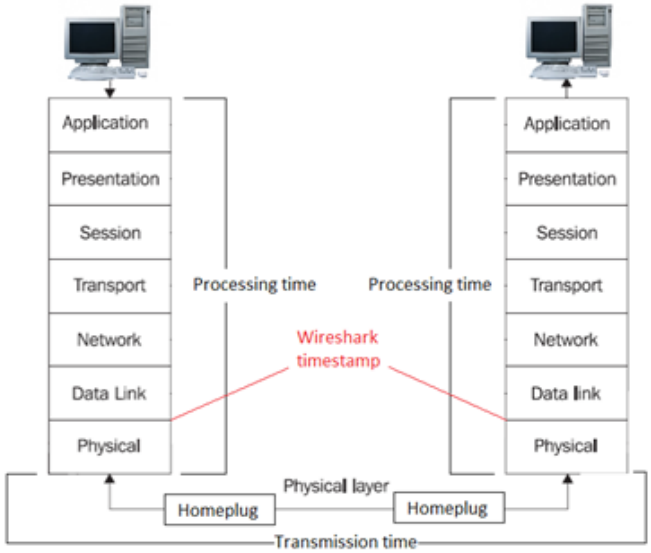

Figura 4.20: Timestamp Wireshark

Com os relógios sincronizados e com o *Wireshark* a capturar os pacotes em ambos os computadores, o *Wireshark* medirá o tempo de propagação dos pacotes na rede, acrescido do tempo de bufferização dos pacotes na carta de rede, contudo este tempo foi desprezado no decorrer dos testes realizados neste trabalho pois pode ser considerado como constante em todos os testes e é um tempo bastante reduzido quando comparado com o tempo de latência dos pacotes.

Como já referido, os testes foram realizados em grupos de 10000 pacotes e no final calcula-se o tempo de latência de cada destes. Subtraindo o tempo de recepção ao tempo de envio de cada um dos pacotes transmitidos, obtém-se o tempo de transferência do pacote.

$$Latncia = t_{recepo} - t_{envio} \tag{4.12}$$

Seguidamente foi calculada a média do tempo de latência para grupos de 1000 pacotes, obtendo os valores médios da latência para 10 grupos.

$$\bar{Latncia} = \frac{1}{1000} \sum_{i=1}^{1000} Latncia_i \tag{4.13}$$

No final foi novamente calculado o erro relativo para a média desses 10 grupos, repetindo-se a realização do teste até à obtenção de um erro relativo inferior a 5%.

Jitter

Como definido anteriormente o jitter é a variação no tempo de recepção de dois pacotes consecutivos. Esta medida foi obtida recorrendo novamente à captura de pacotes efectuada pelo *Wireshark*, como já descrito anteriormente, com os relógios sincronizados, conseguimos obter os *timestamps* de envio e de recepção dos vários pacotes. Comparando o intervalo entre estes, obtemos o valor do jitter segundo a seguinte fórmula:

$$jitter(ms) = (t_3 - t_1) - (t_4 - t_2) \tag{4.14}$$

Figura 4.21: Timestamps para cálculo do Jitter

Sendo: t1=*timestamp* envio do pacote1; t2=*timestamp* recepção pacote1; t3=*timestamp* envio pacote2; t4=*timestamp* recepção pacote2.

Mais uma vez o valor médio do Jitter foi calculado para grupos de 1000 pacotes, e foi ainda calculado o respectivo intervalo de confiança. Caso este estivesse abaixo dos 95%, a experiência seria repetida.

4.4.2 Tráfego periódico

Para a avaliação do comportamento da rede HPAV, quando utilizada para a transferência de tráfego periódico, configurou-se o PC 1 para gerar tráfego UDP a ser transmitido entre este e

o PC 2, através do software *packETH* [32], de tamanho 45 bytes. Assim permite-se simular, aproximadamente, o tipo de tráfego utilizado em aplicações industrias, para diferentes frequências, com um intervalo de tempo entre pacotes de 100 ms, 50 ms, 10 ms e 1 ms. Valores mais baixos para o período entre pacotes a transmitir não foram considerados, pois são mais baixos do que o próprio tempo de latência já anteriormente calculado.

Os testes realizados foram efectuados nos mesmos moldes já descritos para a medição da Latência e do Jitter e repetidos em todos os cenários de rede considerados no decorrer desta dissertação.

Numa primeira fase, os testes foram realizados isoladamente, apenas com o tráfego UDP periódico em todos os tipos de cenários (Figura 4.22). Seguidamente foram novamente realizados, mas com a introdução do PC 3 a transmitir tráfego TCP a uma velocidade de 15 Mbps para o PC 2 (Figura 4.22). Por último, todos os testes foram repetidos, com a alteração do tipo de tráfego entre o PC 3 e PC 2, sendo alterado para tráfego UDP a 15 Mbps (Figura 4.22). Esta velocidade de transmissão foi escolhida de modo a garantir que não se estrangulava a rede, provocando alterações indesejadas no comportamento do tráfego periódico.

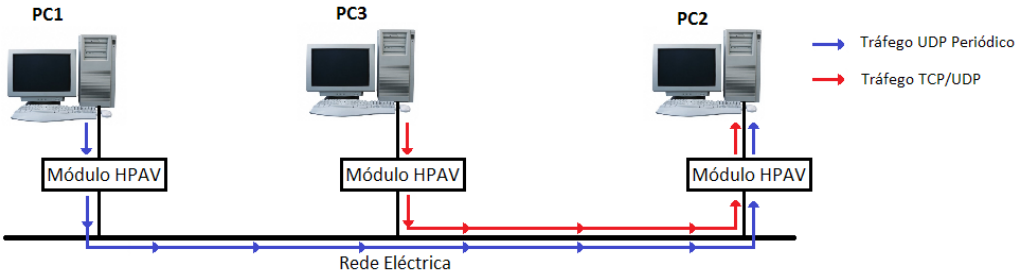

Figura 4.22: Tráfego periódico

Os resultados apresentados seguem a metodologia já descrita para o teste da latência e do jitter.

4.5 Testes adicionais

Diferença entre relógios

Para testar a sincronização dos relógios entre o PC 1 e o PC 2, uma vez que o relógio do PC 3 não influencia em nada os resultados, foi transmitido tráfego ICMP do PC 1 para PC 2. Este tráfego foi capturado pelo *Wireshark* e posteriormente analisado.

Sabendo que, através da utilização do tráfego ICMP, ao ser enviado um pedido por parte do PC 1, vai ser retornada uma resposta por parte do PC 2 (Figura 4.23). Recorrendo à utilização do software *Wireshark*, podemos então obter os valores de t1, t2, t3 e t4.

Obtidos estes valores pode ser calculado o valor do *Round Trip Time* (RTT), independentemente da sincronização dos relógios pela seguinte fórmula:

Figura 4.23: Timestamps para cálculo da diferênca entre relógios

$$R_{tt1} = (t_4 - t_1) - (t_3 - t_2) \tag{4.15}$$

Assumindo que o valor da latência de PC1 para PC2 é o mesmo que de PC2 para PC1, o valor de latência de uma viagem é dado por:

$$Latncia_1 = \frac{R_{tt}}{2} \tag{4.16}$$

Utilizando agora a sincronização entre os relógios o valor da latência dos pacotes de PC1 para PC2 pode ser obtida pela seguinte fórmula:

$$Latncia_2 = (t_2 - t_1) \tag{4.17}$$

Finalmente a diferença entre os relógio pode ser obtida comparando os dois valores da latência.

$$Dif = |Latncia_1 \check{} Latncia_2| \tag{4.18}$$

Tempo de processamento na pilha protocolar

Para medir o tempo decorrido no processamento dos pacotes nas diferentes camadas das pilhas protocolares, utilizou-se como meio físico de transmissão de dados, um cabo *Ethernet* montado em *loopback*, tal como apresentado na Figura 4.24.

Com este tipo de configuração, o pretendido seria que os pacotes enviados através da carta de rede, percorressem o cabo e voltassem a ser recebidos pela mesma carta de rede. Este tipo de configuração, aliada à utilização dos *timestamps* do *wireshark* permitiria calcular os tempos da pilha protocolar.

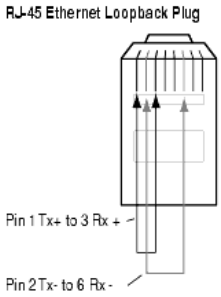

Figura 4.24: Ethernet Loopback [27]

Contudo, após a realização dos testes verificou-se que os pacotes não chegam a ser enviados para o meio físico pela carta de rede, sendo logo encaminhados directamente pelo *loopback* interno do Sistema Operativo. Este efeito impossibilita a captura do pacotes por parte do *Wireshark*, o que inviabiliza toda a experiência.

Capítulo 5

Apresentação e discussão de resultados

Neste capítulo serão apresentados e discutidos os principais resultados obtidos. Estes resultados foram obtidos segundo o plano de testes apresentado no Capítulo 4.

Por forma a obter uma visão geral do comportamento da rede Homeplug, os principais resultados obtidos encontram-se representados na Tabela **??**. Este resultados foram obtidos para as situações de largura de banda máxima e pacotes de 1472 bytes para tráfego genérico, e pacotes de 45 bytes para tráfego de tempo real com um período do 10 ms.

Tabela 5.1: Principais resultados obtidos

	Tráfego genérico					Tráfego de tempo real (10ms)					
	TCP	UDP (1472 bytes)				Isolado		UDP + TCP		UDP + UDP	
	Largura de banda	Largura de banda	Perda pacotes	Latência	Jitter	Latência	Jitter	Latência	Jitter	Latência	Jitter
Cenário 1	94	96	0%	0,148	0,005	0,013	0,005	-	-	-	-
Cenário 2	79	74	30%	3,091	0,045	1,704	0,048	2,927	1,256	1,780	0,850
Cenário 3	83	94	0%	3,092	0,031	1,771	0,059	3,270	1,178	2,106	0,614
Cenário 4	83	93	3%	2,650	0,075	1,757	0,064	2,865	1,241	2,400	0,629
Cenário 5	83	93	2%	3,963	0,025	1,717	0,064	2,448	1,184	2,491	0,612
Cenário 6	83	93	3%	3,597	0,029	1,749	0,051	2,160	1,195	1,892	0,604
Cenário 7	83	93	3%	3,597	0,045	1,698	0,066	2,901	1,120	2,014	0,824
Cenário 8	83	93	3%	3,150	0,027	1,691	0,070	2,444	1,010	1,902	0,639

Todos os resultados serão ainda apresentados e discutidos nas secções seguintes.

5.1 Tráfego não periódico

5.1.1 TCP

Largura de banda

O primeiro teste realizado foi a medição da largura de banda disponível para transporte de tráfego TCP. Esta medição foi efectuada em 3 cenários distintos: cenário 1 - ligação *Ethernet* ponto a ponto (100 Mbps), cenário 2 - ligação com módulos *Homeplug* na rede eléctrica do laboratório e cenário 3 - ligação com módulos *HomePlug* na rede eléctrica isolada.

Como se verifica na Figura 5.1, este teste pode ser visto como a medida de uma grandeza que tende para um regime estacionário, mas com um período inicial, em regime transitório. Para eliminação deste efeito os 5 primeiros segundos foram descartados, tal como referido na subsecção 4.4.1.

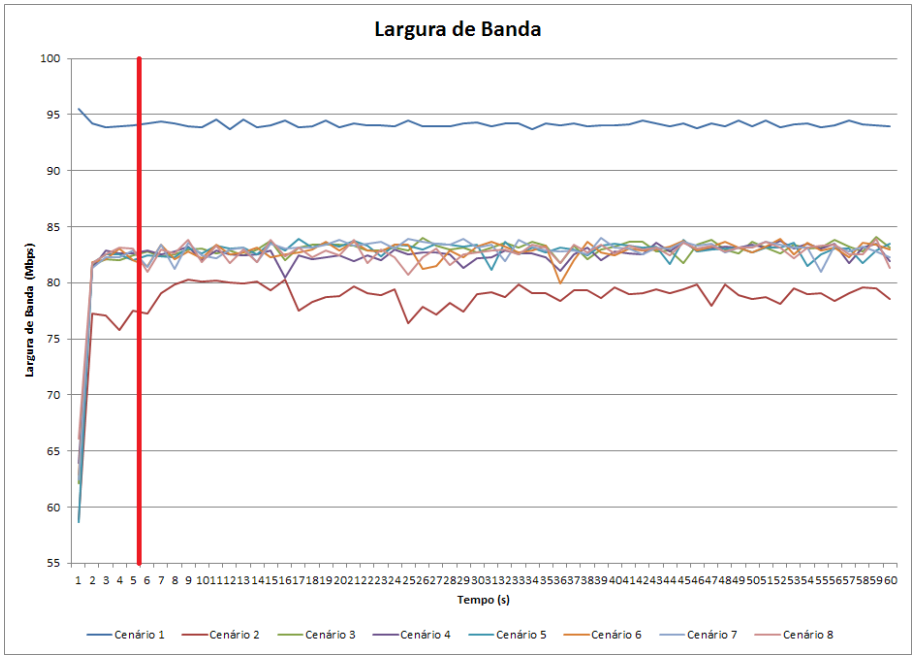

Figura 5.1: Largura de banda em função do tempo, para TCP Window Size = 256 KBytes

Na Figura 5.2, pode-se verificar que os valores obtidos para a ligação na rede isolada são ligeiramente superiores aos obtidos na rede do laboratório, o que corresponde ao previsto, uma vez que a rede isolada encontra-se limpa de interferências externas. Por outro lado os valores obtidos para a rede *Ethernet* são também superiores aos obtidos com a rede *Homeplug* confirmando assim o esperado, uma vez que o tráfego na rede *Homeplug* tem que ser processado por dois interfaces adicionais. Verifica-se ainda que os restantes equipamentos conectados à rede eléctrica isolada não provocaram alterações significativas na largura de banda máxima atingida.

Para diferentes valores do *TCP Window Size* verifica-se que o valor da largura de banda baixa com a diminuição do *Window Size*, o que está de acordo com o esperado, uma vez que este valor define o número de pacotes que podem ser transmitidos sem ter sido recebida a respectiva confirmação.

Denota-se também que esta variação é bastante acentuada aquando da utilização do protocolo *Homeplug*, mas pelo contrário é bastante ligeira aquando da utilização da rede *Ethernet*. Esta diferença é justificada devido às diferenças dos tempos de latência entre as duas redes. Como os

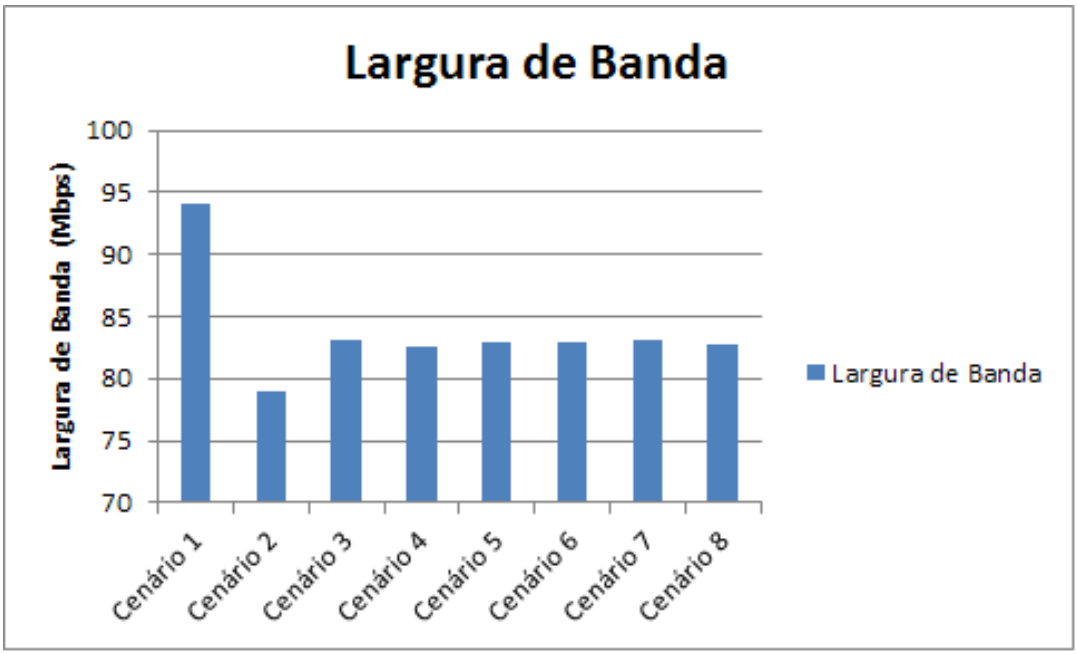

Figura 5.2: Valor médio da Largura de Banda máxima atingida em cada um dos cenários

tempos da rede *Homeplug* são superiores, implica um elevado aumento no tempo de espera pelas mensagens de confirmação dos pacotes enviados e quantas mais confirmações forem necessárias, maior este tempo, o que provoca uma diminuição drástica na largura de banda máxima disponível.

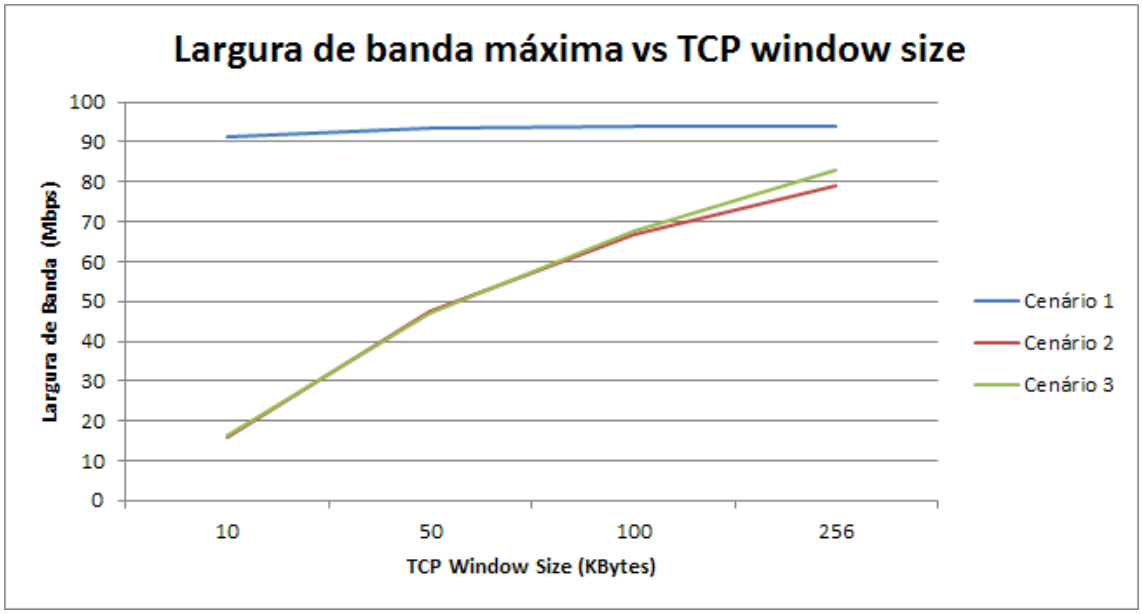

Figura 5.3: Largura de banda máxima em função da TCP Window Size

5.1.2 UDP

Largura de banda

Para o tráfego UDP, mediu-se também a largura de banda útil máxima, para pacotes de diferentes tamanhos, bem como o seu valor médio para pacotes com 1472 bytes nos diversos cenários (Figura 5.6), pois é com este valor que se consegue atingir uma largura de banda máxima (Figura 5.4). Tal como referido anteriormente, a largura de banda tende para um regime estacionário, por esse facto considerou-se novamente um período de regime transitório inicial de 5 segundos, que foi posteriormente eliminado nos restantes cálculos (Figura 5.5).

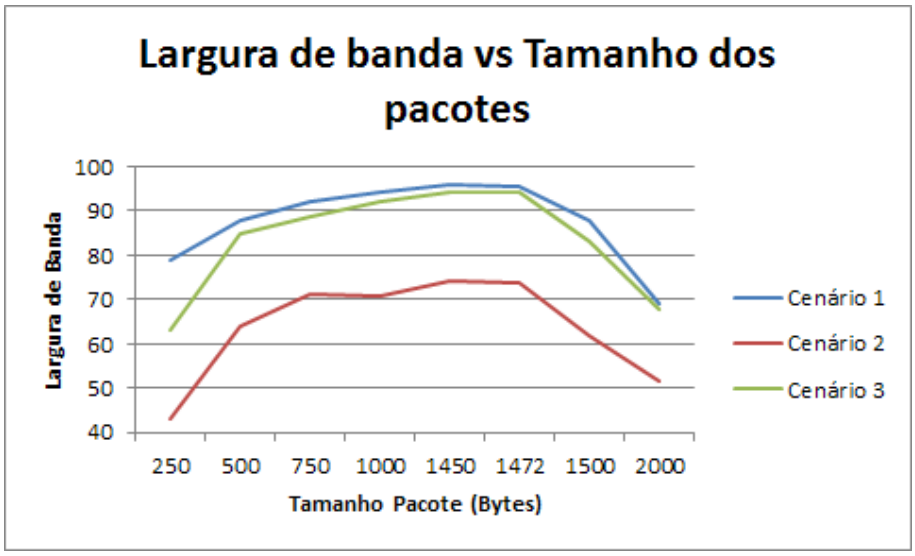

Figura 5.4: Largura de banda máxima em função do tamanho dos pacotes

Tal como previsto, a largura de banda máxima é obtida aquando da utilização de pacotes UDP com o tamanho de 1472 Bytes, que corresponde na totalidade a um pacote IP de 1500 Bytes. Caso seja utilizado um valor inferior para o tamanho dos pacotes, perde-se largura de banda, devido à não utilização da capacidade máxima de cada pacote para transferência de informação. Este impacto na largura de banda não é significativo até ao tamanho de 750 bytes, sendo mais acentuado para pacotes com tamanho inferior. Este decréscimo é aproximadamente igual para os 3 cenários apresentados, obtendo-se sempre taxas superiores no cenário 1, seguidas do cenário 3.

Caso se utilizem pacotes de tamanho superior a 1472 Bytes, torna-se necessária a sua fragmentação, o que provoca um aumento do número de pacotes na rede e consequentemente uma diminuição na largura de banda útil. Os valores obtidos para a largura de banda baixaram para cerca de 70% , para pacotes com 2000 bytes, em relação valor máximo obtido (pacotes com 1472 bytes). Esta situação ocorreu nos 3 tipos de rede utilizados.

Para além da variação no valor médio da largura de banda, verifica-se que para ambientes mais ruidosos a variação deste ao longo do tempo é maior. Esta situação deve-se principalmente ao facto das alterações das condições do meio de transmissão e consequente ajuste das bandas subportadoras a utilizar.

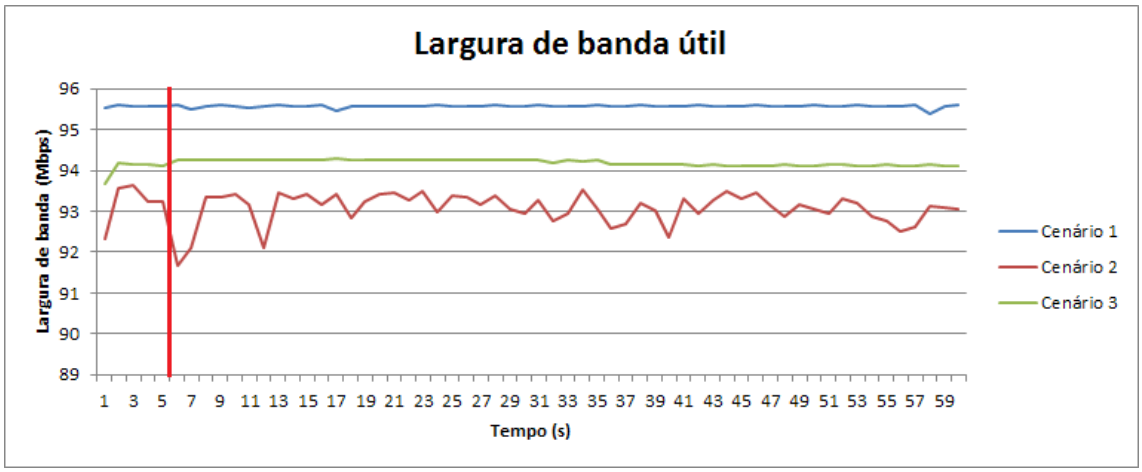

Figura 5.5: Largura de banda máxima em função do tempo, para pacotes com 1472 Bytes

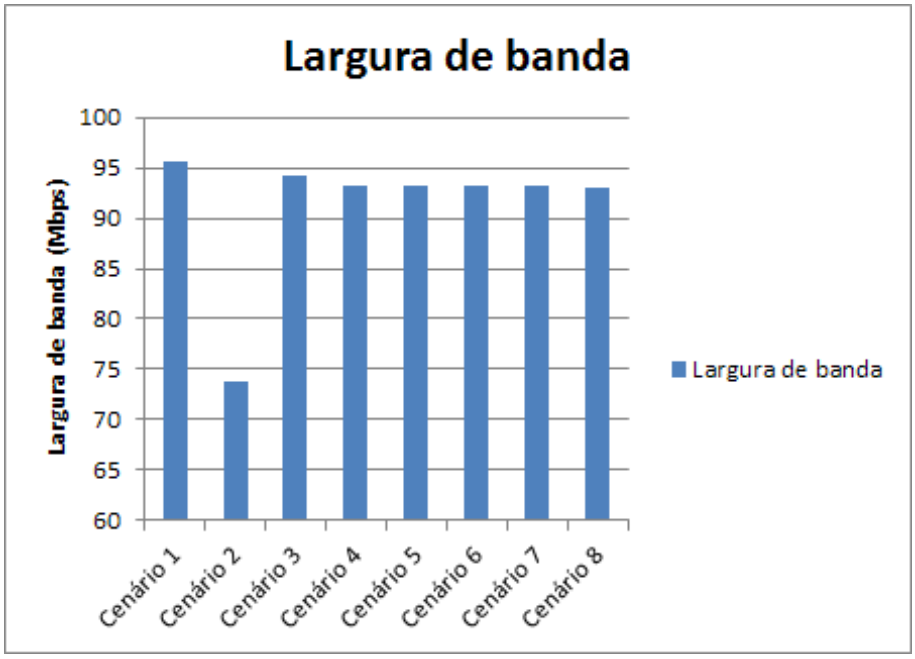

Figura 5.6: Valor médio da Largura de Banda máxima atingida em cada um dos cenários

Como se verifica na Figura 5.6, a largura de banda diminui com a introdução de equipamentos conectados na mesma rede que os módulos *Homeplug*. Apesar de esta diminuição ser apenas de no máximo 2 Mbps, para os equipamentos de teste, o mesmo não acontece no cenário 2, onde há uma queda de cerca de 20 Mbps. Esta diferença de desempenho pode ser devida aos vários tipos de equipamentos conectados à rede do laboratório, sobre os quais não há controlo.

Outro aspecto de salientar é o aumento da largura de banda em relação ao tráfego TCP, e consequente diminuição da diferença entre a rede *Ethernet* e a rede *Homeplug*. Este aumento da largura de banda deve-se à não existência de pacotes de confirmação para tráfego UDP, ou seja, a

comunicação é unidireccional.

Pacotes perdidos

A medição da taxa de pacotes perdidos por segundo numa transferência foi efectuada em conjunto com a medição da largura de banda disponível para tráfego UDP, como descrito no Capítulo 4.

Inicialmente os testes foram efectuados com pacotes de diferentes tamanhos e a diferentes taxas de transmissão, para os cenários 1, 2 e 3 e verificou-se que independentemente do tamanho dos pacotes, só existem perdas quando se transmite à velocidade máxima permitida pela rede (Figura 5.7). Este era um resultado já espectável, uma vez que a perda de pacotes ocorre devido à saturação do meio de transmissão, e a um possível esgotamento do buffer dos módulos HPAV, pois não foram incorporados quaisquer equipamentos adicionais, a não ser as cartas de rede e os módulos *Homeplug*, o que elimina a possibilidade dos *buffers* de equipamentos de rede como *switches* ou *routers* serem demasiado reduzidos, e esgotarem a sua capacidade rapidamente.

Posto isto, apenas os testes com pacotes de diferentes tamanhos, mas à velocidade máxima de transmissão foram efectuados em todos os cenários (Figura 5.8).

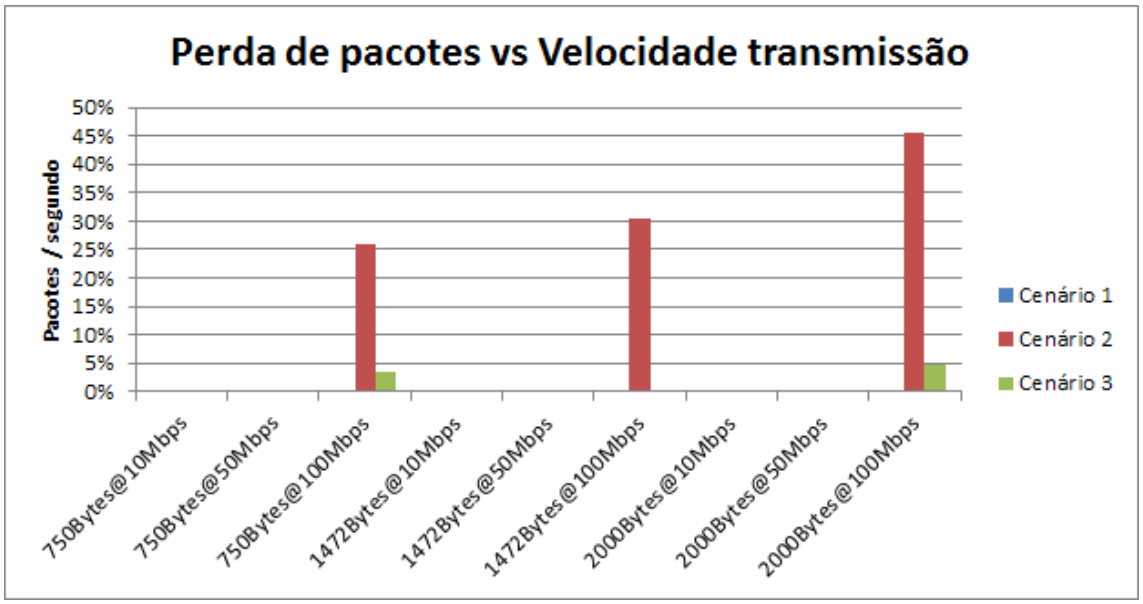

Figura 5.7: Percentagem de pacotes perdidos por segundo

Como se verifica, a taxa de perda de pacotes nos testes realizados com a rede *Ethernet* ponto a ponto foi residual, já o mesmo não aconteceu com a rede *Homeplug*, principalmente na rede do laboratório onde a perda de pacotes foi sempre superior a 25% dos pacotes transmitidos por segundo. Este fenómeno é provocado pela insuficiência da largura de banda útil do meio para transmitir a informação à taxa a que esta é gerada. Como se verificou anteriormente, o valor máximo da largura de banda útil obtido para Cenário 2, foi de 74 Mbps, valor este que é bastante

inferior aos 100 Mbps de taxa de produção de informação. Esta diferença implica que hajam pacotes que são descartados.

Considerando a taxa de perda de pacotes com 1472 bytes como referência, verifica-se que diminuindo o tamanho dos pacotes para metade existe um aumento do número de pacotes perdidos para aproximadamente o dobro, já para pacotes com 2000 bytes a diferença é diminuta, ocorrendo em alguns casos a diminuição do número de pacotes perdidos por segundo.

Em termos percentuais, a análise do número de pacotes perdidos pode ser efectuada, tendo em conta a largura de banda máxima obtida anteriormente e o respectivo tamanho dos pacotes como se segue:

$$\frac{PacotesTransmitidos}{Segundo} = \frac{LarguraBanda}{TamanhoPacote} \tag{5.1}$$

$$\frac{PercentagemPacotesPerdidos}{Segundo} = \frac{PacotesPerdidos}{PacotesTransmitidos} \tag{5.2}$$

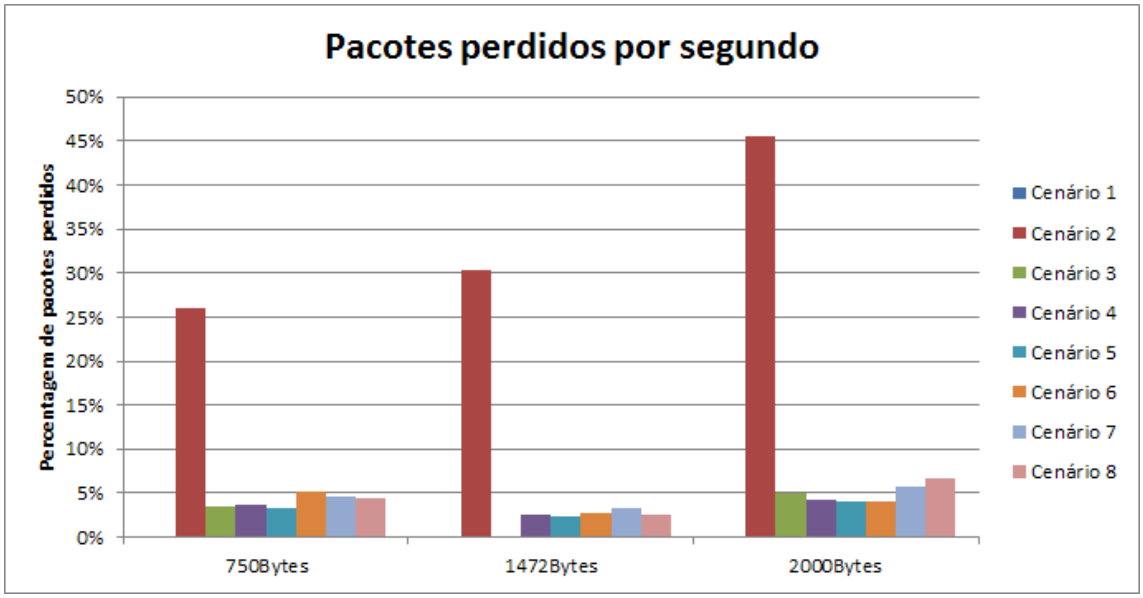

Figura 5.8: Percentagem de pacotes perdidos por segundo, em cada um dos cenários

Como se verifica na Figura 5.8, a percentagem de pacotes perdidos por segundo tende a diminuir com o aumento do tamanho dos pacotes, desde que não exista fragmentação. Este facto deve-se principalmente à diminuição do número de pacotes transmitidos, para a mesma quantidade de informação.

Latência

Tal como descrito no Capítulo 4, a latência foi medida para um conjunto de 10000 pacotes de diferentes tamanhos, transmitidos a 10 Mbps, 50 Mbps e 100 Mbps. De notar que para pacotes com 45 bytes, apenas são apresentados os resultados para uma taxa de transmissão de 10 Mbps, devido à taxa de amostragem do *Wireshark*, que no caso de velocidades superiores para este tipo de pacotes, não é suficiente para amostrar todos os pacotes transmitidos, o que inviabiliza o sucesso do teste e consequente obtenção de medidas.

Na Figura 5.9 é apresentado o valor da latência em função do número do pacote transmitido, para os cenários 1, 2 e 3, para pacotes de 1472 bytes e à taxa de transmissão máxima, 100 Mbps.

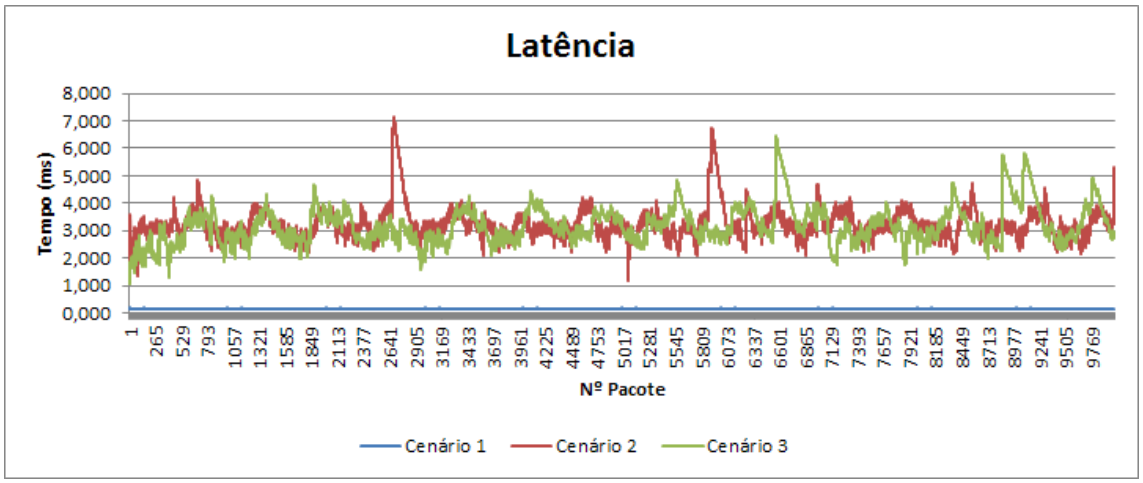

Figura 5.9: Valor da Latência em função do número do pacote

Como se pode verificar, o valor da latência das redes *Homeplug* é bastante superior ao valor da rede *Ethernet*.

O valor obtido para a rede *Ethernet*, com uma média de 0,148 milissegundos, pode ser confirmado através de cálculos teóricos, como se apresenta:

Tamanho pacote UDP = 1472 bytes => Tamanho pacote IP = 15000 bytes => 12000 bits

O valor da latência pode ser obtido segundo a seguinte expressão:

$$Latncia = \frac{n^o bits}{throughput} \tag{5.3}$$

Assumindo que na rede *Ethernet* toda a largura de banda é utilizada para transporte de dados obtemos o seguinte:

$$Latncia = \frac{12000}{100000000} = 0,120ms \tag{5.4}$$

Valor este, que difere em 28 microsegundos do valor prático obtido, o que comprova uma boa qualidade dos resultados obtidos.

De salientar ainda que o valor obtido para a latência, ao contrário das medidas anteriores não é afectado de uma forma significativa pelo tipo e número de equipamentos conectados na mesma rede que os equipamentos *Homeplug*, pois como se verifica na Figura 5.10, o valor e comportamento da latência matêm-se bastante semelhantes, quer para o cenário 2, quer para o cenário 3, tendo sido obtidos valores médios na ordem dos 3 milisegundos, para ambos os cenários.

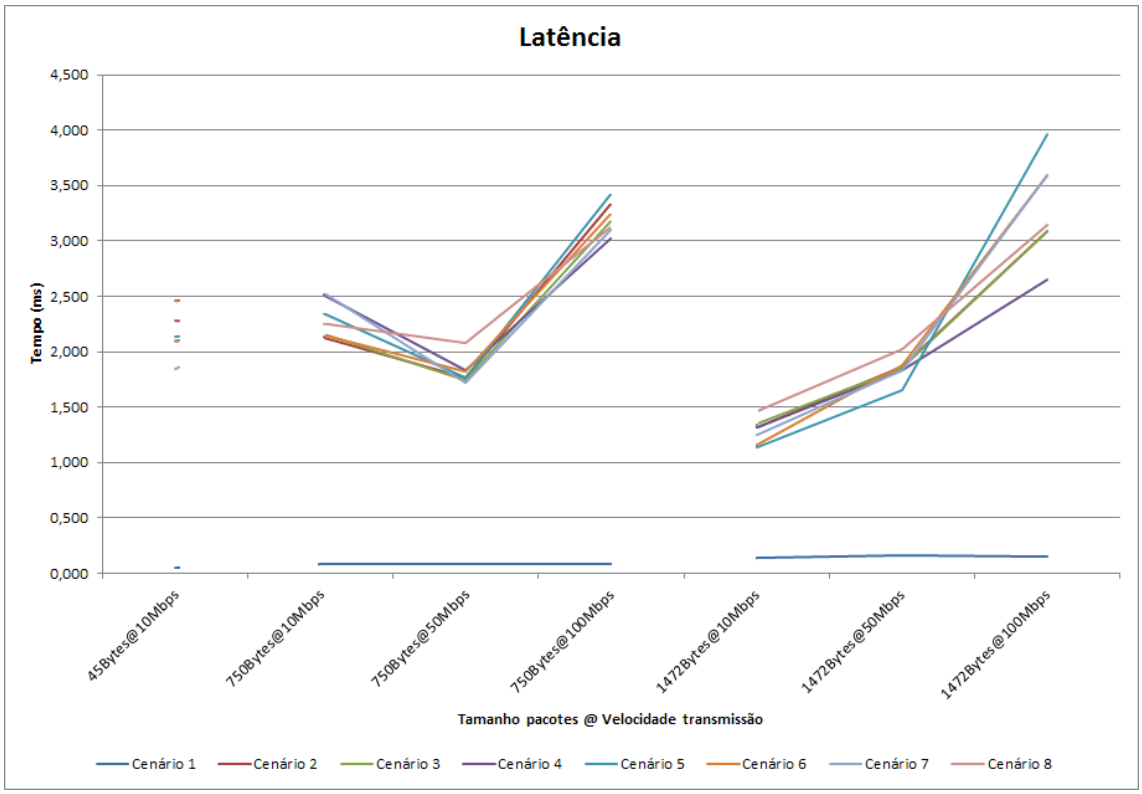

Figura 5.10: Valor médio da Latência em função do tamanho e da velocidade de transmissão, para os diferentes cenários

Na Figura 5.10 são apresentados os resultados obtidos para a diferentes topologias de rede utilizadas, bem como para diferentes tamanhos de pacotes e velocidade de transmissão.

Como seria de esperar os valores de latência obtidos para pacotes de tamanhos superiores são, na generalidade mais elevados, pois como se demonstrou anteriormente o valor aproximado da latência só depende do tamanho do pacote e da velocidade de transmissão. Por outro lado, e contrariando esta teoria, verifica-se que na rede *Homeplug* o valor da latência tende a diminuir com a diminuição da taxa de transmissão dos dados, tendo-se atingido os valores máximos desta, sempre à velocidade máxima de transmissão. Este facto deve-se principalmente ao mecanismo de modulação dos dados nas frequências portadoras e ao aumento do número de pacotes na rede e consequente aproximação do ponto de saturação da rede.

Da Figura 5.10 pode-se ainda majorar os limites superior e inferior para a latência dos pacotes UDP de uma rede *Homeplug* AV, como sendo 4.5 ms e 1 ms , respectivamente.

De salientar ainda o facto de que estes valores apenas reportam os atrasos introduzidos pelos módulos *Homeplug* e pela própria infra-estrutura física da rede, uma vez que não são considerados os atrasos decorridos da pilha protocolar, como explicado no Capítulo 4.

Jitter

O valor do Jitter foi calculado em conjunto com o cálculo do valor da latência. Uma vez que, à semelhança do teste anterior, são utilizados os timestamps introduzidos pelo *Wireshark* para o cálculo da grandeza pretendida, segundo a seguinte fórmula:

$$jitter(ms) = (t3 - t1) - (t4 - t2) \tag{5.5}$$

Sendo t1= *timestamp* envio do pacote1; t2= *timestamp* recepção pacote1; t3=*timestamp* envio pacote2; t4= *timestamp* recepção pacote2.

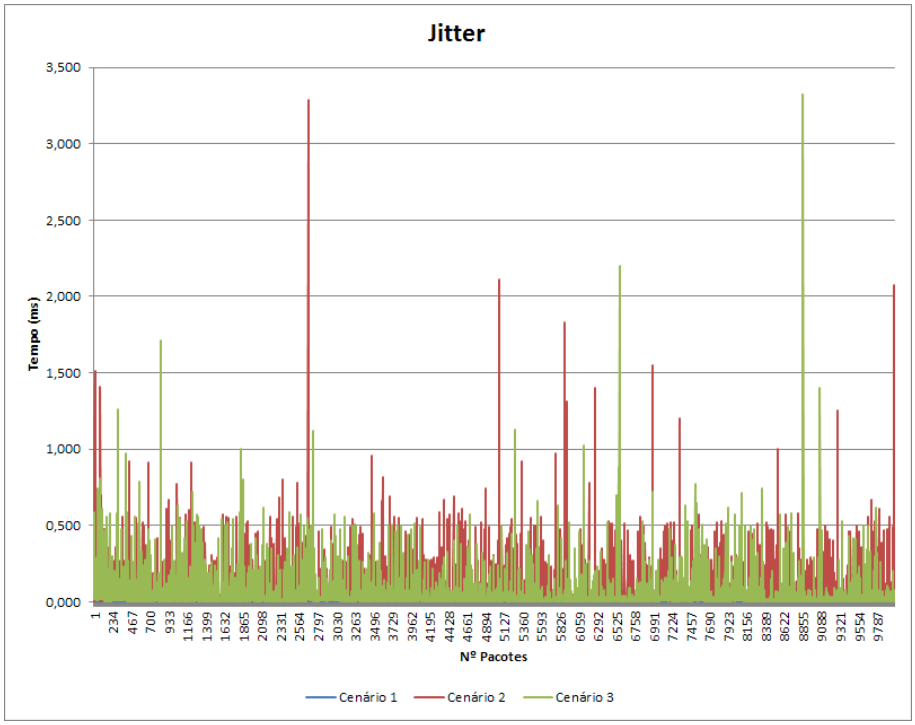

Figura 5.11: Valor do jitter em função do número do pacote

O valor do Jitter em função do número do pacote transmitido é apresentado na Figura 5.11, e como se pode constatar o seu valor para redes *Ethernet* ponto a ponto é bastante diminuto, quando comparado com o obtido para redes *Homeplug AV*. Este valor pode ser justificado pela constante alteração no meio de transmissão, e consequente ajuste das sub-bandas portadoras, o que provoca

alterações no tempo de entrega dos pacotes. Da Figura 5.11, verifica-se ainda que o valor do Jitter é influenciado pelas cargas conectadas na rede eléctrica. Esta influência é traduzida essencialmente na frequência da ocorrência de picos de valor elevado do Jitter, que se devem principalmente à razão apresentada anteriormente.

Estes valores do Jitter podem ser confirmados através do histograma abaixo, Figura 5.12 que representa a frequência dos valores de latência para pacotes de 1472 bytes, a uma taxa de transmissão de 100 Mbps, nos cenários 2 e 3. Como se verifica, os valores obtidos durante os testes da rede no cenário 2, apresentam uma maior frequência para valores mais distantes da média, o que indica à partida, um valor do Jitter mais elevado, tal como apresentado anteriormente.

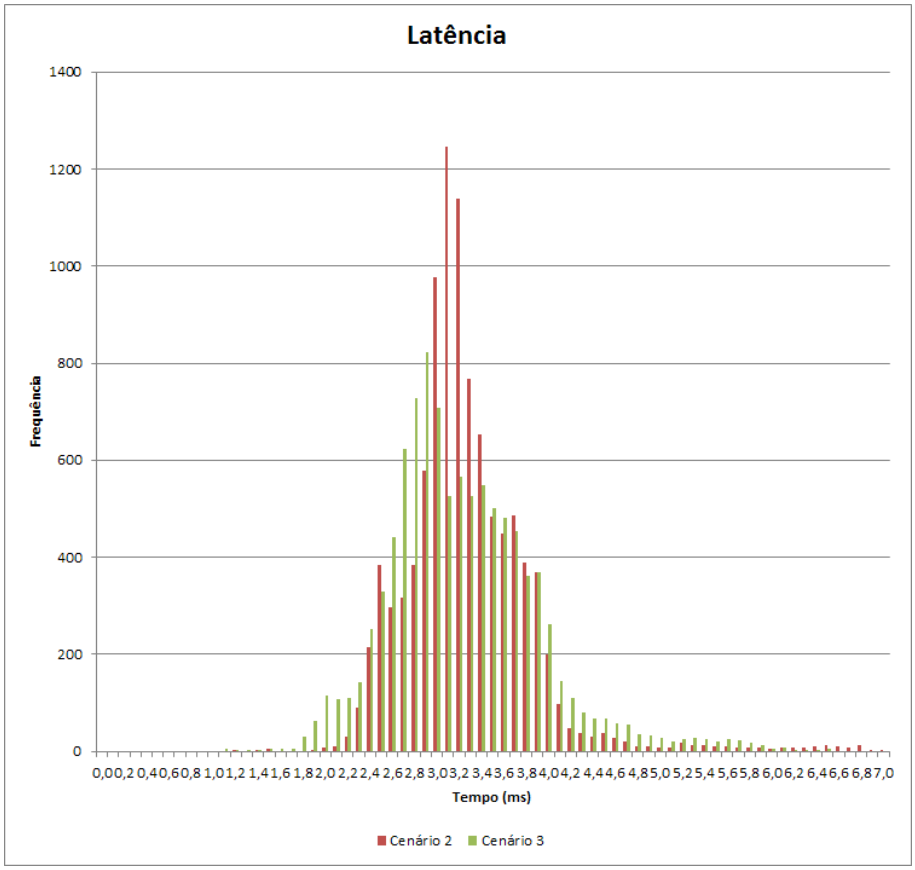

Figura 5.12: Histograma dos valores da latência para os cenários 2 e 3

Na Figura 5.13, são apresentados os valores obtidos para diferentes tamanhos de pacotes e diferentes taxas de transmissão.

Analisando a Figura 5.13 conclui-se que o valor do Jitter tende a diminuir com o aumento da taxa de transmissão, independentemente do tamanho dos pacotes transmitidos. Por outro lado, e à semelhança da latência, verifica-se que o valor do Jitter não é significativamente influenciado pelas cargas conectadas na rede eléctrica. De notar que os valores anteriores contêm um erro de +/- 0.1 ms, devido à sincronização entre relógios.

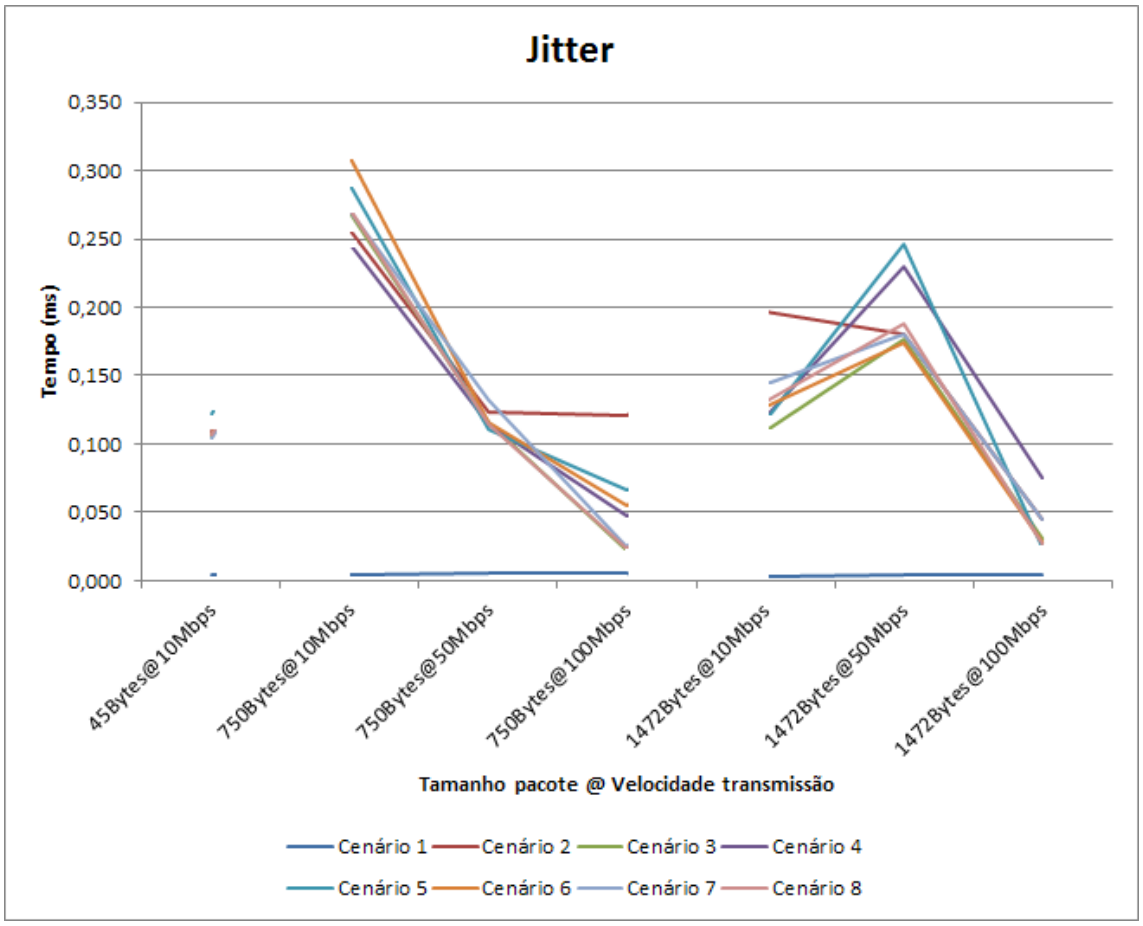

Figura 5.13: Valor médio do Jitter em função do tamanho e da velocidade de transmissão, para os diferentes cenários

5.2 Tráfego periódico

Os testes anteriormente efectuados para obtenção do valor da latência e do jitter, foram repetidos, mas agora com tráfego UDP periódico, com 45 bytes de tamanho, por forma a simular o mais possível o tipo de tráfego utilizado em aplicações industriais. A metodologia utilizada na realização destes testes encontra-se descrita no Capítulo 4.

5.2.1 Tráfego UDP periódico

Latência

Na Figura 5.14 são apresentados os valores médios da latência obtidos para os diferentes cenários, e para diferentes períodos de transmissão de pacotes UDP com 45 Bytes, nomeadamente 100 ms, 50 ms, 10 ms e 1 ms.

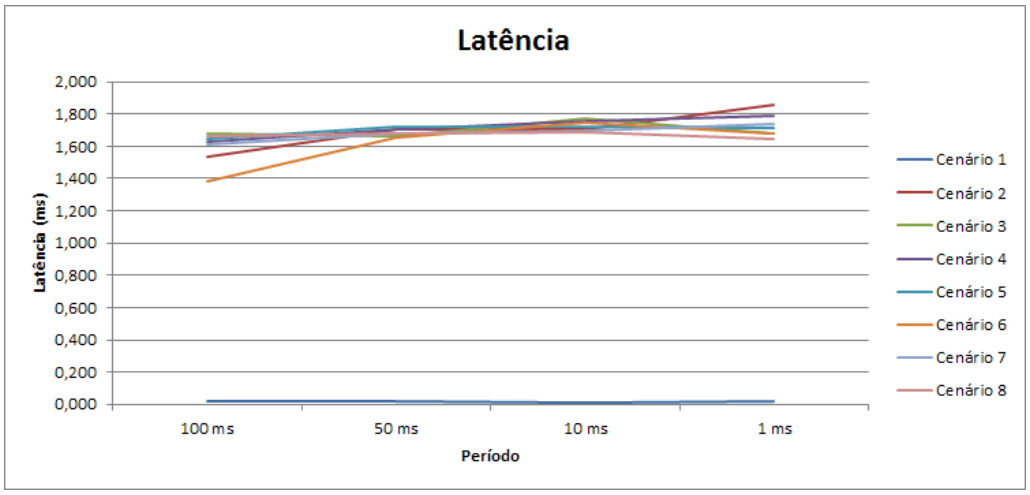

Figura 5.14: Valor médio da latência em função do período de transmissão, para os diferentes cenários

Como se verifica na Figura 5.14, os valores da latência mantêm-se praticamente inalterados para os diferentes tempos entre pacotes, existindo contudo um ligeiro aumento deste tempo com a diminuição do período de transferência. Este facto é provocado pelo aumento da taxa de transferência de dados, e consequente aumento do número de pacotes em simultâneo na rede.

Jitter

Para a situação em que apenas se transmitiu tráfego UDP periódico, verifica-se na Figura 5.15, que este valor se mantém constante e próximo dos 0.1 ms aumentando substancialmente para tráfego com um período de 1 ms. Este fenómeno repete-se em todos os cenários implementados, à excepção do cenário 1, onde o valor se mantém constante e próximo de 0.05 ms.

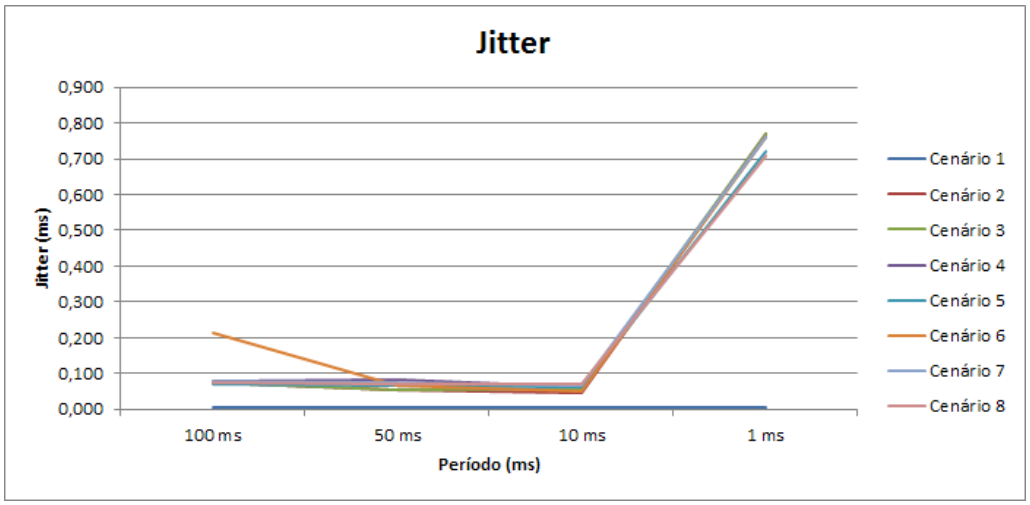

Figura 5.15: Valor médio do jitter em função do período de transmissão, para os diferente cenários

5.2.2 Tráfego UDP periódico em conjunto com TCP aperiódico

Latência

Após realizados os testes com tráfego UDP periódico isolado, foi adicionada à rede uma terceira estação (PC3), a transmitir tráfego TCP à taxa de 15 Mbps para o PC1. Este teste tem como objectivo avaliar o desempenho da rede aquando da existência de tráfego adicional, que não aquele que se pretende medir.

O ideal para a realização destes testes, seria a utilização de quatro estações, duas para tráfego tempo real e outras duas para tráfego genérico. Contudo, e devido a limitações de *hardware* esta situação não foi possível. No entanto, este facto não invalida os resultados das experiências, pois existe exclusividade no acesso ao meio.

Os resultados encontram-se representados na Figura 5.16.

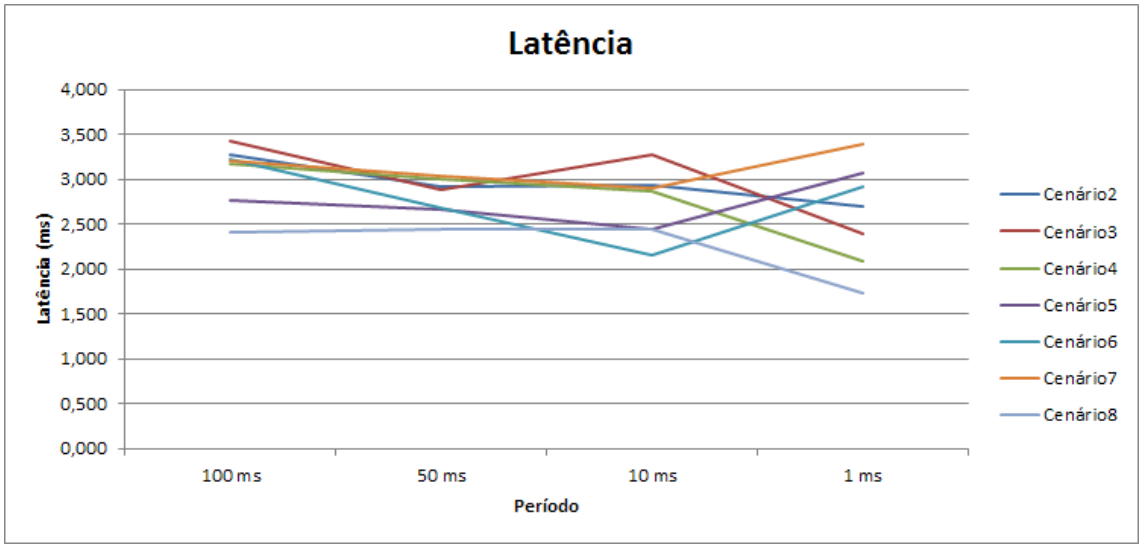

Figura 5.16: Valor médio da latência em função do período de transmissão, para os diferentes cenários

Para a transferência de tráfego UDP periódico em conjunto com tráfego TCP, verificou-se um acréscimo nos tempos de latência para aproximadamente o dobro, quando comparados com os tempos obtidos para tráfego de apenas pacotes UDP periódicos. Este era um resultado espectável, pois o tráfego de dados na rede foi substancialmente aumentado. Para além deste aumento no tráfego, existiu ainda o acréscimo de uma nova estação PLC a partilhar o mesmo meio de comunicações. Esta situação implica que sejam utilizados os mecanismo CSMA/CA previstos para acesso ao meio, uma vez que nenhum dos tráfegos foi definido como prioritário. Como o mecanismo de acesso ao meio CSMA/CA é não determinístico ocorre um aumento nos valores da latência e do jitter, tal como apresentado a seguir.

Jitter

Para o tráfego UDP periódico, em conjunto com tráfego TCP, pode-se confirmar na Figura 5.17 que o valor do Jitter tende a diminuir ligeiramente com a diminuição do período entre pacotes UDP. Verifica-se ainda que o seu valor não é directamente afectado pelos equipamentos conectados na rede e que para todos os períodos considerados o seu valor é bastante superior ao obtido com o tráfego UDP isolado.

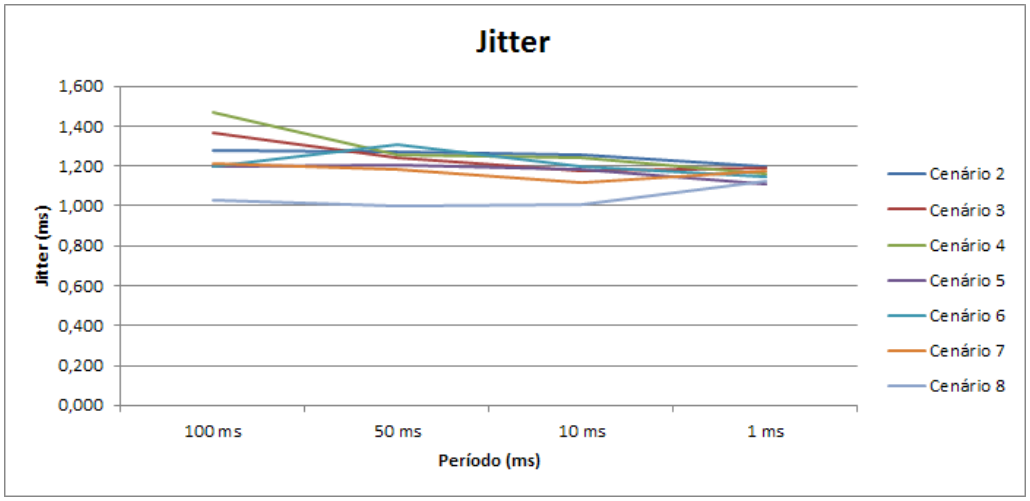

Figura 5.17: Valor médio do jitter em função do período de transmissão, para os diferente cenários

5.2.3 Tráfego UDP periódico em conjunto com UDP aperiódico

Latência

Os testes anteriores foram repetidos, mas com a alteração do tipo de tráfego gerado pelo PC3, que passou a ser tráfego UDP com 1472 Bytes a uma taxa de transmissão de 15 Mbps. Os resultados obtidos são apresentados na Figura5.18.

Novamente, verifica-se que os valores obtidos são pouco influenciados pelo período de transmissão dos pacotes e mantêm-se aproximadamente constantes nos diferentes cenários de teste, tal como verificado anteriormente.

Analisando as Figuras 5.14, 5.16 e 5.18 verifica-se ainda que o tempo de latência obtido para o tráfego de pacotes periódicos UDP em conjunto com tráfego UDP aperiódico é superior ao obtido aquando do tráfego periódico isolado, mas inferior ao tráfego periódico em conjunto com o tráfego TCP. Este facto pode ser explicado, tal como referido anteriormente, pela necessidade de concorrência pelo meio de comunicações entre estações. Contudo os valores obtidos para a situação em que foi introduzido tráfego TCP foram superiores, devido à existência de retransmissões e mensagens confirmação, o que tende a aumentar o número de colisões e consequentes retransmissões.

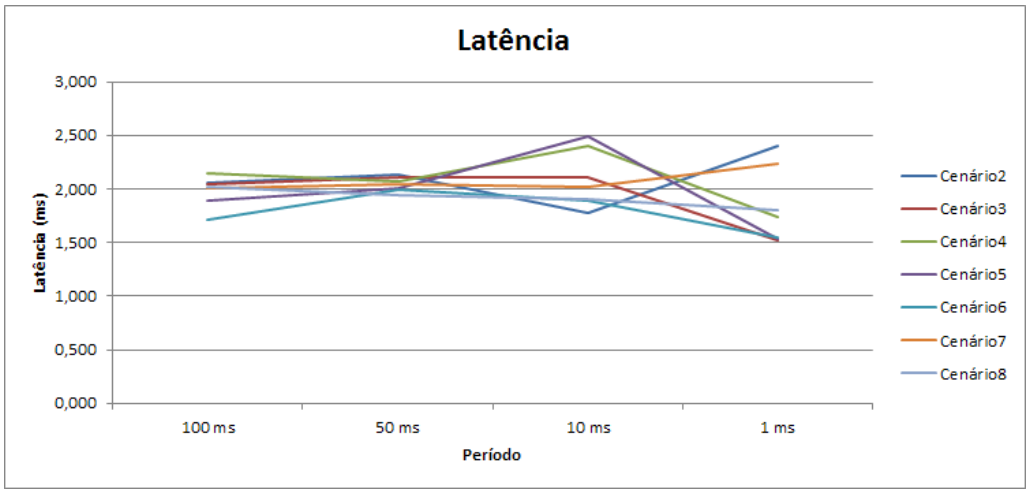

Figura 5.18: Valor médio da latência em função do período de transmissão, para os diferente cenários

Jitter

No tráfego UDP periódico, em conjunto com UDP aperiódico verifica-se que o valor do Jitter diminui consideravelmente em relação aos valores obtidos para os testes com tráfego UDP periódico em conjunto com tráfego TCP.

Confirma-se ainda que ao contrário do teste anterior, neste caso, o valor do Jitter diminui com a diminuição do período de transferência de 100 ms para 50 ms, mas volta a sofrer um aumento aquando da diminuição do período de transferência para 10 ms e 1 ms.

Novamente, os valores obtidos para este teste são bastante inferiores aos obtidos para os testes com tráfego TCP. Esta situação, deve-se essencialmente à não existência de tráfego bidireccional e consequente diminuição do número de colisões no tráfego UDP.

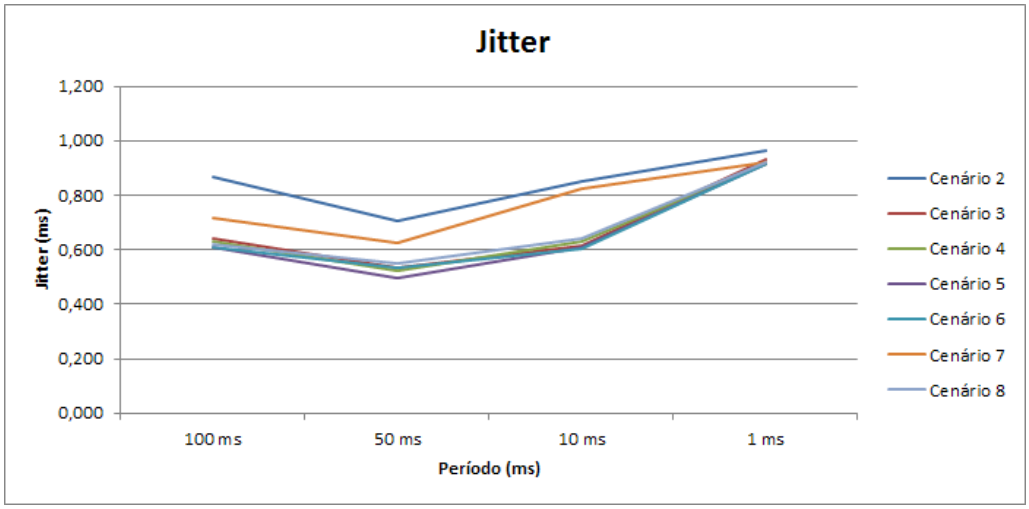

Figura 5.19: Valor médio do jitter em função do período de transmissão, para os diferentes cenários

5.3 Diferença entre relógios

Para a medição e verificação da precisão da sincronização entre os dois relógios, foram utilizados pacotes ICMP, pois estes permitem o envio e obtenção da consequente resposta. Na Figura 5.20, está representada a diferença entre os relógios ao longo do tempo para os cenários 1, 2 e 3.

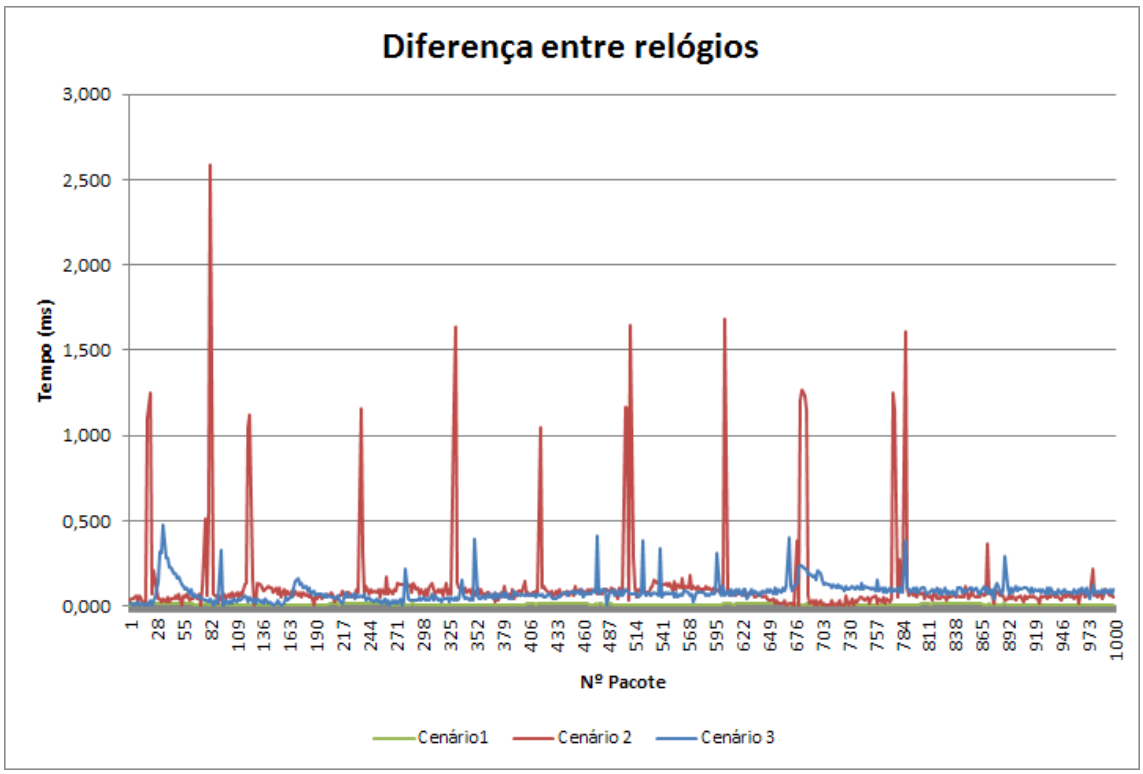

Figura 5.20: Diferença entre relógios, em função do tempo

Como podemos observar, na Figura 5.20, a sincronização entre relógios foi obtida com uma precisão bastante boa, na ordem dos 0.1 milisegundos para redes *Homeplug*, apresentando um valor ainda mais preciso para a rede *Ethernet* ponto a ponto. Esta diferença deve-se principalmente ao facto da existência de um aumento da latência entre os pacotes enviados nas redes *Homeplug* e na rede *Ethernet*. Observa-se ainda que no Cenário 2 existem picos de discrepância entre os relógios, que atingem um máximo de 2.6 milisegundos. Este valor deve-se ao facto da existência de um maior número de interferências neste tipo de ligação, e consequente maior número de pacotes perdidos, o que influencia negativamente o funcionamento do método de sincronização utilizado. Apesar destes picos de discrepância o valor médio foi considerado suficientemente preciso para ser utilizado no decorrer dos restantes testes.

5.4 Análise da rede eléctrica

De modo a confirmar o correcto desempenho do *TestBed* implementada no decorrer dos trabalhos, foi ainda efectuado como teste complementar, a análise espectral da rede eléctrica. Os cenários utilizados para esta análise foram o Cenário 2 e o Cenário 3.

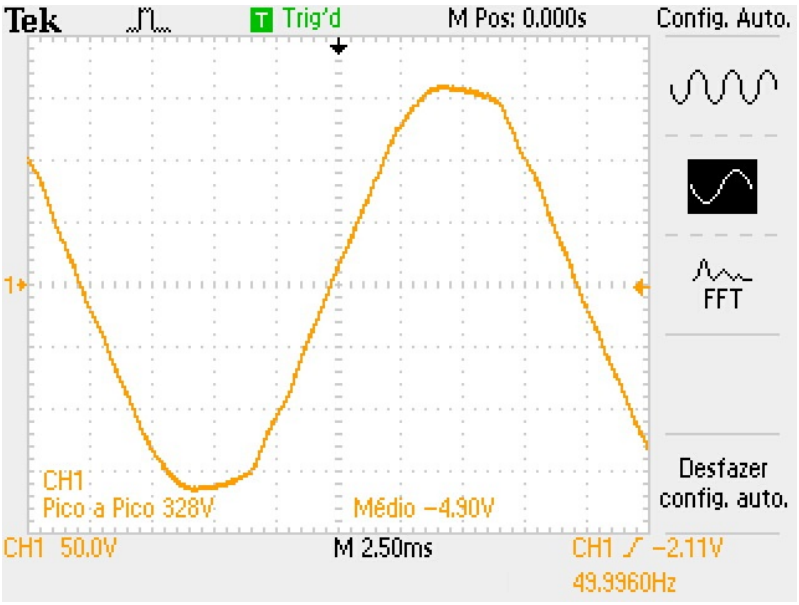

Figura 5.21: Forma de onda da rede eléctrica do laboratório

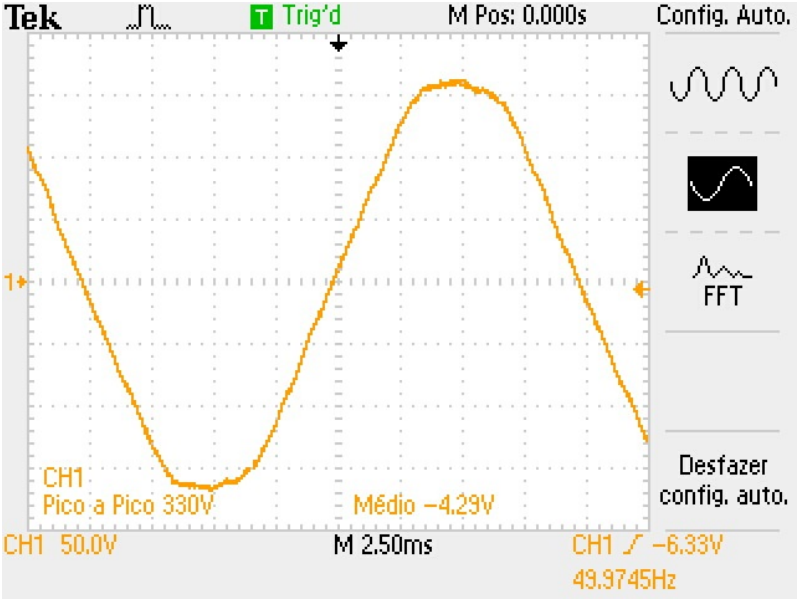

Figura 5.22: Forma de onda da rede eléctrica da TestBed

Como se verifica pela forma de onda da tensão sinusoidal presente tanto na rede eléctrica do

laboratório (Figura 5.21), como no troço de rede eléctrica isolada (Figura 5.22), esta sofre uma deformação provocada pelas interferências causas pelos equipamentos conectados à rede. Como seria de esperar, esta deformação é mais acentuada para o Cenário 2, do que para o Cenário 3, onde existe um isolamento e filtragem de interferências externas.

Para além das formas de onda, são ainda apresentados nas figuras seguintes, os componentes harmónicos presentes em cada um dos cenários. Estes componentes foram obtidos tanto para baixas frequências (Figura 5.23 e Figura 5.24), como para altas frequências (Figura 5.25 e Figura 5.26)

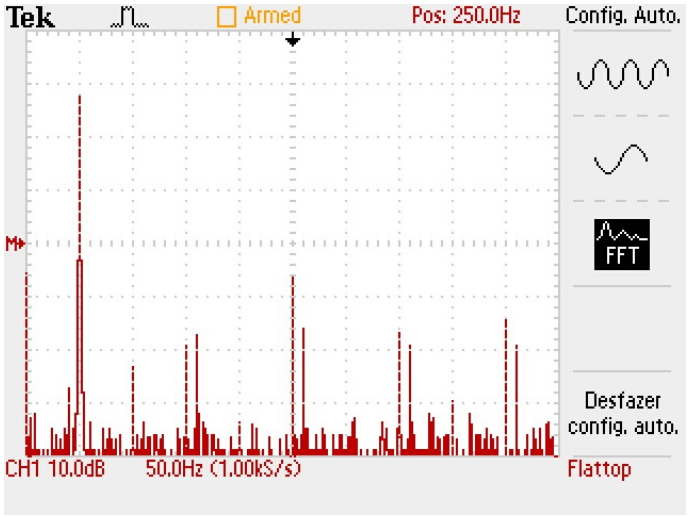

Figura 5.23: Análise espectral para baixas frequências na rede eléctrica do laboratório

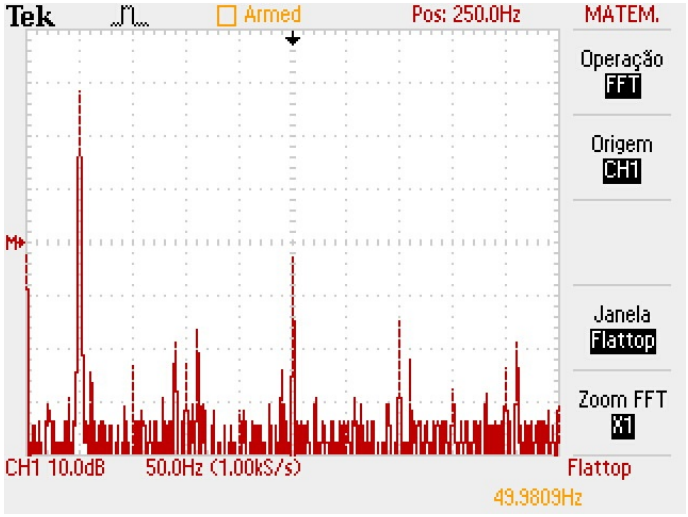

Figura 5.24: Análise espectral para baixas frequências na rede eléctrica da TestBed

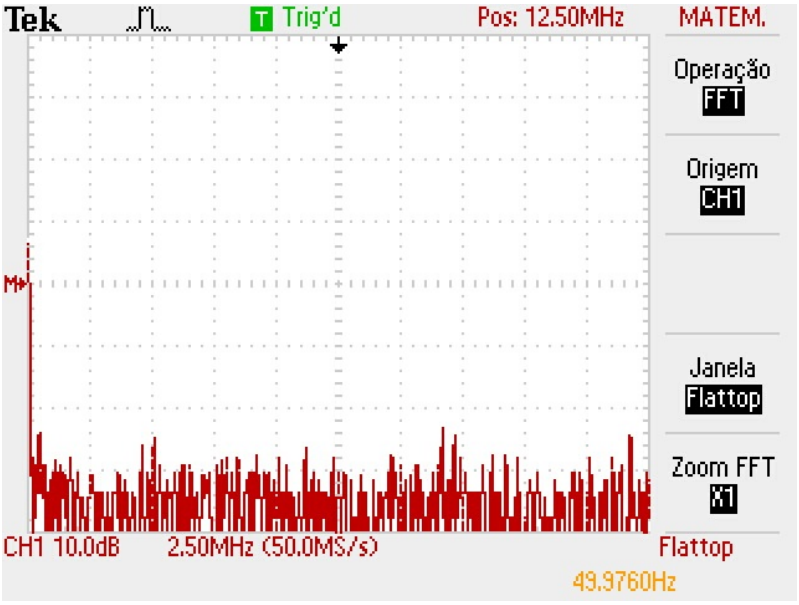

Figura 5.25: Análise espectral para altas frequências na rede eléctrica do laboratório

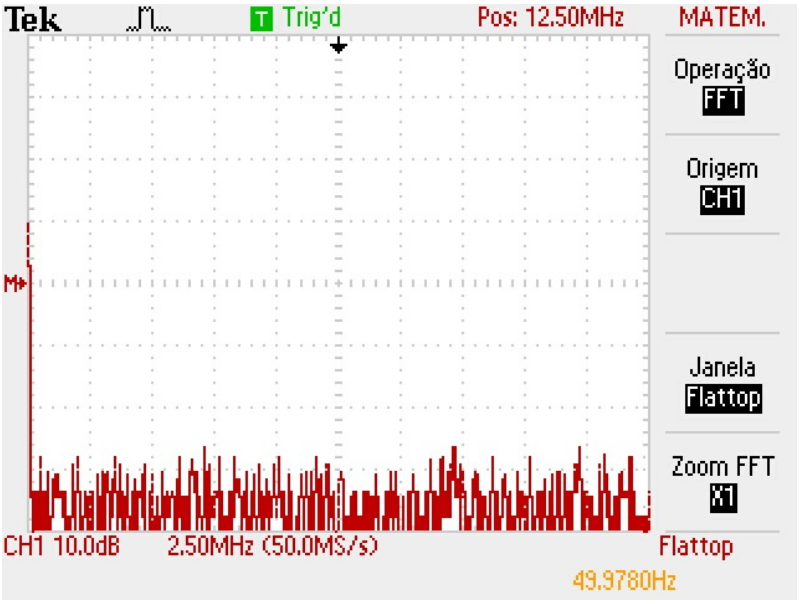

Figura 5.26: Análise espectral para altas frequências na rede eléctrica da TestBed

Capítulo 6

Conclusões e Trabalho Futuro

Neste capítulo apresentam-se as principais conclusões obtidas pelo trabalho efectuado, bem como os trabalhos propostos a desenvolver futuramente, com o intuito de avaliar o desempenho da rede HPAV noutros parâmetros, que não os aqui avaliados.

6.1 Conclusões

Este trabalho teve como principal objectivo avaliar o desempenho da rede *Homeplug* para suporte de aplicações industriais. Inicialmente foram avaliadas duas hipóteses quanto ao protocolo a utilizar, mas rapidamente se optou pelo protocolo *Homeplug AV*, pois em relação ao *Homeplug 1.0*, este garante uma largura de banda superior, maior imunidade às interferências eléctricas, melhores garantias dos parâmetros *QoS*, garantindo simultaneamente a interoperabilidade com equipamentos *Homeplug 1.0*. Outro aspecto relevante para a escolha desta tecnologia foi o facto desta ser relativamente recente, não existindo muitos estudos sobre o seu desempenho.

No decorrer do trabalho, foram efectuados vários testes com duas e três estações *Homeplug* a transmitir em simultâneo, registando-se os valores da largura de banda, pacotes perdidos, latência e jitter em cada um dos cenários de teste, o que permitiu caracterizar de uma forma sistemática o comportamento da rede para diferentes cenários.

Na primeira fase, os testes foram realizados com os módulos HPAV conectados directamente na rede eléctrica do laboratório I005 da FEUP, com o intuito de verificar, de uma forma genérica, o comportamento da rede HPAV.

Na segunda fase foi implementada uma rede isolada, a qual possibilitou controlar os equipamentos conectados à mesma, assim como as interferências eléctricas geradas por estes. Este troço da rede eléctrica isolado permitiu ainda garantir a repetibilidade dos testes, fazendo com que as condições em que estes decorreram não fossem alteradas entre repetições. Estes testes permitiram avaliar a influência das diferentes cargas em cada um dos parâmetros medidos.

As cargas utilizadas foram escolhidas por forma a simular o mais possível um ambiente industrial. Tendo em conta os equipamentos disponíveis no laboratório, foram utilizados monitores, computadores e motores, sendo estes equipamentos típicos num ambiente industrial.

À partida, um dos pontos críticos identificado em estudos anteriores sobre redes *Homeplug* foi a influência das interferências eléctricas no desempenho da mesma, sendo este um dos efeitos que se pretendeu avaliar. Contudo, e de acordo com os resultados obtidos, verifica-se que existe uma degradação no desempenho da rede, aquando da sua implementação directamente na rede eléctrica do laboratório, não sendo esta mesma degradação apresentada aquando da utilização do troço de rede eléctrica isolado. Posto isto, conclui-se que a tecnologia HPAV possui bastante robustez às interferências eléctricas, quando implementada em ambientes com cargas semelhantes às utilizadas neste estudo. No entanto, esta pode sofrer um abaixamento na largura de banda máxima disponível quando implementada em conjunto com outros equipamentos, os quais não foram identificados, uma vez que não fazem parte do objecto de estudo deste trabalho. Mesmo num ambiente com muitas interferências eléctricas, como é o caso do laboratório de electrotécnica, os resultados obtidos foram satisfatórios, pelo que, para aplicações que não necessitem de uma largura de banda bastante elevada, o HPAV poderá ser uma solução a considerar.

No que concerne aos valores médios obtidos para a latência e para o jitter, apresentados pelos pacotes transferidos, pode-se concluir que estes não são significativamente afectados pelas interferências geradas pelos equipamentos conectados na mesma rede eléctrica que a rede de dados HPAV.

Relativamente ao tráfego em tempo real, e mesmo considerando a exclusividade de transferência de tráfego UDP, o valor mais baixo obtido para a latência foi de 1,4 ms, tendo sido superior para a existência de tráfego em tempo real em conjunto com outro tráfego, nomeadamente tráfego TCP, onde foram obtidos os piores resultados. Tanto o elevado valor da latência, como do jitter, quando comparados com os valores obtidos para a rede *Ethernet* ponto a ponto, podem ser factores limitadores na utilização desta tecnologia para suporte de aplicações industriais com constantes de tempo bastante restritas.

Outro aspecto detectado aquando da realização dos testes foi a falta de conectividade quando os módulos foram conectados em dois laboratórios separados, contudo este tipo de testes não pôde ser efectuado de uma forma mais detalhada e sistemática, devido à falta de acesso às plantas da rede eléctrica do Departamento. Este é um aspecto muito importante a ter em conta aquando da escolha do tipo de rede a implementar numa planta industrial. Apesar da rede *Homeplug* não necessitar da instalação de cablagem nova, pode não funcionar correctamente quando implementada em locais com cablagem antiga e deficiente, ou em locais conectados a diferentes fases ou equipamentos que bloqueiem o sinal *Homeplug*.

Em termos de segurança na transferência de dados, verificou-se que existe a possibilidade de encriptação dos dados, o que garante a confidencialidade da informação transmitida.

O conjunto de testes efectuados teve uma duração bastante alargada, tendo sido de várias semanas, e nunca se tendo registado uma quebra do serviço devida ao mau funcionamento dos módulos *Homeplug*, pelo que se pode afirmar que a rede implementada por esta tecnologia é bastante fiável e robusta. Contudo, para caracterizar correctamente os níveis de fiabilidade deste tipo de redes deverão ser levados a cabo testes extensivos de alto tráfego de dados durante períodos de tempo mais longos.

Na realização deste trabalho foram algumas as limitações encontradas.

Inicialmente, o objectivo do trabalho era desenvolver um módulo *Homeplug* de entradas e saídas remotas para controlo de processos industriais. No entanto, devido ao elevado orçamento que seria necessário, optou-se pela avaliação do desempenho dos equipamentos já existentes no mercado. Esta alteração fez com que houvesse algum tempo despendido na execução da ideia original, reduzindo a disponibilidade temporal para a actual.

Além da anterior, outra dificuldade sentida, esteve relacionada com o *hardware* utilizado, uma vez que este se encontrava em condições incertas de funcionamento, tendo sido necessário testá-lo, verificando-se inclusive que um dos variadores de velocidade estava danificado.

Outro obstáculo, prendeu-se com a realização da medição dos valores de latência e de jitter para pacotes UDP. Uma vez que o tráfego UDP é unidireccional, esta medição requeria que os relógios estivessem sincronizados para se poder comparar o *timestamp* de envio com o *timestamp* de recepção. Assim, e de forma a resolver esta questão, utilizou-se do protocolo PTP para sincronização dos relógios, o que se demonstrou ser uma boa escolha, como se apresenta nos resultados obtidos. Porém, a utilização deste *software*, implicou a utilização do sistema operativo Linux, com o qual não estava familiarizado, tendo sido necessário aprofundar conhecimentos nas características específicas deste sistema operativo, principalmente ao nível das interfaces de rede. Apesar de moroso, este facto revelou-se de todo positivo pela aprendizagem efectuada.

Além destas, questões de ordem pessoal, como o facto de ser trabalhador-estudante e estar deslocado do local de trabalho, foram dificuldades sentidas aquando da execução do trabalho. No entanto, com esforço, empenho e muita gestão de tempo, foi possível minorar as repercussões que poderiam ter sobre o trabalho desenvolvido, e superar esses obstáculos.

Em suma, e fazendo uma apreciação global da Dissertação, considera-se que os objectivos propostos foram atingidos na sua totalidade. Os bons resultados obtidos comprovam a evolução da tecnologia PLC, demonstrando que esta poderá ser uma alternativa às soluções empregues actualmente para suporte de aplicações industriais, cada vez mais próxima da realidade, quer em termos de desempenho, quer em termos monetários.

Esta dissertação revelou-se muito gratificante quer pela aprendizagem efectuada, quer pelos novos conhecimentos adquiridos e, espera-se, que tenha sido um bom contributo para soluções futuras.

6.2 Trabalhos futuros

Relativamente aos trabalhos futuros, sugere-se a repetição dos testes realizados no decorrer desta Dissertação, mas com outro tipo de cargas conectadas à rede eléctrica, ou até mesmo repetir os testes efectuados num ambiente industrial real.

A implementação deste tipo de redes num ambiente industrial real permitiria também avaliar aspectos bastante importantes na escolha de uma solução para suporte deste tipo de aplicações, nomeadamente a resistência dos equipamentos a condições adversas, como poeiras, humidade,

temperatura, vibrações, entre outros. Estes aspectos não foram abordados neste trabalho, devido às limitações temporais e espaciais da Dissertação.

Outro ponto a ter em consideração, seria a repetição dos testes, mas colocando os módulos HPAV a diferentes distâncias entre si, até à distância máxima anunciada pelo fabricante.

Por fim, poderia também proceder-se à implementação de protocolos *Ethernet* industriais utilizando a tecnologia HPAV, avaliando o seu desempenho.

Referências

[1] Xavier Carcelle. *Power line communications in practice*. Artech House, 2009.

[2] Paulo Portugal e Luís Almeida. *Comunicações Industriais*, 2009.

[3] Zdenek Kaspar. Power-line communication - regulation introduction, pl modem implementation and possible application. 2001.

[4] Institute of electrical and electronics engineers. Disponível em http://www.ieee.org, acedido a última vez em 18 de Dezembro de 2010.

[5] Ieee standard for broadband over power line networks: Medium access control and physical layer specifications. *IEEE Std 1901-2010*, 2010.

[6] Open plc european research alliance. Disponível em http://www.ist-opera.org/, acedido a última vez em 18 de Dezembro de 2010.

[7] Zdenek Kaspar. D54: Final plan for using and disseminating knowledge. *OPERA. IST Integrated Project No 026920. Funded by EC*, 2007.

[8] Plc forum. Disponível em http://www.plcforum.com/, acedido a última vez em 18 de Dezembro de 2010.

[9] PLC Utilities Alliance. *PLC Utilities Alliance Introduction*, 2003.

[10] Universal powerline association (upa) and opera announce joint agreement on powerline specification. Disponível em http://www.powerlinenetworking.co.uk/content/view/134/1/, acedido a última vez em 18 de Dezembro de 2010.

[11] Homeplug alliance. Disponível em http://www.homeplug.org/, acedido a última vez em 18 de Dezembro de 2010.

[12] HomePlug Powerline Alliance Inc. *HomePlug 1.0 Technology White Paper*.

[13] Telecommunications Industry Association TIA. *TIA 1113: Medium-Speed (up to 14 Mbps) Power Line Communications (PLC) Modems using Windowed OFDM*.

[14] HomePlug Powerline Alliance Inc. *HomePlug AV White Paper*, 2005.

[15] HomePlug Powerline Alliance Inc. *Home Plug Green PHY The Standard For In-Home Smart Grid Powerline Communications*, 2010.

[16] European committee for electrotechnical standardization. Disponível em http://www.cenelec.eu/Cenelec/Homepage.htm, acedido a última vez em 18 de Dezembro de 2010.

[17] International electrotechnical commission. Disponível em http://www.iec.ch, acedido a última vez em 18 de Dezembro de 2010.

[18] European telecommunications standards institute. Disponível em http://www.etsi.org, acedido a última vez em 18 de Dezembro de 2010.

[19] Introduction to x10 home automation technology. Disponível em http://www.oreillynet.com/pub/a/network/2005/01/10/x10_hmhck.html, acedido a última vez em 18 de Dezembro de 2010.

[20] The history of x10. Disponível em http://home.planet.nl/~lhendrix/x10_history.htm, acedido a última vez em 18 de Dezembro de 2010.

[21] X10 Pro. *X-10 Communications Protocol and Power Line Interface PSC04 PSC05*, Rev 2.4.

[22] G Evans. *CEBus demystified: the ANSI/EIA 600 user's guide*. McGraw-Hill, 2001.

[23] Echelon Corporation. *Introduction to Lonworks System*, Version 1.0.

[24] Jawwad Shamsi e Monica Brocmeyer. Chapter 1 principles of network monitoring.

[25] James F. Kurose e Keith W. Ross. *Computer Networking: A Top-Down Approach*. Addison-Wesley, 5 edição, 2010.

[26] TE Connectivity Ltd. *Multipurpose Power Line RFI Filter for Emission Control Datsheet*, 2011.

[27] Ethernet rj-45 loopback, crossed and pinouts. Disponível em http://sites.google.com/site/kalman/tech-break/ethernetrj-45loopback, acedido a última vez em 2 de Fevereiro de 2011.

[28] Devolo AG, Germany. *dLAN® 200 AVmini Starter Kit - Technical Data*, 2009.

[29] Iperf. Disponível em http://sourceforge.net/projects/iperf/, acedido a última vez em 12 de Maio de 2011.

[30] Jperf. Disponível em http://sourceforge.net/projects/jperf/, acedido a última vez em 12 de Maio de 2011.

[31] Iperf - the easy tutorial. Disponível em http://openmaniak.com/iperf.php, acedido a última vez em 12 de Maio de 2011.

[32] Packeth - ethernet packet generator. Disponível em http://packeth.sourceforge.net/, acedido a última vez em 24 de Maio de 2011.

[33] Wireshark wiki. Disponível em http://wiki.wireshark.org/, acedido a última vez em 24 de Maio de 2011.

[34] Precision time protocol (ptp). Disponível em http://ptpd.sourceforge.net/, acedido a última vez em 13 de Junho de 2011.

[35] IEEE Instrumentation and Measurement Society. *IEEE 1588-2008 Standard for a Precision ClockSynchronization Protocol for Networked Measurement and ControlSystems*, 2008.

[36] IEEE Instrumentation and Measurement Society. *IEEE 1588-2002 Standard for a Precision ClockSynchronization Protocol for Networked Measurement and ControlSystems*, 2002.

[37] Caleb Gordon. White paper introduction to ieee 1588 and transparent clocks. 2009.

[38] Michael Branicky Kendall Correll, Nick Barendt. Design considerations for software only implementations of the ieee 1588 precision time protocol.

[39] Mahbub Hassan e Raj Jain. *High Performance TCP/IP Networking*. Prentice-Hall, Inc., 2003.