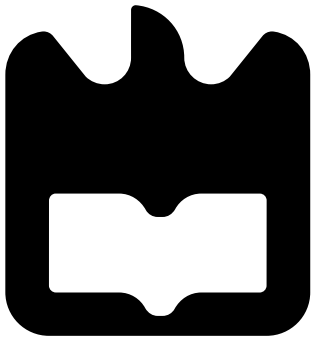
Universidade de Aveiro
Departamento de
Electrónica, Telecomunicações e Informática
2012

Jorge Filipe Dias

Mobilidade em Comunicações Veiculares



Jorge Filipe Dias

Mobilidade em Comunicações Veiculares

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Eletrónica e Telecomunicações, realizada sob a orientação científica da Doutora Susana Isabel Barreto de Miranda Sargento e do Doutor Arnaldo Silva Rodrigues de Oliveira, Professores Auxiliares do Departamento Eletrónica, Telecomunicações e Informática da Universidade de Aveiro

o júri / the jury

presidente / president

Prof. Doutor João Nuno Pimentel da Silva Matos
Professor Associado da Universidade de Aveiro (por delegação da Reitora da Universidade de Aveiro)

vogais / examiners committee

Prof. Doutor Daniel Enrique Lucani Rotter
Professor Auxiliar Convidado do Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto (Arguente)

Prof. Doutora Susana Isabel Barreto de Miranda Sargento
Professora Auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro (Orientadora)

Prof. Doutor Arnaldo Silva Rodrigues de Oliveira
Professora Auxiliar do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro (Coorientador)

agradecimentos / acknowledgements

Em primeiro lugar, gostaria de agradecer aos meus Pais por me darem a oportunidade de obter um curso superior, assim como todo o apoio oferecido durante todo o meu percurso académico. Gostaria também de agradecer ao meu Irmão que sempre me apoiou e ajudou, quer nos assuntos relacionados com os estudos, quer em todos os outros assuntos.

Agradeço a todos os colaboradores do projeto DRIVE-IN que me ajudaram no desenvolvimento desta Dissertação, em especial ao Filipe Neves pela ajuda na integração e nos testes práticos realizados em ambiente veicular. Gostaria também de agradecer ao Nelson Capela pela disponibilização da sua versão do protocolo MIPv6.

Agradeço a todos os meus amigos que me acompanharam ao longo de todos estes anos, em especial ao Tiago Pina que me acompanhou em grande parte do percurso académico.

Por fim, gostaria de agradecer à Professora Susana Sargento e ao Professor Arnaldo Oliveira por me terem oferecido a oportunidade de realizar esta Dissertação, bem como toda a orientação prestada ao longo desta. Agradeço também ao meu colaborador André Cardote por estar sempre pronto a ajudar, indicando o melhor caminho a seguir e discutindo os problemas encontrados.

Palavras-chave

VANET, Comunicações Veiculares, IEEE 802.11p, Protocolos de Encaminhamento, Mobilidade, MIPv6, PMIPv6, *Handover*, *Testbed*

Resumo

As redes veiculares têm emergido com o objetivo de aumentarem a segurança nas estradas e também de providenciarem viagens mais confortáveis aos passageiros e condutores, utilizando para tal comunicações entre veículos ou entre veículos e infraestruturas colocadas ao longo das estradas. Devido ao facto de estas redes serem constituídas por veículos, estas vão enfrentar uma série de desafios, como: elevada mobilidade, frequentes perdas ligações, particionamento da rede, etc.. Face a estes desafios, o trabalho realizado nesta Dissertação pretende desenvolver mecanismos capazes de providenciar *handover* transparente entre as várias estações fixas. Foram também estudados vários mecanismos de encaminhamento, pretendendo-se perceber quais poderiam ser utilizados em redes veiculares, e quais as adaptações necessárias para tal.

Nas redes veiculares cada nó deve ser capaz de encaminhar a informação para os restantes, assim, torna-se necessário a utilização de protocolos de encaminhamento. Deste modo foram estudados três protocolos de encaminhamento para redes *ad-hoc*, concluindo-se que os protocolos BABEL e B.A.T.M.A.N. se podem adaptar a redes veiculares, ao contrário do protocolo OLSR. No entanto, foi também possível concluir que estes não são capazes de suportar a mobilidade dos veículos entre as várias estações fixas, sendo assim necessária a utilização de mecanismos capazes de o fazer.

De forma a ser possível efetuar *handover* rápido e transparente é necessário utilizar um protocolo de mobilidade que irá garantir a continuidade do endereço de IP e da sessão, efetuando todo o processo de registo necessário para tal. Sabendo desta necessidade, foram estudados dois protocolos de mobilidade, o MIPv6 e o PMIPv6, com o objetivo de se perceber qual apresenta melhor desempenho e qual se adapta melhor a VANETs. Ambos os protocolos evidenciaram limitações que impediam a realização de *handover* transparente. Para fazer face a estas limitações foram desenvolvidos mecanismos para as ultrapassar. Para além do protocolo de mobilidade, para que se efetue um *handover* eficiente, é necessário utilizar um mecanismo que monitorize as redes existentes, faça a ligação com estas e comunique com o protocolo de mobilidade, ou seja, um gestor de conetividade, o qual foi também desenvolvido no âmbito desta Dissertação.

Devido à existência de uma grande diversidade de tecnologias sem fios de acesso à rede, pretende-se perceber até que ponto a utilização da norma IEEE 802.11p, criada especificamente para redes veiculares, melhora o desempenho durante o *handover*, em comparação com o desempenho obtido através das tecnologias de acesso à rede mais comuns, como o Wi-Fi e o 3G. Para tal utilizaram-se três tecnologias: o IEEE 802.11p, IEEE 802.11g e o 3G.

Os resultados obtidos mostram que o PMIPv6 apresenta um desempenho global superior ao MIPv6, especialmente quando utilizada a tecnologia IEEE 802.11p. Observou-se também que utilizando o PMIPv6 é possível realizar *handover* entre duas redes IEEE 802.11p sem que exista qualquer perda de dados durante o processo, mesmo quando esta se faz a uma velocidade elevada. Além disso, verificou-se também que o 3G não é adequado para comunicações veiculares que tenham restrições de latência.

Keywords

VANET, Vehicular Communication, IEEE 802.11p, Routing Protocols, Mobility, MIPv6, PMIPv6, Handover, Testbed

Abstract

Vehicular networks have emerged in order to increase road safety and also to provide more comfortable trips to both passengers and drivers, using communication between vehicles and between vehicles and infrastructure placed along the road. Since the network is composed by vehicles, it faces many challenges, such as: high mobility, frequent network disconnection, network partition, etc. Due to these challenges, the work done in this Thesis intends to develop mechanisms capable to provide seamless handover between the fixed stations. It also performed a study on the several routing mechanisms, in order to understand which could be used in vehicular networks, and what enhancements are necessary to do so.

In vehicular networks each node must be able to route the information to other nodes; thus, it is necessary the use of routing protocols. Therefore, three routing protocols for ad-hoc networks were studied, concluding that BABEL and B.A.T.M.A.N. can be used in vehicular networks, unlike OLSR. Nonetheless, it was also possible to conclude that these protocols are not capable of supporting the vehicles' mobility between fixed stations, and therefore it is required the use of mechanisms capable of doing so.

In order to achieve seamless handover, it is necessary to use a mobility protocol, which will ensure IP address and session continuity, performing the entire process of registration required for mobility. This Thesis studied two mobility protocols, the MIPv6 and PMIPv6, in order to understand which one performs better and best fits in VANETs. Both protocols showed limitations that prevented the execution of seamless handover. To address these limitations we developed mechanisms to enhance their performance. In addition to the mobility protocol, in order to make an efficient handover, it is necessary to use a mechanism to monitor the existing networks, connect with these and communicate with the mobility protocol, i.e., connectivity manager, which was also developed within this Thesis.

Due to the existence of a wide variety of wireless access network technologies, this study seeks to realise how far the use of IEEE 802.11p standard, designed specially for vehicular networks, improves the performance during the handover, compared to the performance achieved through the more common access technologies, such as Wi-Fi and 3G. For this purpose, we used three technologies: the IEEE 802.11p, IEEE 802.11g and 3G.

The results show that, in overall, the PMIPv6 show a better performance than the MIPv6, especially when using the IEEE 802.11p. It was also noted that, using the PMIPv6, it is possible to perform handover between two IEEE 802.11p networks without any data loss during this process, even when this is done at considerable speeds. Furthermore, it was also verified that the 3G is not suitable for vehicular communications which have latency constraints.

Conteúdo

Lista de Figuras

Lista de Tabelas

Acrónimos

AODV *Ad-hoc On-Demand Distance Vector*

AU *Application Unit*

AP *Access Point*

B.A.T.M.A.N. *Better Approach To Mobile Ad-hoc Networking*

BA *Binding Acknowledgement*

BC *Binding Cache*

BCE *Binding Cache Entry*

BS *Base Station*

BSS *Basic Service Set*

BU *Binding Update*

C2C-CC *Car-to-Car Communication Consortium*

CCA *Cooperative Collision Avoidance*

CCH *Control Channel*

CN *Correspondent Node*

CoA *Care-of-Address*

CoT *Care-Test*

CoTI *Care-of Test Init*

CPU *Central Processing Unit*

CSMA *Sense Multiple Access*

DAD *Duplicate Address Detection*

DHCP *Dynamic Host Configuration Protocol*

DSR *Dynamic Source Routing Protocol*

DSRC *Dedicated Short-Range Communications*

DIVERT *Development of Inter-VEhicular Reliable Telematics*

DRIVE-IN *Distributed Routing and Infotainment through VEhicular Inter-Networking*

ECDSA *Elliptic Curve Digital Signature Algorithm*

ETX *Expected Transmission count*

EUA Estados Unidos da América

EWM *Emergency Warning Message*

FCC *Federal Communication Commission*

FMIPv6 *Fast Mobile Internet Protocol version 6*

FN *Foreign Network*

FSR *Fisheye State Routing Protocol*

GPS *Global Positioning System*

GS *Group Signature*

HA *Home Agent*

HMIPv6 *Hierarchical Mobile Internet Protocol version 6*

HN *Home Network*

HNP *Home Network Prefix*

HoT *Home-Test*

HoTI *Home Test Init*

HSPA *High-Speed Packet Access*

ICMP *Internet Control Message Protocol*

ID *Identity*

IEEE *Institute of Electrical and Electronics Engineers*

IGW *Internet Gateway*

IP *Internet Protocol*

IPv4 *Internet Protocol version 4*

IPv6 *Internet Protocol version 6*

LISP *Locator/ID separation protocol*

LMA *Local Mobility Anchor*

MAC *Medium Access Control*

MAG *Mobile Access Gateway*

MANET *Mobile Ad-hoc NETwork*

MAP *Mobility Anchor Point*

MICS *Media Independent Command Service*

MIES *Media Independent Event Service*

MIIS *Media Independent Information Service*

NAR *New Access Router*

MN *Mobile Node*

MIH *Media Independent Handover*

MIHF *Media Independent Handover Function*

MIPv6 *Mobile Internet Protocol*

MPR *Multipoint Relay*

NA *Neighbor Advertisement*

NEMO *Network Mobility*

NS *Neighbor Solicitation*

NS-2 *Network Simulator 2*

OAI PMIPv6 *OpenAirInterface Proxy Mobile IPv6*

OBU *On Board Unit*

OGM *Originator Message*

OLSR *Optimized Link State Routing Protocol*

OSI *Open Systems Interconnection*

PAC *Packet Forwarding Control*

PAR *Previous Access Router*

PBA *Proxy Binding Acknowledgement*

PBU *Proxy Binding Update*

PC *Personal Computer*

PDR *Packet Delivery Ratio*

PHY *Physical Layer*

PMIPv6 *Proxy Mobile Internet Protocol version 6*

PrRtAdv *Proxy Router Advertisement*

PTP *Precision Time Protocol*

QoS *Quality of Service*

RA *Router Advertisement*

RERR *Route ERRor*

RREP *Route REPly*

RREQ *Route REQuest*

RS *Router Solicitation*

RSSI *Received Signal Strength Indicator*

RSU *Road Side Unit*

RtSolPr *Router Solicitation for Proxy Advertisement*

SCH *Service Channel*

SSID *Service Set IDentifier*

STDMA *Self-Organized Time Division Multiple Access*

TC *Topology Control*

TCP *Transmission Control Protocol*

TESLA *Timed Efficient Stream Loss-tolerant Authentication*

TORA *Temporally-Ordered Routing Algorithm*

UMIP *USAGI-patched Mobile IPv6 for Linux*

UDP *User Datagram Protocol*

USB *Universal Serial Bus*

VAC *Vehicular Address Configuration*

V2I *Vehicle-to-Infrastructure*

V2V *Vehicle-to-Vehicle*

VANET *Vehicular Ad-hoc NETwork*

VOD *Video-on-Demand*

VoIP *Voice over Internet Protocol*

WAVE *Wireless Access in the Vehicular Environment*

WBSS *Wave-mode Basic Service Set*

WLAN *Wireless Local Area Network*

WSA WAVE *Service Announcement*

WSMP WAVE *Short-Message Protocol*

ZOR *Zone-Of-Relevance*

Capítulo 1

Introdução

1.1 Motivação

Nas últimas décadas as redes sem fios sofreram uma enorme evolução e consequente massificação, tendo vindo a crescer bastante nos últimos anos, prevendo-se um crescimento ainda maior no futuro (de acordo com dados da Cisco [1], o tráfego gerado através de redes móveis irá crescer 18 vezes entre 2010 e 2016). Paralelamente os fabricantes de automóveis têm vindo a introduzir uma série de serviços nos seus veículos, como sensores, sistemas de posicionamento e navegação, computadores de bordo, etc.. Tendo em conta estes acontecimentos surgiu recentemente uma nova classe de redes sem fios, as VANETs, que pretendem fazer com que os carros comuniquem entre si, aumentando assim a segurança nas estradas. É também de esperar que os veículos possam comunicar com redes externas, como a *Internet*, oferecendo assim uma série de aplicações de conforto aos ocupantes dos veículos. Esta Dissertação foca-se neste aspeto, ou seja, pretende-se estudar qual a melhor forma de fornecer estes serviços aos veículos e qual a capacidade de serem utilizadas as redes e infraestrutura já existentes, em conjunto com as novas tecnologias de redes veiculares.

Para que os veículos se possam ligar à *Internet* durante o seu movimento é necessário ter em conta uma série de fatores condicionantes, como o próprio movimento em si, que criará a necessidade de mudança de rede, as falhas de cobertura existente, pois não se espera que as estradas estejam completamente cobertas com dispositivos capazes de fornecer esta ligação, entre outros. Espera-se também que os veículos acedam à *Internet* não só através comunicações veiculares, baseadas na norma IEEE 802.11p, mas também através das redes já existentes, como o Wi-Fi ou 3G/4G. Para que se possam utilizar todas estas tecnologias em simultâneo e para suportar a mobilidade dos veículos existem dois desafios essenciais que

se têm de ultrapassar. O primeiro está relacionado com a necessidade de efetuar a ligação com a rede que apresentar melhor qualidade de ligação, por cada tecnologia utilizada, pois caso tal não aconteça, as perdas de ligação irão ser frequentes e a qualidade de serviço será bastante afetada, fazendo com que estas redes tenham pouca aceitação por parte dos utilizadores. Tendo em conta todos estes fatores é necessário estudar e desenvolver um mecanismo de que possa lidar com esta condicionante, determinando e efetuando a ligação com a rede que oferece melhores caraterísticas. O segundo desafio está relacionado com a necessidade de se efetuar o *handover* ao nível da camada de rede, quer esta seja dentro da mesma tecnologia de acesso à rede, quer seja entre tecnologias de acesso à rede diferentes. Caso este processo não seja efetuado de uma forma eficiente, os utilizadores irão perder a ligação sempre que se movimentarem entre redes e irão também perder todas as sessões que existirem naquele momento, por exemplo: se um utilizador está a utilizar um serviço de *Voice over Internet Protocol* (VoIP), esse serviço iria ser desligado quando ocorresse a movimentação entre redes, sendo depois necessário iniciar uma nova ligação. Face a este condicionamento torna-se necessário utilizar um mecanismo capaz de otimizar o processo de registo associado à transição de rede, para que este processo se torne rápido e transparente, fazendo com que os utilizadores das VANETs não sintam quebras na qualidade do serviço, aquando do movimento entre redes.

1.2 Enquadramento

Os trabalhos desenvolvidos ao longo desta Dissertação enquadram-se no projeto *Distributed Routing and Infotainment through VEhicular Inter-Networking* (DRIVE-IN) [2]. O objetivo deste projeto é estudar as comunicações veículo-a-veículo e a forma como estas podem melhorar a experiência dos ocupantes dos veículos, bem como a eficiência do tráfego rodoviário. Este projeto pretende, não só estudar e desenvolver aplicações para VANETs, bem como as próprias comunicações entre veículos, ou seja, pretende-se abranger uma grande área de investigação, desde a implementação da norma IEEE 802.11p / IEEE 1609.x / WAVE, parte mais próxima do *hardware*, até ao desenvolvimento de aplicações em redes veiculares. Deste modo destacam-se as seguintes linhas de investigação:

- ***Geo-Optimized VANET Protocols*** - Pretende-se explorar novas arquiteturas de comunicação tendo em conta o posicionamento geográfico;
- ***Intelligent and Collaborative Car Routing*** - Através de comunicações entre veículos

pretende-se criar um sistema de navegação descentralizado e inteligente;

- ***VANET Applications and Services*** - Um dos objetivos deste projeto é o desenvolvimento de aplicações e serviços baseados em comunicações veiculares, aplicações orientadas à segurança, e também o aproveitamento das redes já existentes (*hotspots* Wi-Fi e 3G) para o desenvolvimento de aplicações de conforto;
- ***High Performance VANET Simulation*** - Pretende-se melhorar o simulador *Development of Inter-VEhicular Reliable Telematics* (DIVERT) [3] para a versão 2.0, de forma a se poderem obter simulações mais precisas, através de melhores modelos de tráfego;
- ***Deployment and Experimentation*** - Será colocado em prática o maior exemplo de uma rede VANET, com as devidas tecnologias e protocolos, utilizando 465 táxis na cidade do Porto.

Tendo em conta a necessidade dos veículos se ligarem à *Internet*, referida na secção anterior, e sabendo que esta *testbed* decorre numa cidade em que existe um grande número de infraestruturas de acesso à *Internet*, o trabalho desenvolvido no âmbito desta Dissertação pretende dar a capacidade aos veículos de obterem uma ligação constante com a infraestrutura já existente, e também a infraestrutura desenvolvida durante este projeto. Deste modo, é necessário ter em conta a gestão da conetividade, pois é necessário perceber quais as redes que oferecem melhor qualidade de ligação e efetuar a ligação com as mesmas. É também necessário ter em conta a gestão da mobilidade, para que a transição entre infraestruturas se efetue de forma rápida e transparente.

1.3 Objetivos

Sabendo que os veículos apresentam uma elevada mobilidade e que tendo em conta as diferentes tecnologias de acesso à rede disponíveis, esta dissertação tem como objetivo estudar e desenvolver mecanismos que permitam aos veículos obterem acesso à rede durante o seu movimento. Face aos desafios enunciados na Secção 1.1, o principal objetivo desta dissertação é o desenvolvimento de mecanismos capazes de lidar com estes desafios, tentando minimizar o tempo de perda de ligação durante as movimentações entre redes.

Assim, os objetivos desta dissertação são os seguintes:

- Fazer um levantamento dos protocolos de encaminhamento adaptados a VANETs;

- Realizar as adaptações e configurações necessárias para integrar os protocolos de encaminhamento utilizados em cenários de comunicações *Vehicle-to-Vehicle* (V2V) e *Vehicle-to-Infrastructure* (V2I).
- Estudar a capacidade de os protocolos de encaminhamento suportarem o processo de mobilidade entre diferentes RSUs;
- Fazer um levantamento dos protocolos de mobilidade e efetuar a sua integração nos equipamentos utilizados neste projeto;
- Desenvolvimento de um gestor de mobilidade capaz de determinar e efetuar a ligação com as redes que ofereçam melhor qualidade de ligação;
- Analisar o desempenho dos dois protocolos de mobilidade utilizados, propor e implementar melhorias nos mesmos;
- Idealizar uma *testbed*, em ambiente laboratorial, capaz de fornecer dados sobre os protocolos de mobilidade em estudo, para que se possa efetuar uma comparação do desempenho de cada um;
- Definir as métricas e metodologia utilizada para caraterizar o processo de *handover* de cada um dos protocolos. Concluir acerca do desempenho de cada um dos protocolos em ambiente laboratorial;
- Desenvolver e implementar uma *testbed* capaz de testar o protocolo PMIPv6 em ambiente veicular e concluir sobre a capacidade ser utilizado como protocolo de mobilidade em redes veiculares.

Este trabalho deu origem a um artigo cientifico "*Seamless Mobility in VANET using Proxy Mobile IP*"a submeter à IEEE *Vehicular Networking Conference*, 2012.

1.4 Organização do Documento

Esta dissertação está organizada da seguinte forma:

- No Capítulo 1 é efetuada uma contextualização da dissertação, sendo apresentada a motivação, o enquadramento e os seus objetivos;
- No Capítulo 2 é apresentado o estado da arte das redes veiculares, sendo neste apresentados os principais conceitos sobre este tipo de redes para que o leitor se possa enquadrar neste assunto. São também apresentados alguns conceitos acerca de protocolos de encaminhamento e de mobilidade e da sua integração em redes veiculares;

- No Capítulo 3 é apresentado todo o estudo efetuado sobre protocolos de encaminhamento. Numa primeira fase é apresentada a sua integração com os equipamentos utilizados, enquanto numa segunda parte é estudada a possibilidade de serem utilizados de forma a darem suporte a mobilidade entre as várias RSUs;
- No Capítulo 4 é descrita a arquitetura que se pretende estudar, seguindo-se uma descrição das implementações e alterações efetuadas em cada um dos protocolos de mobilidade estudados. Ainda neste capítulo é apresentado o gestor de mobilidade desenvolvido;
- No Capítulo 5 são apresentadas as *testbeds* utilizadas para testar os protocolos de mobilidade, seguindo a apresentação e discussão dos resultados obtidos, em ambiente laboratorial e em ambiente veicular;
- No Capítulo 6 é apresentada uma conclusão de todo o trabalho efetuado durante esta Dissertação. Por fim, são também sugeridos trabalhos que podem ser efetuados como continuação do trabalho desenvolvido.

Capítulo 2

Estado da Arte

Neste capítulo será apresentado um resumo do trabalho na área de redes veiculares baseadas em livros e artigos científicos com o objetivo de enquadrar o leitor nesta área de conhecimento.

2.1 O que são Redes Veiculares?

As redes veiculares, também conhecidas por VANETs, são uma nova classe de redes sem fios que têm vindo a emergir nos últimos anos, devido, por um lado aos avanços feitos nas tecnologias de redes sem fios, sobretudo após a massificação das *Wireless Local Area Network*s (WLANs) e das redes celulares, por outro lado aos avanços na indústria automóvel: hoje em dia já quase todos os automóveis vêm equipados com sistema de posicionamento *Global Positioning System* (GPS), múltiplos sensores, etc.. Neste contexto surgem as redes veiculares que consistem em redes formadas espontaneamente entre veículos equipados com tecnologia que possibilite a comunicação sem fios. Designa se por OBU a unidade responsável pelo tratamento, envio e receção de informações de e para a rede. As VANETs permitem a comunicação entre veículos – V2V – e também a comunicação entre veículos e equipamentos fixos – V2I – , equipamentos estes usualmente designado de RSUs.

Estas redes poderão ser utilizadas por todo o tipo de veículos, quer estes sejam privados, ou empresariais, quer sejam veículos públicos (autocarros, ambulâncias, carros de policia, etc.). Já as RSUs podem pertencer aos governos locais ou a operadores de telecomunicações.

As VANETs têm como grande objetivo reduzir a sinistralidade nas estradas, introduzindo uma série de serviços de segurança que possibilitem essa redução, mas, para além da segurança, têm também como objetivo melhorar a circulação e ainda proporcionar ao condutor

e aos ocupantes dos veículos viagens mais cómodas, proporcionando a possibilidade de consultar *e-mails* e ler noticias, por exemplo. Assim, as VANETs são bastante promissoras e têm atraído a atenção da comunidade científica, autoridades governamentais e também da indústria automóvel. Neste contexto, surgiu nos Estados Unidos da América (EUA) um sistema de comunicações de curto alcance DSRC, sendo em 1999 aprovados 75 MHz de espetro (nos 5.9 GHz) pela *Federal Communication Commission* (FCC) reservados para comunicações entre veículos. Por outro lado, na Europa, foi iniciado o *Car-to-Car Communication Consortium* (C2C-CC) [4] que teve origem em construtores de automóveis e fabricantes de equipamentos para automóveis, com o objetivo de aumentar a segurança e eficiência da circulação rodoviária através de comunicação entre veículos. Também o *Institute of Electrical and Electronics Engineers* (IEEE) fez avanços na área das redes veiculares através da criação dos *standards Wireless Access in the Vehicular Environment* (WAVE), IEEE 1609.x e IEEE 802.11p.

2.1.1 Desafios Técnicos

Devido às caraterísticas específicas das VANETs estas exibem uma série de desafios que necessitam de ser tidos em conta durante o seu desenvolvimento destas redes. De acordo com Moustafa et al. [5] estes são:

- **Comunicação e protocolo *Medium Access Control* (MAC) confiável** - Devido à natureza dinâmica e à alta mobilidade da rede, deve ser garantido uma rápida associação e baixa latência de forma a garantir que existe fiabilidade na transmissão de mensagens de segurança e que existe qualidade e continuidade nas comunicações de outro tipo de aplicações;
- **Disseminação da informação e Encaminhamento** - Os algoritmos de disseminação de informação e encaminhamento devém-se adaptar às caraterísticas das VANETs e suas aplicações, de forma a permitir diferentes prioridades de transmissão consoante o tipo de aplicação;
- **Segurança** - Deve ser desenvolvido um sistema de segurança que providencie confiança, autenticação, controlo de acesso e autorização ao acesso a conteúdos seguros;
- **Configuração de endereço *Internet Protocol* (IP) e Mobilidade** - Deve existir um processo automático e rápido para configuração do endereço IP e deve também ser implementado um mecanismo de controlo de mobilidade, que garanta a qualidade e continuidade da ligação com a *Internet*.

2.2 Conceitos Básicos

2.2.1 Caraterísticas Específicas

Nas VANETs, tal como nas *Mobile Ad-hoc NETwork*s (MANETs), os nós auto organizam-se sem a necessidade de uma autoridade central. Os seus nós podem atuar como *Mobile Node*s (MNs) ou como *router* para outro MN. Mas nas VANETs como os seus nós são veículos, estas vão ter características únicas e diferenciadoras em relação a todas as outras redes sem fios existentes, segundo Li e Wang [6] estas são:

- **Topologia bastante dinâmica** - Devido às altas velocidades a que os veículos circulam a topologia da rede vai estar em constante alteração. Considerando dois veículos em autoestrada a circular a 120 km/h e em sentidos opostos, apenas vão estar conectados durante 10 segundos, assumindo que cada veículo tem um raio de comunicação de 250 metros;
- **Frequente perda de ligação** - De acordo com o ponto anterior a conetividade entre veículos vai alterar-se frequentemente, sobretudo em cenários com pouca densidade de veículos. Nestes casos, este problema pode ser contornado com a colocação de RSUs;
- **Alta capacidade energética e de processamento** - Ao contrário das MANETs, nas VANETs, como os nós são veículos com uma grande capacidade de energética (devido à bateria), não apresentam restrições a este nível. Possuem também uma grande capacidade de processamento, pois os nós da rede não têm tamanho limitado, não sendo assim limitados por este fator;
- **Comunicação geográfica** - Comparando com outro tipo de redes que utilizam *unicast* ou *multicast*, nas VANETs pode-se utilizar um novo tipo de comunicação em que os pacotes são encaminhados para uma determinada zona de acordo com um endereço geográfico;
- **Mobilidade previsível** - Uma vez que, normalmente, os veículos circulam em estradas ou ruas, e tendo em conta a sua posição, velocidade e sentido é possível saber a posição futura de um certo veículo;
- **Ambientes variados** - Existem dois ambiente típicos de comunicação, em autoestrada em que o ambiente é relativamente simples já que os veículos circulam todos na mesma direção, alterando apenas a velocidade e o sentido, ou o ambiente em cidade em que existem inúmeras ruas e bastantes obstáculos;

- **Restrições de latência** - Em aplicações de segurança o atraso na entrega dos pacotes tem que ser bastante pequeno, pois, caso assim não aconteça, quando o pacote chegar ao destino pode já ter existido um acidente;

- **Sensores a bordo** - É assumido que os veículos estão equipados com sensores, que providenciem informações úteis a os outros veículos da rede. Por exemplo, se um carro faz uma travagem brusca, é necessário que tenha instalado um sensor que detete essa travagem, para depois esta informação ser propagada para a rede para que os outros veículos evitem uma colisão.

2.2.2 Equipamento Básico

Numa rede veicular é necessário que os veículos estejam equipados com uma OBU. De acordo com Kihl [7] é assumido, na maior parte dos artigos científicos nesta área, que estas possuam os seguintes componentes:

- Uma ***Central Processing Unit*** **(CPU)** que implementa as aplicações e os protocolos de comunicação;

- Uma **antena** que permite o envio e receção de informação;

- Um recetor de **GPS** que dá informação sobre a posição e sincronismo;

- **Sensores** apropriados que permitam a medição de vários parâmetros;

- Uma ***Interface Input/Output*** para permitir a interação entre o utilizador e o sistema.

2.2.3 Arquitetura da Rede

A arquitetura da rede tem sido um dos temas mais discutidos nas redes veiculares, pois a introdução de RSUs pode ajudar a melhorar a conetividade da rede. No entanto, pode tornar-se um problema, pois envolve a criação de novas infraestruturas, com o consequente aumento de custos que tal acarreta.

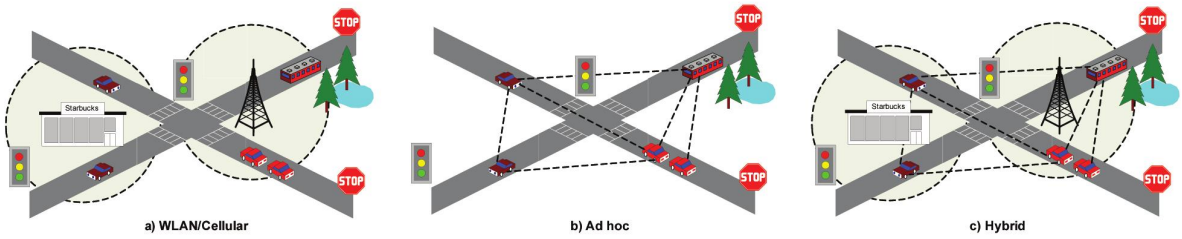


Figura 2.1: Arquitetura das *Vehicular Ad-hoc NETwork*s (fonte:[8])

Segundo Lee et al. [8], existem três possibilidades para a arquitetura da rede como se pode observar na figura 2.1:

- Arquitetura **WLAN/Celular** recorre a infraestruturas, ligadas entre si e colocadas ao longo das estradas para garantir a comunicação V2I: estes nós centralizam todo o tráfego da rede. Esta arquitetura tem a vantagem de se obter sempre conetividade dos veículos com a rede, caso as estradas estejam completamente cobertas por estas infraestruturas, o que acaba por trazer a desvantagem de um custo insuportável. Este tipo de arquitetura tem também a vantagem de as infraestruturas poderem estar ligadas a outras redes, como a *Internet*, possibilitando assim aos veículos a ligação a estas redes;

- Arquitetura puramente ***ad-hoc*** em que os veículos se comportam como *routers* e encaminham a informação entre eles através de múltiplos saltos. Esta implementação tem como vantagem o custo de implementação pois, não sendo necessárias infraestruturas, apenas é necessário equipar os automóveis com OBU para se garantir comunicação entre eles. Como é de esperar esta arquitetura vai estar bastante dependente da densidade de veículos para fazer o encaminhamento da informação, sendo que em cenários de pouca intensidade de tráfego será bastante difícil obter-se comunicação. Este tipo de arquitetura apresenta também o problema de os veículos não terem acesso a redes externas;

- A arquitetura **híbrida** é uma solução que pretende juntar as duas anteriores de forma a minimizar as desvantagens de cada uma. Nesta arquitetura não é garantida uma cobertura total pelas infraestruturas, mas sim a sua colocação em locais que possibilitem a maximização da conetividade da rede.

2.2.3.1 Arquitetura C2C-CC

A C2C-CC propôs em [9] uma arquitetura para redes veiculares que se divide em três domínios: domínio do veículos, domínio *ad-hoc* e domínio das infraestruturas, como se pode observar na Figura 2.2.

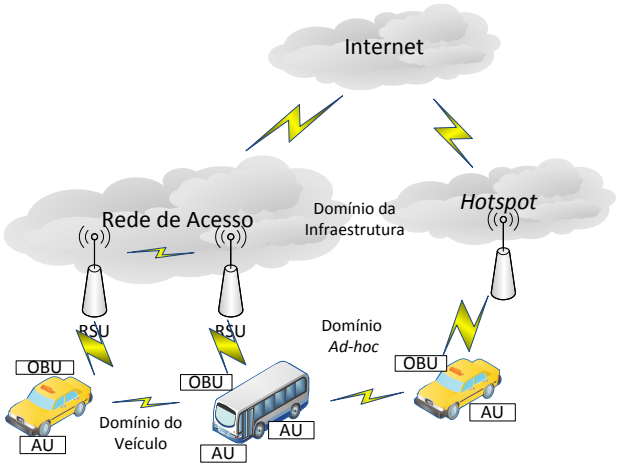


Figura 2.2: Arquitetura referencia da *Car-to-Car Communication Consortium*

O domínio do veículo é composto por dois tipos de unidades, a OBU e uma ou mais *Application Unit*s (AUs). A OBU é responsável pela comunicação com outros veículos ou com as RSU, a AU é a unidade que executa as aplicações pretendidas pelo utilizador. Assim, a AU pode ser parte integrante do veículo e estar permanentemente ligada com a OBU ou pode ser um dispositivo portátil (*Smartphone*, *Personal Computer* (PC), etc.). A OBU e a AU ligam-se normalmente através de cabo (*Ethernet*, por exemplo), mas podem também comunicar através de uma ligação sem fios, utilizando por exemplo a tecnologia *Bluetooth*. De salientar também que estas duas unidades, apesar de terem funções diferentes, podem estar integradas na mesma unidade física.

O domínio *ad-hoc* é composto pelas RSUs e pelos veículos equipados com OBUs. Estas duas unidades podem ser vistas como nós de uma rede *ad-hoc*, sendo as RSUs nós estáticos e as OBUs nós móveis.

No domínio da infraestrutura existem dois tipos de infraestruturas: as RSUs que permitem aos veículos aumentar a conetividade entre si, podendo também proporcionar o acesso à *Internet*; e os *hotspots* que permitem também a conexão das OBUs com a *Internet*. Caso um veículo esteja numa zona onde não existam RSUs ou *hotspots*, este pode ligar-se à *Internet* através de redes celulares, caso este esteja integrado na sua OBU.

2.2.4 Endereçamento

Nas VANETs, tal como em outras redes, a maioria das aplicações necessite de um esquema de endereçamento. Mohsin e Prakash [10] afirmam que um protocolo para atribuir endereços de IP deve cumprir os seguintes requerimentos:

- Não devem existir endereços de IP duplicados;
- Um endereço de IP deve ser atribuído a um nó apenas enquanto este se encontra na rede;
- Não devem ser negados endereços a novos nós que pretendam entrar na rede, isto é, se os endereços da rede não estiverem todos utilizados e um nó pretenda entrar na rede um endereço deve-lhe ser facultado;
- O protocolo deve estar preparado para lidar com redes particionadas;
- O protocolo deve garantir que apenas nós autorizados a entrar na rede conseguem um endereço IP.

Kihl [7] sugere que utilizem os mesmos esquemas de endereçamento que são utilizados nas MANETs, pois também nas VANET, os nós formam uma rede *ad-hoc*. De acordo com Chlamtac et al. [11] estes esquemas de endereçamento podem ser divididos em:

- **Endereçamento fixo** consiste em cada nó obter um endereço quando entra pela primeira vez na rede e mantém esse endereço até sair da rede. Este é o esquema de endereçamento mais comum na *Internet* e a maior parte das aplicações e protocolos existentes para redes *ad-hoc* assumem este esquema;
- **Endereçamento Geográfico** consiste em cada nó da rede obtém um endereço conforme a sua posição geográfica, alterando-se de acordo com o seu movimento. Para além da posição, o endereço pode também conter informações extra como: a direção em que o veículo se move; a identificação da estrada; o tipo de veículo (automóvel, camião, autocarro, etc.); características físicas do veículo; ou ainda caraterísticas sobre o condutor.

Como já foi referido, o tempo de conexão entre nós das VANETs pode ser bastante reduzido, consequentemente o tempo necessário para a obtenção de endereço de IP deve ser o menor possível. Fazio et al. [12] propõem um novo protocolo de endereçamento chamado *Vehicular Address Configuration* (VAC) que pretende aumentar a eficiência deste processo,

através eleição dinâmica de um "Líder"que atua como servidor de *Dynamic Host Configuration Protocol* (DHCP) para os outros veículos, reduzindo assim ocorrência de reconfigurações devido à elevada mobilidade da rede. Segundo os autores, este novo protocolo de endereçamento permite um *overhead* de sinalização e um tempo de configuração menor que os esquemas normalmente utilizados.

Nesargi e Prakash [13] abordam o problema do endereçamento em MANETs de forma distribuída, isto é, quando um nó pretende entrar na rede envia uma mensagem de *broadcast* para avisar os outros nós da rede que pretende um IP. Nessa altura, um nó propõe um IP e, se todos os nós aceitarem essa proposta, o IP é atribuído ao nó que pretende entrar na rede. Caso a proposta não seja aceite, o processo é repetido durante um número finito de vezes. Esta é uma solução que embora seja muito simples e fácil de implementar, poderá causar problemas de *flooding* na rede, pois para um novo nó ser aceite na rede é necessário todos os outros trocarem mensagens entre eles, o que em redes como as VANETs (que podem conter um grande número de veículos e estarem pouco tempo ligados à rede) vai originar uma grande troca de mensagem e consequentemente um *overhead* muito elevado.

Outra forma de se obter um endereço, é ser o próprio nó que pretende entrar na rede a escolher aleatoriamente um IP e depois ser utilizado um sistema de *Duplicate Address Detection* (DAD), sendo esta técnica denominada "*Best-Effort*". Vaidya [14] propõe uma solução, que em conjunto com a solução proposta em [10], chamada "*weak*"DAD, tem como objetivo prevenir que os pacotes sejam entregues ao nó "errado"mesmo que existam endereços duplicados na rede. Segundo os autores, esta solução apresenta melhorias de desempenho face às outras soluções baseadas em DAD, pois estas utilizam um esquema de *timeouts* que não é adequado para redes em que o atraso dos pacotes seja limitado como, é o caso das mensagens de segurança nas VANETs.

2.3 Tecnologia de Acesso à Rede

2.3.1 Espetro alocado a *Dedicated Short-Range Communications*

Como já foi referido anteriormente, em 1999 a FCC alocou 75 MHz do espetro nos 5.9 GHz para comunicações V2V e V2I, sendo o principal objetivo melhorar a segurança e o tráfego rodoviário. Foram também tidos em conta outro tipo de serviços privados (como o acesso à *Internet*), por forma a dividir os custos de desenvolvimento e encorajar um rápido desenvolvimento e adoção destas tecnologias.

Tabela 2.1: Espetro da banda DSRC

Número do canal	172	174	176	178	180	182	184
Tipo de canal	SCH	SCH	SCH	CCH	SCH	SCH	SCH
Frequência (GHz)	5.86	5.87	5.88	5.89	5.90	5.91	5.92

Como se pode ver na Tabela 2.1 o espetro DSRC está dividido em sete canais de 10 MHz. O canal 178 é o *Control Channel* (CCH) e está reservado para comunicações de segurança, enquanto os restantes canais são classificados como *Service Channel* (SCH), sendo destinados a todo o tipo de comunicações, segurança e entretenimento.

A banda DSRC é livre mas licenciada, isto é, não é cobrada nenhuma taxa pela sua utilização, mas esta não pode ser utilizada como as bandas dos 2.4 GHz e dos 5 GHz onde não existem restrições nas tecnologias utilizadas, apenas a potência de emissão e algumas regras de coexistência de tecnologias.

Esforços semelhantes foram feitos noutras partes do mundo, na Europa as bandas de 5795-5815 MHz e de 5875-5905 MHz [15] é reservada para comunicações de segurança rodoviária, tendo 20 MHz acima desta banda para extensões futuras, e o espetro 5855-5875 *MHz* é reservado para aplicações não relacionadas com segurança. Também no Japão foi reservada uma banda para DSRC, mais concretamente a banda de 5.770 a 5.850 MHz

2.3.2 Normas WAVE

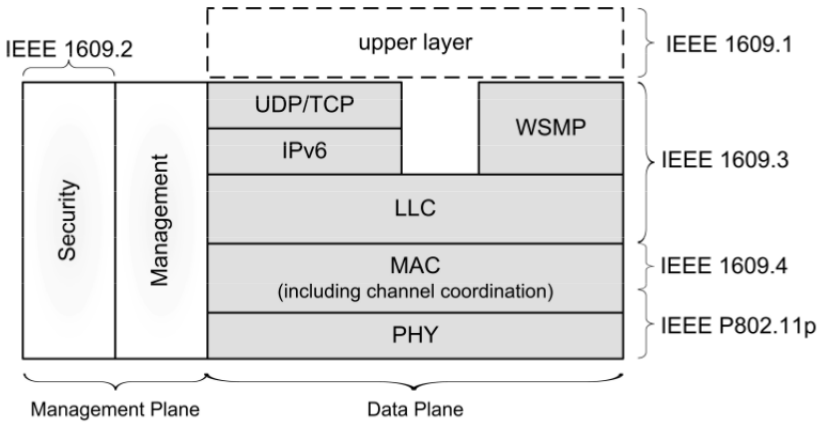


Figura 2.3: Pilha protocolar das normas WAVE (fonte: [16])

Para fazer face às caraterísticas e necessidades das VANETs, o IEEE desenvolveu esforços para criar uma nova série de normas, denominadas por normas WAVE, especialmente de-

senvolvidos para redes veiculares. Estas normas são compostos por: IEEE 802.11p e IEEE 1609.X. O IEEE 802.11p [17] foca-se nas camadas inferiores: *Physical Layer* (PHY) e MAC. Enquanto o IEEE 1609.X [18] lida com a camada MAC e com as camadas superiores.

Como se pode observar na figura 2.3, as normas WAVE suportam duas pilhas protocolares: a tradicional *Internet Protocol version 6* (IPv6) e a WAVE *Short-Message Protocol* (WSMP). desenvolvida especificamente para estas normas. A razão para a existência destas duas pilhas protocolares é oferecer a capacidade de acomodar mensagens com alta prioridade e altas restrições de latências (mensagens de segurança), com as mensagens comuns a outras redes.

A Tabela 2.2 apresenta as principais normas que constituem a WAVE e os seus principais objetivos.

Tabela 2.2: Descrição das normas WAVE (adaptado de [19])

Norma	**Protocolo**	**Propósito**
IEEE 802.11p	WAVE PHY e MAC	Especifica as funções exigidas ao nível PHY e MAC, para um dispositivo IEEE 802.11 poder trabalhar no ambiente variando rapidamente de veículos
IEEE 1609.1	Gestor de recursos WAVE	Descreve uma aplicação que permite a ma OBU, com recursos computacionais limitados e processos complexos de funcionamento, os possa executar fora dela, a fim de dar a impressão de estes são executados na OBU
IEEE 1609.2	Serviços de segurança WAVE	Trata do formato das mensagens de segurança e do seu processamento
IEEE 1609.3	Serviços de rede WAVE	Trata do endereçamento e encaminhamento nos sistemas WAVE
IEEE 1609.4	Operação em múltiplos canais	Fornece melhorias à camada de ligação de dados do IEEE 802.11p, de forma a ser possível a operação múltiplos canais

2.3.2.1 IEEE 802.11p

A norma IEEE 802.11p foi criada através do ajuste da norma IEEE 802.11a por forma a se obterem operações com *overhead* reduzido na banda DSRC.

A norma IEEE 802.11p, de acordo com Jiang e Delgrossi [20], tem como objetivos:

- Executar as funções e serviços requeridas pelas estações WAVE que encontram num ambiente que varia rapidamente e trocar mensagens sem ser necessário a associação a um *Basic Service Set* (BSS);
- Definir as técnicas de sinalização WAVE e as funções da *interface* que são controladas pelo MAC do IEEE 802.11.

Ainda de acordo com Jiang e Delgrossi [20], foram feitas três alterações, para além da alteração da frequência dos 5 GHz para os 5.9 GHz, na camada PHY do IEEE 802.11a por forma a torna-la mais ajustada às necessidades das comunicações veiculares. Estas alterações foram:

- **Canais de 10 *MHz***, pois com canais de 20 MHz o tempo de guarda pode não ser suficiente para interferência inter-símbolos. Cheng et al. [21] efetuaram um estudo aprofundado sobre este assunto e chega à conclusão que a escolha mais correta são canais com 10 *MHz*;
- **Requisitos de desempenho melhorados no recetor**, sobretudo com a introdução de melhorias na rejeição de canais adjacentes;
- **Máscara de transmissão melhorada**, esta é mais rigorosa do que a exigida pelo IEEE 802.11a.

Depois de definida a norma foram feitos vários estudos sobre o desempenho da mesma, de seguida serão mostrados alguns resultados e conclusões mais importantes retiradas desses estudos.

Wang et al. [22] utilizam o simulador *Network Simulator 2* (NS-2) [23] para estudar o comportamento da camada MAC focando-se nas comunicações V2I. Concluíram que utilizando o sistema de janelas de tamanho fixo, presente na norma, vão existir problemas ao nível do *throughput* nas condições dinâmicas das redes veiculares. Para resolver este problema são apresentados dois algoritmos (algoritmo centralizado e algoritmo distribuído) para melhorar o protocolo e aumentar o *throughput*. O algoritmo centralizado assume que as RSUs sabem o número de veículos para o qual querem transmitir e calcula a probabilidade de transmissão ótima de forma a aumentar o *throughput*. No algoritmo distribuído cada veículo necessita da informação local e calcula o tempo de *backoff* dependendo das condições do canal. Simulações realizadas com os dois algoritmos revelam melhorias significativas na norma IEEE 802.11p.

Já Eichler [24] realiza um estudo sobre o desempenho da norma, onde se conclui que em cenários com uma grande densidade de veículos e devido ao problema referido anteriormente

e acentuado pelo facto existir uma troca constante entre o SCH e o CCH pode levar a que as mensagens de segurança não sejam entregues em tempo útil. Este propõe que se utilize algo semelhante ao proposto por Kosch et al. [25], de maneira a reduzir o número de mensagens de alta prioridade para prevenir longas filas de espera. Este mecanismo baseia-se em atribuir relevância às mensagens: a relevância de uma mensagem é calculada por estimação do benefício que o nó recetor irá ter. Stibor et al. [26] avaliam o número de potenciais nós em comunicação e o máximo tempo de comunicação entre eles, utilizando um cenário de autoestrada, conclui-se que o número de veículos vizinhos é um importante parâmetro de entrada em algoritmos de escolha do próximo transmissor em cenário de comunicação *multi-hop*.

Um estudo sobre a camada MAC foi realizado por Bilstrup et al. [27], concluindo-se que utilizando um sistema de *Sense Multiple Access* (CSMA) em condições de alta densidade de tráfego leva a uma grande degradação do desempenho das comunicações, chegando a existir perdas de pacotes da ordem dos 80%. Neste artigo estuda-se também o esquema *Self-Organized Time Division Multiple Access* (STDMA), verificando-se que este apresenta uma melhoria de desempenho em relação ao esquema CSMA.

Alasmary e Zhuang [28] analisam o impacto de mobilidade no desempenho da camada MAC num cenário sem infraestrutura, concluindo que a velocidade relativa entre nós tem um grande impacto no acesso ao canal por parte da camada MAC. Neste estudo são propostos dois sistemas de prioridade dinâmica para reduzir a contenção e melhorar o *Packet Delivery Ratio* (PDR), simulações efetuadas utilizando NS-2 mostraram uma melhoria ao nível do PDR e do número médio de retransmissões por pacote. Uma avaliação das potencialidades de comunicações do IEEE 802.11p é realizada por Neves et al. [29], onde é realizado um estudo sobre o alcance de comunicação em cenário real, concluindo-se que se podem obter comunicações até distâncias de mais de 1 km se os veículos estiverem em linha de vista e cerca de 100 m se os veículos não se encontrarem em linha de vista.

2.3.2.2 Operação em múltiplos canais

A norma IEEE 1609.4 é responsável pelas operações em canais múltiplos. Esta define intervalos de utilização para o CCH e SCH, que normalmente correspondem a iguais intervalos de 50 milissegundos para cada canal. No entanto, tal como se pode observar na figura 2.4, existem quatro formas distintas de comutação: (a) acesso contínuo (apenas se utiliza o canal de controlo), (b) acesso alternado (comutação entre CCH e SCH a cada 50 ms), (c) acesso imediato ao canal de serviço (dá-se a comutação imediata para o canal de serviço antes de

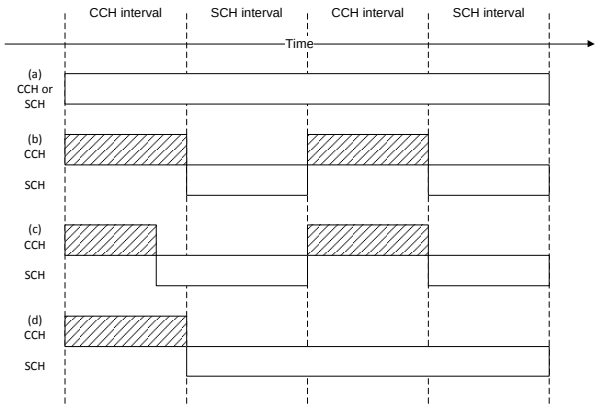


Figura 2.4: Formas de Acesso ao Canal: (a) contínuo, (b) alternado, (c) imediato e (d) estendido

acabar o intervalo do canal de controlo) e (d) acesso estendido (o aparelho ficar durante um certo período de tempo apenas no SCH).

Para que se possam obter comunicações fiáveis é necessário que todos os dispositivos WAVE se encontrem sincronizados, para tal a norma define que os veículos devem estar sincronizados recorrendo a informação proveniente no sinal GPS. No entanto, caso os veículos não disponham deste sistema terá de se sincronizar através de informações provenientes de outros veículos.

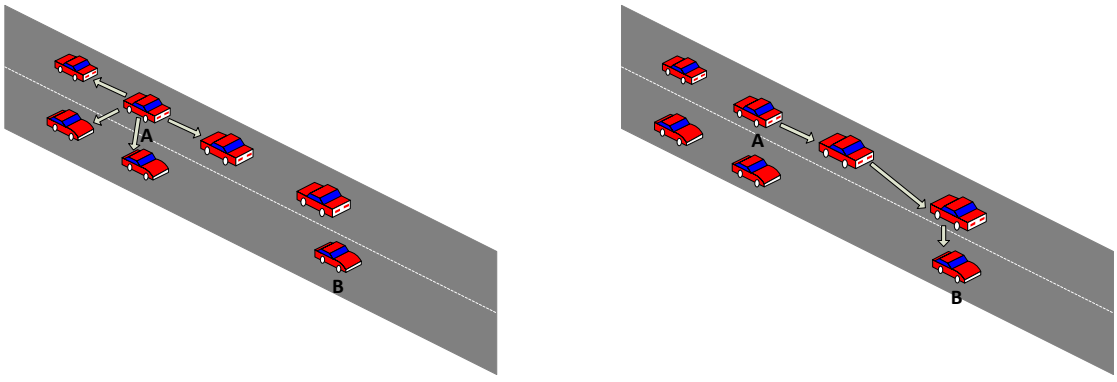
Assim que um nó entra numa rede IEEE 802.11p/1609 deve operar no CCH, de modo a adquirir as informações necessárias. Os nós pertencentes a uma rede IEEE 802.11p/1609 formam uma *Wave-mode Basic Service Set* (WBSS). O nó que inicia a WBSS denomina-se WBSS *provider*, enquanto os nós que se juntam à mesma denominam-se WBSS *user*. Para estabelecer esta rede, o WBSS *provider* envia periodicamente mensagens WAVE *Service Announcement* (WSA) no canal de controlo, estas contém as informações necessárias (por exemplo: o identificador da WBSS e o número do canal de serviço utilizado). Depois de receberem as mensagens WSA, os WBSS *user* podem entrar na WBSS, efetuando a comutação entre o CCH e o SCH utilizado na WBSS.

A operação em múltiplos canais tem sido um tema bastante abordado na literatura, se seguida serão apresentados os principais estudos na área. Devido à comutação de canais existente, Wang et al. [30] detetaram um problema de desperdício de recursos, que denominaram de "*bandwidth wastage problem*". Para fazer face a este problema propõe dois novos esquemas de transmissão, os resultados obtidos mostram melhorias na taxa de transmissão obtida.

Também Du et al. [16] se focam neste problema, propondo uma melhoria a um dos esquemas apresentados pelo estudo anterior, concluindo-se que as alterações introduzidas melhoram a taxa transmissão em situações de comutação de canal. Grafling et al. [31] efetuam simulações das normas WAVE em ambiente veicular, concluindo que é possível obter comunicações (no canal de controlo) com pouca latência se a utilização do canal for inferior a 1000 pacotes por segundo. Por fim, Ameixieira et al. [32] concluem, através de uma implementação prática das normas IEEE 802.11p/1609.X, que não existe aumento na latência de mensagens de segurança (transmitidas no CCH), mesmo quando se verifica grande congestionamento no SCH utilizado.

2.4 Disseminação de Informação

Como já foi visto anteriormente, as redes veiculares têm a particularidade de ter que se adaptar a diferentes densidades de nós, desde grandes densidades em áreas urbanas ou autoestrada em hora de ponta, a densidades muito baixas em zonas rurais. Assim é necessário o desenvolvimento de algoritmos de disseminação de informação, uma vez que as aplicações de segurança têm restrições de latência muito apertadas. Têm então, que existir mecanismos que garantam a entrega destas mensagens em tempo útil.



(a) *Disseminação de informação em broadcast e single-hop*

(b) *Disseminação de informação em unicast e multihop*

Figura 2.5: Esquemas de disseminação de informação

A disseminação de informação nas VANETs pode ser feita através de *single-hop* ou *multihop*. O esquema *single-hop* é geralmente implementado utilizando *broadcast* ao nível da camada MAC, como se pode ver na Figura 2.5(a), o veículo A envia mensagens para todos os

veículos que estão no seu alcance, mas como o veículo B não está a mensagem não lhe será entregue. A disseminação *single-hop* pode também ser utilizada caso existam RSUs, mas não terá de ser obrigatório, pois um veículo pode utilizar outro como *relay* para comunicar com uma RSU. A propagação de informação *multihop* deverá ser a mais comum em VANETs. Nesta os dados serão propagados através de vários veículos entre o emissor e recetor, como se pode observar na Figura 2.5(b). De notar que para ser implementado um esquema *multihop* é necessário que exista um mecanismo de encaminhamento na rede, estes mecanismos vão ser abordados mais adiante, na Secção 2.5.

A propagação de informação pode também ser classificada segundo o número de destinatários a que uma mensagem pretende chegar. Assim tem-se: *unicast* se a mensagem é apenas destinada a um nó, *multicast* se a mensagem tem vários destinatários e *broadcast* se a mensagem é destinada a todos os nós da rede. As mensagens transmitidas em *unicast* serão sobretudo mensagens correspondeste a aplicações de lazer (transmissão de vídeo, jogos, acesso a conteúdos na *Internet*, etc.). As mensagens *multicast* são geralmente destinadas a um grupo específico dentro da rede (por exemplo, supondo que um troço de estrada se encontra em obras apenas num sentido, seriam enviadas mensagens de aviso em *multicast* para todos os veículos que circulassem nesse sentido, mas não seria necessário os veículos que circulam no sentido oposto receber essas mensagens). Por fim, existe a transmissão em *broadcast* que, como já foi referido anteriormente, aplica-se sobretudo em mensagens de segurança. No entanto, como as VANETs podem tornar-se redes globais, estas mensagens de segurança podem ser relevantes apenas para uma certa zona. Kremer [33] introduziu o conceito de *Zone-Of-Relevance* (ZOR), que basicamente consiste na atribuição de uma zona onde uma certa mensagem é importante e as mensagens de *broadcast* destinam-se apenas aos veículos que se situam nessa determinada zona.

A disseminação da informação tem sido um tema bastante estudado e, de seguida, serão apresentadas algumas conclusões e possíveis melhorias propostas. Torrent-Moreno et al. [34] analisam a probabilidade de receção de mensagens enviadas em *broadcast* num cenário em que as VANETs estão completamente difundidas e a rede está constantemente a operar no estado de saturação. Concluindo que a probabilidade de entrega de mensagens será na ordem de 20% a 30% para distâncias de 100 m e ainda mais pequenas para distâncias maiores. Assim, concluem que é necessário um esquema de atribuição de prioridades. Um possível problema na propagação de informação em redes *ad-hoc* é o fenómeno de *broadcast storm* identificado por Ni et al. [35]: como os sinais rádio muitas vezes se sobrepõem na mesma área,

uma transmissão em *broadcast* não pode ser realizada através do simples método de *flooding* pois isto iria resultar em bastante redundância, contenção e colisões. Neste estudo é ainda apresentado um esquema de propagação baseado na posição geográfica dos nós que, segundo os autores, reduz em grande parte este problema. Um outro mecanismo de transmissão em *broadcast*, para fazer face ao problema de *broadcast storm*, é apresentado por ALshaer e Horlait [36]: neste esquema é proposto que os veículos retransmitam as mensagens de *broadcast* com uma certa probabilidade calculada dinamicamente, baseada na densidade de veículos presentes na zona. Outra abordagem a este problema foi analisada por Nekovee e Bogason [37]: neste artigo é proposto um novo protocolo de disseminação de informação num cenário altamente dinâmico e com conetividade intermitente. Através de simulações os autores concluem que podem ter uma taxa de entrega de mensagens de 100%. O problema da propagação de informação em condições em que nem sempre existe conetividade com a rede foi estudado em [38]. Aqui Kitani et al. propõem um esquema de transporte de mensagens chamado "*ferrying technique*". Este consiste em dividir os veículos em duas categorias: *regular nodes* e *message ferries*. Os *regular nodes* são nós que se movem livremente, enquanto os *message ferries* circulam por rotas específicas (autocarros, por exemplo). Estes são utilizados para o transporte da informação partes da rede que não teriam conexão de outra forma. Segundo os autores, o esquema proposto pode melhorar a entrega de mensagens em cerca de 50% em cenários de pouca densidade de veículos. Grossglauser e Tse [39] apresentam um estudo interessante em que é aproveitada a mobilidade dos nós da rede para aumentar a taxa de transmissão. Para isso, sugerem que os nós em vez de terem apenas uma rota entre eles possam utilizar várias, através de simulações mostram que com rotas com dois saltos são suficientes para conseguir a taxa de transmissão máximo dentro dos limites de interferência impostos. No entanto, este esquema tem o problema de se obterem atrasos elevados na transmissão.

Em todos os trabalhos referidos anteriormente são estudados cenários em que apenas se considera comunicação V2V. No entanto, existem também estudos que contemplam a utilização de RSUs. Wischhof et al. [40] propõem que as RSUs possam servir para ligar grupos de veículos isolados. Neste sistema, um veículo que receba uma mensagem reencaminha-a para a RSU mais próxima e esse então faz o *broadcast* para todos os veículos pertencentes a essa ZOR. Desta forma os veículos não iriam transmitir mensagens em *broadcast* e deixa de existir o problema de *broadcast storm*. Tanto Lochert et al. [41] como Li et al. [42] estudam a forma ideal de colocar as RSUs através de algoritmos de análise geográfica calculam o local em que

estas irão maximizar a disseminação da informação. Finalmente, Reis et al. [43] efetuam uma análise ao impacto que a colocação de RSUs têm no *re-healing time* (tempo requerido para transmitir informações entre origem e destino em uma estrada de duas vias cenário) e conclui-se que a introdução de RSUs reduz significativamente este tempo, especialmente se estas tiverem ligação entre elas.

2.5 Protocolos de encaminhamento

A comunicação em redes veiculares pode ser feita através de caminhos com mais de um salto, tornando-se necessário que exista um protocolo que possa escolher o melhor caminho entre a fonte e do destino da informação. Dada a natureza específica das VANETs, já referida neste texto, este protocolo tem particularidades específicas mesmo em comparação com os protocolos de encaminhamento já desenvolvidos para as MANET. Assim, os protocolos de encaminhamento têm sido um dos principais focos de investigação nesta área. Face às caraterísticas apresentadas em 2.2.1, os protocolos de encaminhamento, segundo Francisco J. Ros e Ruiz [44], terão os seguintes desafios e requisitos:

- **Operação localizada** - As VANETs são redes com grande escalabilidade, logo é necessário que os protocolos de encaminhamento tomem decisões baseados apenas na informação local, caso contrário irá existir um grande aumento do *overhead* introduzido pelo protocolo;
- **Descoberta de vizinhos** - A descoberta de novos vizinhos é uma parte fundamental dos protocolos de encaminhamento. Maioritariamente utilizam um esquema de envio de mensagens de controlo, daí que o intervalo de envio destas mensagens deva ser estudado de forma a obter um bom compromisso entre a rapidez de descoberta e o *overhead* introduzido;
- **Identificação do destino** - Os protocolos de encaminhamento têm que estar preparados para ter como destino, não só um nó específico, como por vezes uma área ou posição geográfica;
- **Previsão da trajetória** - Os protocolos de encaminhamento devem utilizar a trajetória dos pacotes como uma vantagem na disseminação dos mesmos;
- **Transmissão de dados** - Em vez de criarem tabelas com o próximo salto os protocolos de encaminhamento para VANETs devem encaminhar os dados, pacote a pacote, baseado na vizinhança corrente;

- **Capacidade para lidar com rede particionada** - Os protocolos devem estar preparados para guardar uma mensagem até surgir um novo salto (*store-carry-forward*);
- **Previsão de eventos futuros** - Tendo acesso a informações como velocidade, posição e trajetória os protocolos devem estar preparados para prever a posição futura dos veículos e, assim, melhorar o encaminhamento dos pacotes;
- **Uso de informações adicionais** - Os protocolos devem ser capazes de utilizar informações disponíveis, como o *software* de navegação ou informação sobre o estado do trânsito para tornar mais eficiente o encaminhamento da informação.

Tabela 2.3: Classificação dos vários protocolos de encaminhamento (fonte:[45])

	Tipo de comunicação				
	Unicast		*Multicast*		*Broadcast*
Tipo de Rede	Topologia	Posição	Geocast	Mobilidade	
Redes Dispersas		Epidemic MDDV VADD		Epidemic MDDV VADD	Epidemic
Gerais	AODV DSR OLSR Fast OLSR	DREAM GSR MGF MORA MURU	DRG GAMER IVG LBM MGF	RBM VTRADE	DREAM
Redes Densas	CBRP HSR	CAR LORA-CBF GPCR GPSR	GeoGRID	LBF OABS ODAM SB SOTIS UMB	

Os protocolos de encaminhamento específicos para redes veiculares podem ser classificados, de acordo com Ducourthial e Khaled [45], em cinco categorias: protocolos baseados na topologia, protocolos baseados na posição geográfica, protocolos hierárquicos, protocolos baseados no movimento e finalmente protocolos específicos para transmissão em *broadcast*. Para além desta classificação, os protocolos podem também ser classificados segundo o tipo

de comunicações a que se destinam: *unicast, multicast* ou *broadcast*, ou em relação ao tipo de redes, se estas são redes dispersas, normais ou densas. A Tabela 2.3 agrupa os vários protocolos existentes segundo estas classificações.

Apesar de ser consensual entre a comunidade científica que os protocolos geográficos são mais adequados a VANETs em relação aos protocolos baseados na topologia, os protocolos geográficos ainda estão numa fase de desenvolvimento não estando disponíveis para a plataforma *Linux*, utilizada no projeto DRIVE-IN. Neste sentido, vai ser dado mais destaque aos protocolos baseados na topologia, pois são estes os utilizados neste projeto, não sendo o foco do trabalho o desenvolvimento de novos protocolos.

2.5.1 Protocolos baseados na topologia

Os protocolos de encaminhamento baseados na topologia utilizam a informação sobre as ligações existentes na rede para fazer o encaminhamento dos pacotes através da rede. Estes protocolos podem ser divididos em protocolos proativos e reativos.

Os protocolos proativos mantêm constantemente a sua tabela de encaminhamento atualizada mesmo que não existam pedidos de comunicação, para isso enviam constantemente pacotes de controlo. A vantagem destes protocolos reside no facto de quando um nó quer enviar uma mensagem, como as rotas já estão criadas, não existe a necessidade de procurar essa rota, reduzindo assim o tempo de entrega dos pacotes; a desvantagem é o enorme *overhead* que o protocolo introduz na rede. Por outro lado, os protocolos reativos apenas criam uma rota quando esta é necessária, isto é, quando um nó tem uma mensagem para enviar para outro, sendo esta mantida durante um período de tempo pré-determinado. Estes protocolos têm a vantagem de introduzirem pouco *overhead* na rede, mas como contrapartida aumentam o atraso na entrega dos pacotes. Os protocolos reativos apresentam melhor desempenho em redes com pouca densidade de nós, alta mobilidade e elevadas interrupções na ligação da rede (ambientes de autoestrada), enquanto os protocolos proativos adaptam-se melhor a rede com pouca mobilidade e alta densidade de nós (ambientes urbanos ou autoestrada em hora de ponta).

Em seguida vão ser explicados ao pormenor os seguintes protocolos de encaminhamento: AODV, OLSR, B.A.T.M.A.N. e BABEL.

2.5.1.1 AODV

O protocolo *Ad-hoc On-Demand Distance Vector* (AODV) [46] foi criado especificamente para redes *ad-hoc* com grande mobilidade. O AODV é um protocolo reativo, ou seja, quando um nó pretende enviar uma mensagem é iniciado o processo de descoberta da rota. Para isso, o nó que pretende transmitir envia uma mensagem de *Route REQuest* (RREQ) para todos os nós no seu alcance (como se pode ver na figura 2.6(a)) e estes fazem o mesmo processo e guardam o endereço do nó que lhes enviou a mensagem, este processo repete-se até as mensagens de RREQ chegarem ao nó pretendido. Quando isto acontece é enviado uma mensagem de *Route REPly* (RREP) pelo caminho previamente descoberto, como se pode observar na Figura 2.6(b). Este processo denomina-se *backward learning*. Assim que uma nova rota é estabelecida esta é mantida enquanto a fonte necessitar da mesma. Caso um nó intermédio se mova e seja detetada a quebra da rota, é difundida uma mensagem de *Route ERRor* (RERR) que serve para informar que a rota deve ser descartada e deve ser iniciado o processo de descoberta de nova rota entre a fonte e o destino.

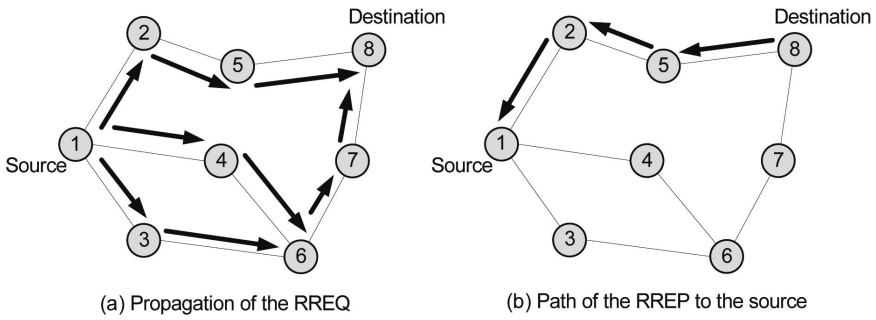


Figura 2.6: Processo de descoberta de nova rota utilizado pelo AODV (fonte:[8])

As principais caraterísticas deste protocolo são:

- Os nós apenas guardam as rotas que são necessárias;
- Minimiza o envio de mensagens de *broadcast* e assim o *overhead*;
- Reduz os requisitos de memória;
- Rápida reposta a quebra de ligações em rotas ativas;
- Rotas isentas de ciclos;
- Escalável a redes com grande densidade de nós.

A principal desvantagem deste protocolo é o aumento que este introduz no tempo de entrega dos pacotes.

2.5.1.2 OLSR

O *Optimized Link State Routing Protocol* (OLSR) [47] é um protocolo proativo com encaminhamento do tipo "*link state*", isto é, cada nó constrói um mapa da conectividade da rede, sob a forma de um grafo, que mostra quais os nós que têm conectividade entre si. Assim, cada nó calcula independentemente o melhor caminho para cada destino possível na rede e os melhores caminhos formam a tabela de encaminhamento.

Para criar as tabelas de encaminhamento cada nó faz o *broadcast* de uma mensagem HELLO para todos os seus vizinhos a um salto, sendo que esta mensagem não é reenviada para nós mais distantes. Esta mensagem de HELLO permite que cada nó tome conhecimento dos seus vizinhos a dois saltos e com base nesta informação cada nó seleciona os seus *Multipoint Relay*s (MPRs) (nó que situado a um salto oferece melhor rota para nós a dois saltos). Para além das mensagens de HELLO o OLSR utiliza mensagens *Topology Control* (TC) em que cada nó declara o seu MPR *Selector*, isto é, a mensagem contém a lista de vizinhos que escolheram o nó como MPR.

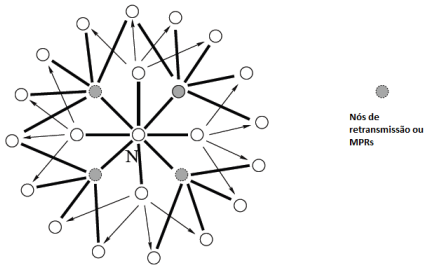


Figura 2.7: *Multipoint Relay* (fonte:[47])

A Figura 2.7 mostra o funcionamento dos MPRs. Como se pode observar, o nó central escolhe os seus MPRs, que são os nós que lhe oferecem melhor rota para os nós situados a dois saltos de distância.

A principal vantagem do OLSR é o facto de, por ser um protocolo proativo, em cada instante cada nó da rede ter uma rota para todos os outros nós, reduzindo assim o atraso na entrega de mensagens. O OLSR adapta-se bem a redes com grande densidade de nós, onde a conectividade é bastante frequente e existe um número bastante elevado de nós.

O principal problema do OLSR é não tomar em atenção a qualidade das ligações, o que pode ser uma grande desvantagem em redes sem fios, pois uma ligação pode existir, mas a sua qualidade ser bastante baixa, sendo que os pacotes que forem encaminhados pela rota que contém essa ligação poderão sofrer uma grande taxa de perdas e aumento no atraso.

2.5.1.3 B.A.T.M.A.N.

O *Better Approach To Mobile Ad-hoc Networking* (B.A.T.M.A.N.), proposto por Neumann et al. [48], é um protocolo proativo baseado no paradigma *distance-vector*, isto é, a sua estratégia passa por determinar para cada destino na rede, qual o melhor próximo salto para esse destino. Assim, para atingir este objetivo todos os nós da rede fazem o *broadcast* de *Originator Message*s (OGMs); quando um nó recebe uma OGM, altera o endereço de envio para o seu e reenvia a mensagem caso a OGM tenha sido originado por um nó a um salto de distância ou, caso a OGM tenha sido enviada por um nó considerado o melhor próximo salto para o nó gerador. Para identificar o melhor próximo salto para um determinado destino, um nó conta o número de OGMs originados por esse destino e recebido de diferentes nós. Assim, o nó seleciona para próximo salto o vizinho que do qual recebeu mais OGMs durante um certo período de tempo (janela deslizante), desta forma um nó não mantém a rota completa para cada destino, mas apenas o melhor salto para chegar a esse destino.

Annese et al. [49] estuda o comportamento do protocolo e verifica que este pode ter falhas em certas circunstâncias, devido ao facto de contar o número de OGMs recebidas durante uma janela deslizante para encontrar qual o melhor próximo salto. O problema surge porque durante esta janela deslizante todos os OGMs têm o mesmo peso, isto é, OGMs antigas ou recentes são consideradas da mesma forma, e em cenários de alta mobilidade isto pode levar a que existam ciclos. Neste mesmo trabalho, é proposta uma alteração ao protocolo, chamada *smart window*-B.A.T.M.A.N., que basicamente consiste em alterar o peso das mensagens OGM, fazendo com que mensagens mais antigas tenham menos peso que mensagens mais recentes.

O B.A.T.M.A.N. como é um protocolo proativo apresenta conceptualmente as mesmas vantagens do OLSR, sendo a sua grande desvantagem também está relacionada com o facto de ser um protocolo proativo e assim manter constantemente rotas entre todos os nós da rede causando um grande *overhead*. Uma comparação mais detalhada sobre o desempenho dos vários protocolos de encaminhamento será feita mais à frente na Secção 2.5.5

2.5.1.4 BABEL

O BABEL [50] é um protocolo de encaminhamento proativo e baseado em *distance-vector*, tal como o protocolo B.A.T.M.A.N., e foi criado a pensar em redes quer com fios, quer sem fios. O principal foco de atenção deste protocolo é criar rotas livres de ciclos, mesmo em redes altamente dinâmicas, o que nem sempre acontece em protocolos baseados em *distance-vector*.

Assim, quando é detetada uma alteração na rede, o protocolo tenta rapidamente encontrar uma nova rota, mesmo que esta não seja a melhor, utilizando depois uma técnica denominada *sequenced routes* para convergir para a melhor rota possível.

Uma das principais vantagens deste protocolo para as redes veiculares está relacionada com o facto de o protocolo ter suporte para *link quality*, sendo este um aspeto fundamental em VANETs pois, devido às caraterísticas destas redes, a escolha da rota com melhor qualidade entre ligações é bastante importante. Outra característica que distingue este protocolo é estar preparado para suportar *Internet Protocol version 4* (IPv4) e IPv6 em simultâneo. Em redes em que coexistam as duas versões do protocolo IP, são poupados grandes recursos na rede, tanto ao nível de computação (pois não é necessário ter dois protocolos, ou duas instâncias do mesmo protocolo), como ao nível do *overhead* introduzido na rede (pois o protocolo utiliza os mesmos pacotes de controlo para anunciar as rotas IPv4 e IPv6).

O BABEL tem duas desvantagens importantes: a primeira está relacionada com o facto de o protocolo depender de atualizações periódicas das suas tabelas de encaminhamento; para redes com pouca mobilidade, cria um *overhead* superior a outros protocolos, mas como em redes veiculares existe uma grande mobilidade este acaba por não ser um grande problema para o caso em estudo. A segunda desvantagem é a imposição de um tempo de espera quando um endereço é retirado, assim quando um endereço que abandonou a rede volta a pretender entrar na rede vai ser necessário esperar, até que o protocolo o volte a ter em consideração. Devido a este problema o BABEL não é aconselhável a redes móveis com agregação automática de endereços.

2.5.2 Protocolos Baseados na Posição Geográfica

Os protocolos de encaminhamento baseados na posição geográfica tomam as decisões sobre o encaminhamento de acordo com a posição do destino do pacote e dos vizinhos a um salto. A posição do destino dos pacotes é guardada no cabeçalho dos pacotes pela fonte de informação e a posição dos vizinhos é obtida através da troca de *beacons*. Como os protocolos baseados na posição não trocam mensagens de estabelecimento de rotas, podem ser mais promissores que os protocolos baseados na topologia de rede para redes com alta mobilidade, como é o caso das VANETs. Por outro lado, em casos onde a velocidade dos nós é bastante elevada, a posição destes muda muito rapidamente, podendo levar a problemas com o encaminhamento dos dados. Para fazer face a este problema, os pacotes terão de ser destinados a uma determinada área e não a uma posição.

2.5.3 Protocolos Hierárquicos

Os protocolos hierárquicos assumem que a rede é composta por vários *clusters* (define-se *cluster* como um determinado número de nós ligado durante um certo intervalo de tempo). O encaminhamento dos pacotes é feito de *cluster* em *cluster* através de nós que estejam integrados em mais de um *cluster* no mesmo instante.

Estes protocolos têm a desvantagem de aumentar o *overhead* introduzido na rede proporcionalmente ao aumento da mobilidade da rede. Assim, estes protocolos não devem ser utilizados de forma isolada, mas sim em cenários específicos com outros tipos de protocolos de forma a se otimizar o encaminhamento dos pacotes.

2.5.4 Protocolos Baseados no Movimento

Nos protocolos baseados no movimento, as mensagens são transportadas pelos nós até ao seu destino, isto é, um nó recebe uma mensagem e vai guardá-la até se encontrar no raio de alcance do nó de destino. Tal como os protocolos hierárquicos, este tipo de protocolos não se devem utilizar de forma isolada, mas sim os seus algoritmos integrados noutros protocolos para melhorar o seu desempenho.

2.5.5 Comparação de desempenho

Nas secções anteriores foi explicado o funcionamento dos diversos tipos de protocolos de encaminhamento existentes. Nesta secção vão ser apresentados alguns estudos comparativos sobre o desempenho dos vários tipos de protocolos de encaminhamento existentes para redes *ad-hoc*.

Jaap et al. [51] desenvolveram um simulador de mobilidade para cenários de autoestrada e, recorrendo ao simulador NS-2, fazem um estudo comparativo entre os protocolos AODV, *Dynamic Source Routing Protocol* (DSR), *Fisheye State Routing Protocol* (FSR) e *Temporally-Ordered Routing Algorithm* (TORA); os autores concluem que o protocolo AODV apresenta um desempenho superior aos restantes, sendo seguido pelo FSR. Tanto o FSR como o DSR apresentam um *overhead* bastante elevado em cenários com grande densidade de tráfego, e é concluído também que o protocolo TORA não é aplicável a redes veiculares. Haerri et al. [52], por outro lado, estudam o desempenho dos protocolos OLSR e AODV em ambiente urbano e, através das simulações realizadas, chegam à conclusão que o OLSR apresenta um desempenho superior ao nível de *overhead*, latência e tamanho das rotas. Apenas ao nível do PDR o AODV apresenta um desempenho superior em certas circunstâncias. Para além destas

conclusões, verificam também que a velocidade média dos veículos não afeta o desempenho dos protocolos. Os mesmos protocolos foram estudados também em ambiente urbano por Khan e Qayyum [53], confirmando as conclusões apresentadas pelo estudo anterior. Aqui também o OLSR apresenta um desempenho superior em comparação com o AODV, sendo outra conclusão importante que os dois protocolos apresentam um PDR bastante elevado.

Os estudos até aqui referidos baseiam-se todos em simulações para retirar conclusões sobre o desempenho dos vários protocolos de encaminhamento utilizados, contudo existem também estudos utilizando implementações práticas, mas apenas em MANETs. Apesar da mobilidade neste tipo de rede ser bastante inferior às redes veiculares é sempre possível retirar conclusões sobre o desempenho dos protocolos. De entre estes estudos destacam-se os trabalhos efetuados por Abolhasan et al. [54] e Murray et al. [55], onde ambos comparam o desempenho de três protocolos, OLSR, B.A.T.M.A.N. e BABEL. No primeiro, os autores concluem que o protocolo B.A.T.M.A.N. apresenta melhor estabilidade e melhor PDR, enquanto o BABEL oferece melhor largura de banda para comunicações *multi-hop* e um tempo de restauro de rotas mais baixo. Em todas as métricas estudadas, o OLSR apresenta um desempenho inferior aos outros. Já no segundo estudo as conclusões são ligeiramente diferentes: neste confirma-se que o BABEL oferece um *throughput* mais elevado, mas neste estudo os protocolos B.A.T.M.A.N. e OLSR apresentam desempenhos similares. Esta divergência de resultados mostra que serão necessários mais estudos práticos acerca do desempenho dos vários protocolos e seria também conveniente estes serem testados em redes veiculares para se perceber se se poderiam utilizar neste tipo de rede.

2.6 Mobilidade

As redes veiculares, como já foi referido em 2.2.1, têm uma série de caraterísticas únicas, uma das quais a sua elevada mobilidade, por isso a gestão da mobilidade em redes é um aspeto fulcral no seu desenvolvimento. Apesar do grande objetivo das VANETs ser o aumento da segurança nas estradas, através de comunicações V2V, é preciso também ter em conta as aplicações de conforto, que, como será explicado com mais detalhe na Secção 2.8.3, estão sobretudo direcionadas ao acesso à *Internet*, motivando uma rápida adoção das redes veiculares por parte dos utilizadores. Deste modo, torna-se necessário dotar os nós da rede da capacidade de manter o seu endereço de IP enquanto estes se deslocam entre as diversas redes disponíveis ao longo das estradas. De acordo com Zhu et al. [56], um protocolo de gestão de mobilidade para redes veiculares deve satisfazer os seguintes aspetos:

- **Mobilidade sem perdas** - As VANETs devem ser uma extensão transparente da *Internet*. Deste modo a mobilidade dos veículos deve ser escondida, isto é, se um *Internet Gateway* (IGW) está disponível, o veículo deve conseguir comunicar com a *Internet* independentemente da sua posição e da tecnologia de acesso à rede que está a utilizar;
- ***Handover* rápido e vertical** - *Handover* rápido é um aspeto essencial em redes veiculares, uma vez que devido à elevada mobilidade destas, um veículo passa pouco tempo ao alcance cada RSU. É também necessário ter em conta o *handover* vertical, pois os veículos podem estar equipados com diferentes tecnologias de acesso à rede;
- **Suporte IPv6** - Para garantir o acesso global é necessário um endereço de IP permanente por cada veículo;
- **Escalabilidade e eficiência** - As VANETs podem vir a acomodar milhares de veículos, assim o protocolo de mobilidade deve ser altamente escalável e eficiente em termos de *overhead* criado.

Com a proliferação das redes celulares e redes Wi-Fi surgiu a necessidade de adaptar a *Internet* para a mobilidade que estas redes proporcionam, para este efeito surgiu o MIPv6 [57]. Este protocolo tem como principal objetivo proporcionar a ligação sem perdas entre nós móveis e a *Internet*. Contudo, com o aumento das redes móveis percebeu-se que o MIPv6 tem algumas limitações, surgindo então novos protocolos como o *Hierarchical Mobile Internet Protocol version 6* (HMIPv6) [58] ou o *Fast Mobile Internet Protocol version 6* (FMIPv6) [59] por forma a melhorar os pontos fracos do MIPv6. O HMIPv6 adiciona um novo componente chamado *Mobility Anchor Point* (MAP), que controla a localização dos nós móveis, com esta adição é possível reduzir a latência de *handover*. O FMIPv6 propõe que o nó móvel realize o processo de *handover* de forma proativa, isto é, antes de perder conexão com um IGW o nó móvel deve procurar por um novo IGW e aí deve requerer a informação da *subnet*, desta forma é possível reduzir o tempo de *handover*. Para além destes protocolos baseados no MIPv6 existem ainda outros como o PMIPv6 [60] ou o *Locator/ID separation protocol* (LISP) [61].

A mobilidade em redes veiculares é ainda um tema pouco estudado existindo no entanto alguns trabalhos na área. Lee et al. [62] propõem um esquema de mobilidade baseado no PMIPv6, mas introduzem um novo elemento na rede, denominado *intermediate Mobile Access Gateway*, que o tempo de perda de ligação durante o processo de *handover* entre diferentes domínios. Para testar as melhorias implementadas ao protocolo PMIPv6, os autores realiza-

ram simulações usando um ambiente veicular. Os resultados obtidos mostram que o esquema proposto melhora a latência de *handover* e o número de pacotes perdidos, no entanto não providencia *handover* transparente. Chen et al. [63] propõem um protocolo *Network Mobility* (NEMO) para redes veiculares. Este permite a um veículo, quando deteta que está a sair do alcance de uma RSU, adquirir um endereço de IP da nova RSU antes de estar no alcance desta, recorrendo a comunicação com os veículos que circulam no sentido oposto. Segundo os autores, este esquema apresenta melhor desempenho que protocolo NEMO original. A utilização do NEMO é também estudada por Mussabbir et al. [64]: neste estudo o protocolo NEMO é utilizado como extensão do FMIPv6, sendo também utilizado o IEEE 802.21 *Media Independent Handover* (MIH) para auxiliar o processo de decisão. Neste artigo são realizadas simulações, em ambiente veicular, e conclui-se que a arquitetura escolhida apresenta melhor desempenho que qualquer um dos protocolos em separado. Os resultados apresentados mostras latências de *handover* de aproximadamente 500 ms para velocidades de 90 km/h.

Apesar destes estudos de sistemas de mobilidade em ambientes veiculares, faltam estudos que integrem os protocolos de mobilidade existentes com as normas IEEE 802.11p/1609.X, pois devido às caraterísticas desta, os protocolos de mobilidade deverão ter em conta essas caraterísticas.

2.6.1 MIPv6

O MIPv6 é um protocolo que opera ao nível da camada de rede do modelo *Open Systems Interconnection* (OSI) [65], ou seja, pode ser classificado como um protocolo da camada 3. Quando um nó móvel se move para uma rede diferente, o seu endereço irá ser inválido na nova rede, sendo aqui que o MIPv6 opera, permitindo ao nó móvel a obtenção de um endereço de IPv6 válido na rede a que este se ligou. O protocolo MIPv6 utiliza uma terminologia específica para as várias entidades introduzidas pelo mesmo. De seguida vão ser apresentadas estas entidades para que se possa ter uma melhor noção de qual a função de cada uma delas.

- ***Mobile Node*** - Um *host* ou *router* que altera o seu ponto de ligação de uma rede para outra, sem alterar o seu endereço;
- ***Home Agent*** - É um *router* na rede de origem do *Mobile Node* que direciona os pacotes para os MNs que se encontram fora da sua rede de origem. Mantém também a localização corrente de cada MN;
- ***Care-of-Address*** - É o nome dado ao endereço de IPv6 que o MN obtém na rede visitada. Este endereço é a terminação do túnel em direção ao MN;

- ***Home Address*** - É o endereço do MN, este mantém inalterado independentemente da rede a que o MN está ligado;
- ***Home Network*** - É a rede à qual o MN pertence, isto é, o seu prefixo corresponde com o prefixo da *Home Address*;
- ***Foreign Network*** - Qualquer rede que não a *Home Network* (HN) do MN;
- ***Correspondent Node*** - Nó com quem o MN está a comunicar.

2.6.1.1 Arquitetura

A Figura 2.8 ilustra a arquitetura do MIPv6 para que seja possível suportar mobilidade do MN entre a HN e as várias *Foreign Network*s (FNs). Nesta figura podem-se observar as entidades referidas na secção anterior.

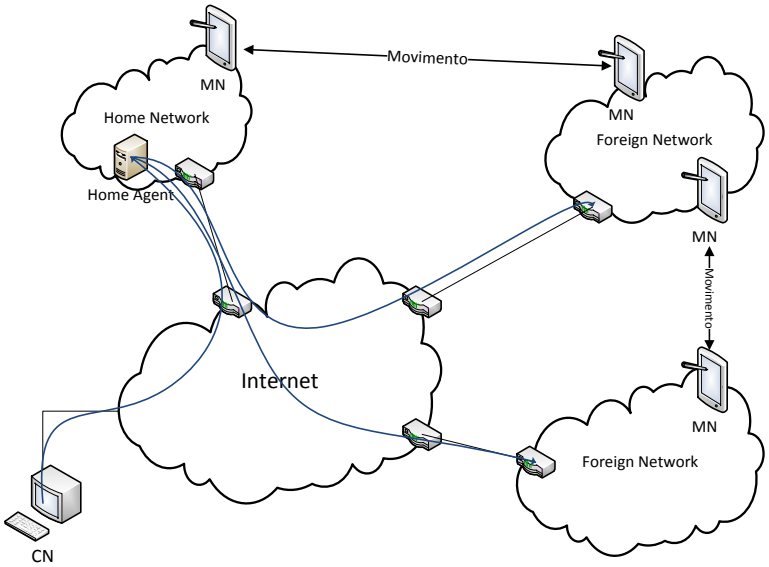


Figura 2.8: MIPv6 - Arquitetura sem otimização de rota

O funcionamento do MIPv6 baseia-se em três mecanismos básicos:

- **Descoberta** - Os agentes de mobilidade (FN) anunciam a sua disponibilidade através do envio de mensagens *Internet Control Message Protocol* (ICMP) *Router Advertisement* (RA). Caso se trate de um *Mobile Node* "impaciente"este pode enviar uma mensagem de ICMP *Router Solicitation* (RS);
- **Registo** - Quando um MN entra numa FN, e depois de ter obtido um *Care-of-Address* (CoA), este envia uma mensagem de *Binding Update* (BU) ao seu *Home Agent* (HA)

com a informação do novo CoA obtido, o HA guarda esta informação na sua *Binding Cache* (BC) para quando receber um pacote destinado ao MN saber para onde o encaminhar. Um MN pode registar vários CoAs caso se consiga ligar a mais de uma FN em simultâneo;

- ***Tunneling*** - Quando o HA recebe a mensagem BU, envia uma mensagem *Binding Acknowledgement* (BA) ao MN, para confirmar o seu registo. De seguida, cria um túnel para o respetivo CoA, encaminhando por este todos os pacotes destinados ao MN.

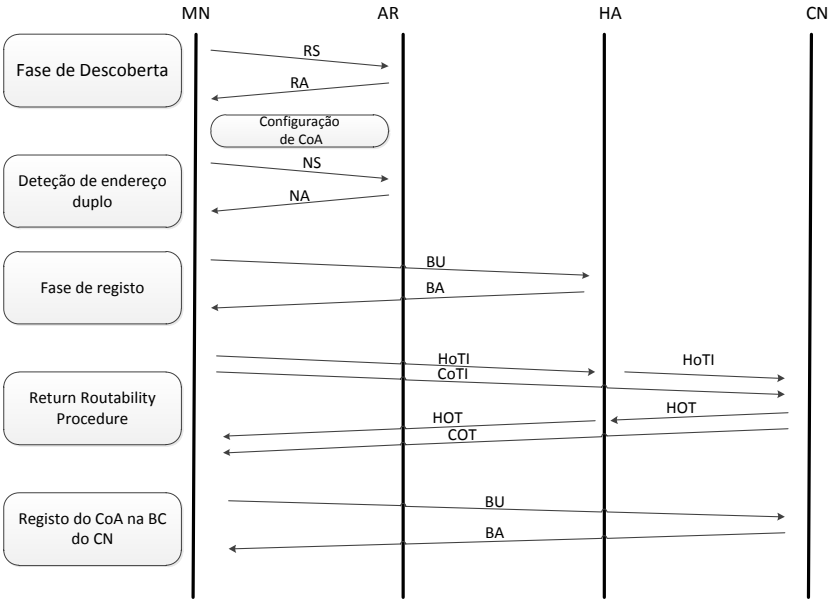


Figura 2.9: MIPv6 - Troca de mensagens durante processo de movimentação com otimização

Na Figura 2.9 pode-se observar todo o processo de troca de mensagens referido anteriormente, desde o processo de descoberta ao registo do MN na BC do *Correspondent Node* (CN).

Adicionalmente, o MIPv6 providencia um mecanismo denominado *Return routability procedure*, para que CNs com suporte IPv6 possam comunicar diretamente com os MNs. O processo de *Return routability* é efetuado através do envio de duas mensagens, a *Home Test Init* (HoTI) que é enviada para o CN via HA e a *Care-of Test Init* (CoTI) que é enviada diretamente para o CN, como se pode observar na Figura 2.9. Estas mensagens têm como finalidade a obtenção de uma *home keygen token* e uma *care-of keygen token* que são enviadas via *Home-Test* (HoT) e *Care-Test* (CoT), respetivamente. De seguida, o MN envia uma mensagem BU para o CN para que este atualize a sua BC. Por fim, o CN envia um BA ao MN indicando que a atualização foi aceite. Quando um CN pretende enviar uma mensagem,

verifica na sua BC se tem alguma entrada para o destino do pacote; caso encontre o pacote é enviado diretamente para o CoA, evitando assim a passagem pelo HA. Consequentemente, irá existir uma melhoria no tempo de entrega do pacote, e como não há a necessidade de encapsular o pacote, é reduzido o *overhead* introduzido na rede. Caso não seja encontrada nenhuma entrada, o pacote é encaminhado normalmente para o HA e daí enviado, através do túnel, para o CoA.

2.6.2 FMIPv6

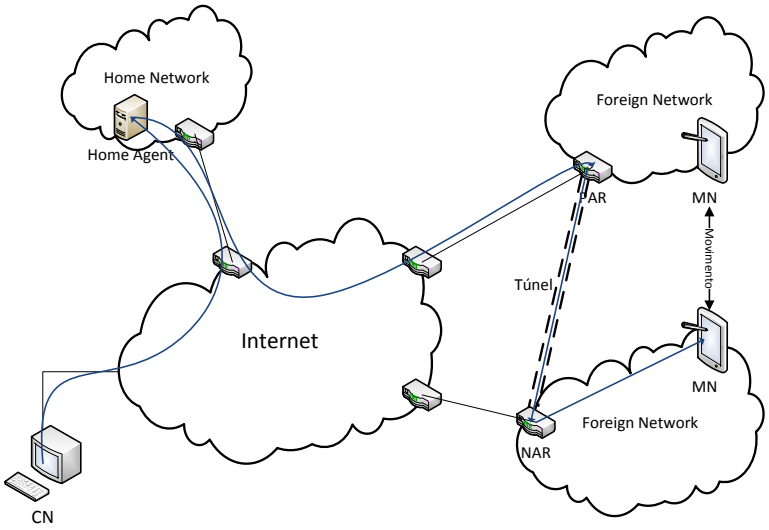


Figura 2.10: FMIPv6 - Arquitetura sem otimização de rota

O protocolo FMIPv6 é uma extensão do protocolo MIPv6, surgindo da necessidade de otimizar o processo de *handover*, permitindo, como o próprio nome indica, que se realizem *handovers* "rápidos".

Para atingir este objetivo, foi introduzida a capacidade de o MN realizar a configuração do endereço referente ao *New Access Router* (NAR), enquanto ainda se encontra ligado ao *Previous Access Router* (PAR). De forma a atingir este objetivo, são utilizadas mensagens de *Router Solicitation for Proxy Advertisement* (RtSolPr) e *Proxy Router Advertisement* (PrRtAdv) para se efetuar a deteção do movimento. Efetuando a troca destas mensagens com o PAR, o MN recebe informação sobre qual o CoA na próxima rede. Deste modo, é reduzida a latência de *handover*, pois elimina-se o tempo necessário para efetuar esta descoberta.

Para além desta melhoria, este protocolo prevê também a criação de um túnel entre o

antigo e o novo CoA, como se pode observar na Figura 2.10. Deste modo, os dados enviados para o CoA antigo, depois de efetuado o movimento para o NAR, são reencaminhados para o novo CoA. Este mecanismo permite uma redução bastante significativa do número de pacotes perdidos durante o processo de *handover*, bem como a redução da própria latência de *handover*, tal é confirmado em Costa et al. [66]. No entanto, neste artigo conclui-se que utilizando os protocolos HMIPv6 e FMIPv6 em conjunto, otimizará ainda mais o processo de *handover*, ao nível da latência do mesmo.

2.6.3 PMIPv6

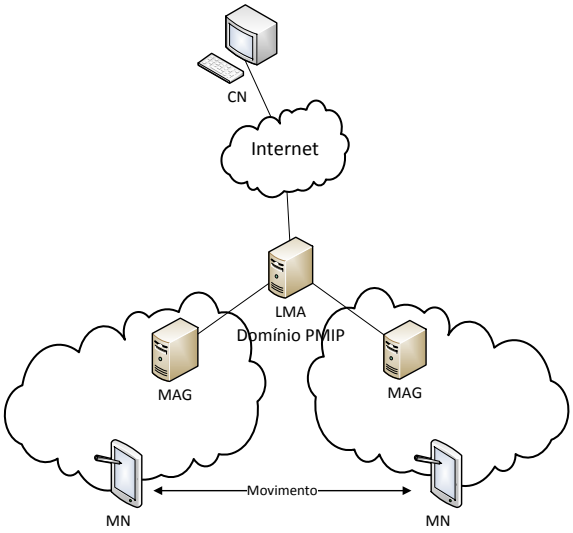


Figura 2.11: PMIPv6 - Arquitetura

O PMIPv6 é um protocolo de mobilidade baseado na rede, isto é, ao contrário do MIPv6, em que o processo de mobilidade é suportado pelo *host*, no PMIPv6 todo o processo de mobilidade é suportado pelo *core* da rede, assim o MN não entra no processo de sinalização do protocolo. O PMIPv6 introduz duas novas entidades denominadas *Local Mobility Anchor* (LMA) e *Mobile Access Gateway* (MAG). O LMA executa as mesmas funções que o HA do protocolo MIPv6, isto é, guarda as informações dos MNs presentes na rede. O MAG tem três funções: a primeira é detetar os movimentos dos MNs e iniciar o processo de sinalização, a segunda é informar o MN do seu prefixo na rede, por fim, a terceira é estabelecer uma rota para os pacotes destinados e proveniente aos MNs. Na Figura 2.12 pode-se observar estas novas entidades introduzidas pelo PMIPv6, estando também ilustrada a arquitetura básica deste protocolo, constituída pelo LMA como unidade central e pelos diversos MAGs.

De acordo com Kong et al. [67], o PMIPv6 foi criado com a finalidade de atingir os seguintes objetivos:

- **Suporte para MN sem modificações** - Como o processo de mobilidade no PMIPv6 é suportado pelo *core* da rede os MNs não necessitam de nenhum *software* para suportar o protocolo;
- **Suporte para IPv4 e IPv6** - Apesar de ter sido criado para redes em que os *hosts* utilizem IPv6 é pretendido que funcione também em redes IPv4;
- **Uso eficiente das ligações sem fios** - Ao evitar o envio de pacotes encapsulados nas ligações sem fios é minimizado o *overhead* nestas ligações;
- **Independente da tecnologia de acesso** - Como a gestão da mobilidade é baseada na rede o PMIPv6 deve suportar qualquer tipo de tecnologia de acesso;
- **Processo de *handover* otimizado** - O processo de mobilidade baseado na rede deve reduzir os tempos necessários para realizar o processo de *handover*.

2.6.3.1 Funcionamento

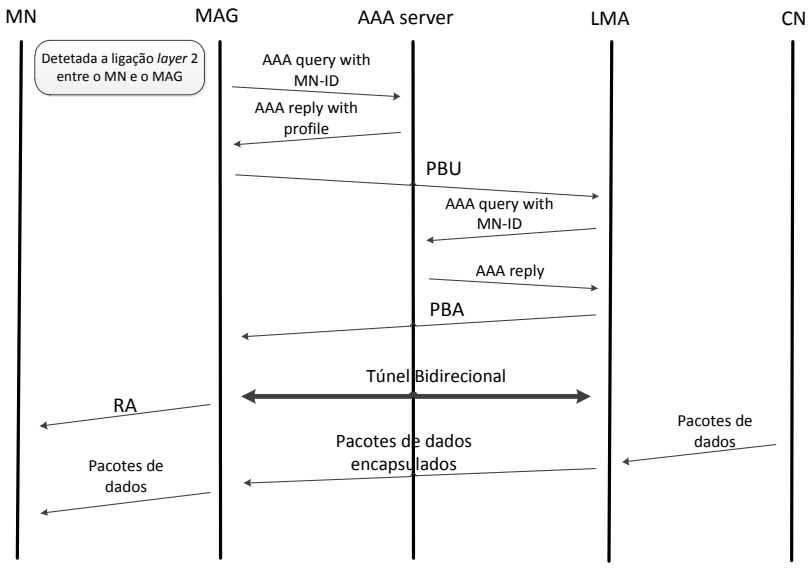


Figura 2.12: PMIPv6 - Troca de mensagens durante processo de movimentação

Através da visualização da Figura 2.12, pode-se perceber todo processo de troca de mensagens após ser detetado um novo MN na rede. O processo registo de um novo nó no domínio

do PMIPv6 segue os seguintes passos:

1. Quando um MN se liga a um MAG, autentica-se utilizando o seu MN-*identifier*;
2. Após o processo de autenticação estar concluído, o MAG envia um *Proxy Binding Update* (PBU) para o LMA com a identificação do MN;
3. Assim que o LMA recebe este PBU verifica se o MN está autorizado a entrar na rede. Se esta verificação for concluída com sucesso o LMA envia um *Proxy Binding Acknowledgement* (PBA) com o *Home Network Prefix* (HNP) do MN e estabelece uma rota para esse prefixo através de um túnel para o MAG;
4. Quando o MAG recebe o PBU emula a HN do MN e envia um RA para o MN, que contém o *Home Network Prefix* do MN;
5. Após receber o RA, o MN configura o seu *Home Agent* utilizando a informação recebida e o endereço da interface utilizada, através de configuração *statefull* ou *stateless*;
6. Por fim é estabelecido o túnel entre o LMA e o respetivo MAG.

2.6.3.2 Comparação de desempenho dos vários protocolos de mobilidade

A Tabela 2.4 faz uma comparação das principais caraterísticas dos protocolos MIPv6 e PMIPv6. Nesta podem-se observar algumas diferenças, já antes referidas, como o tipo de gestão da mobilidade ou a necessidade de recorrer a túneis nas ligações sem fios. Podem-se também observar outras diferenças entre os dois protocolos, como a relação entre o número de túneis criados e o número de *Binding Cache Entry* (BCE). Aqui pode-se concluir que o MIPv6 necessita de criar mais túneis, uma vez que é necessário um por cada BCEs, enquanto no PMIPv6, o mesmo túnel entre um LMA e MAG pode servir mais que um MN. Outra caraterística diferenciadora é a otimização de rota: o MIPv6 suporta esta funcionalidade, explicada em 2.6.1.1, enquanto o PMIPv6 não tem suporte para esta técnica o que se torna numa vantagem para o MIPv6. Finalmente, outra caraterística importante em que estes protocolos diferem prende-se com a necessidade de verificação de DAD: como no MIPv6 esta tem de ser realizada sempre que o MN se move de sub-rede, este facto irá penalizar o tempo de *handover* e *overhead* introduzido na rede.

A comparação do desempenho dos vários protocolos de mobilidade existentes tem sido um tema bastante abordado na literatura nos últimos anos. De seguida, são apresentados alguns destes estudos e as suas principais conclusões. Kong et al. [68] efetuam um estudo, numérico, focado a latência de *handover* apresentada pelos vários protocolos de mobilidade

Tabela 2.4: Comparação entre MIPv6 e PMIPv6 (Adaptado de [67])

	MIPv6	**PMIPv6**
Tipo de Gestão de Mobilidade	Baseada no *host*	Baseada na rede
Modificações no *Mobile Node*	Necessário	Não Necessário
Relação entre número de túneis e BCEs	1:1 (túnel HA-MN)	1:m (túnel LMA-MAG)
Túnel em ligações sem fios	Necessário	Não Necessário
Disseminação de *Router Advertisement*	*Multicast*	*Unicast*
Tipo de ligações suportadas	Qualquer	Ligações Ponto a ponto
Otimização de Rota	Suportado	Não Suportado
Deteção de movimento	Necessário (Através de RS e RA)	Não Necessário (Realizado em L2)
Duplicate Address Detection	Realizado a cada movimentação de rede	Realizado apenas na entrada no domínio
Retrun Routability	Necessário	Não Necessário

existentes. Neste é concluído que o PMIPv6 apresenta um desempenho bastante superior, quando comparado com os protocolos MIPv6 e HMIPv6. No entanto, verificou-se também, que o PMIPv6 e FMIPv6 apresentam latências de *handover* bastante similares. Outro estudo semelhante é apresentado por Guan et al. [69], sendo que neste caso os resultados apresentados foram obtidos recorrendo a uma *testbed*, sendo estes consistentes com os apresentados pelo estudo anterior, ou seja, o protocolo PMIPv6 apresenta uma latência de *handover* e número de pacotes perdidos inferior aos restantes protocolos de mobilidade. Também Kong et al. [67] efetuam uma comparação do desempenho de vários protocolos de mobilidade. Neste caso foram estudados o MIPv6, o HMIPv6 e o PMIPv6, sendo que as conclusões foram em tudo similares às apresentadas pelos estudos referidos anteriormente. No entanto, este artigo vai mais longe e sugere que o PMIPv6 seja utilizado como protocolo de mobilidade local, enquanto o MIPv6 seria utilizado como protocolo de mobilidade global.

2.6.4 IEEE 802.21 MIH

Os protocolos de mobilidade apresentados baseiam o seu funcionamento na camada de rede do modelo OSI. No entanto, o processo de *handover* não se restringe apenas a esta camada, mas também à própria camada de ligação de dados. O protocolo IEEE 802.21 MIH [70] surge com o objetivo de fazer a ponte entre estas duas camadas, ou seja, este protocolo vai abstrair as camadas superiores do tipo de tecnologia de acesso à rede utilizado.

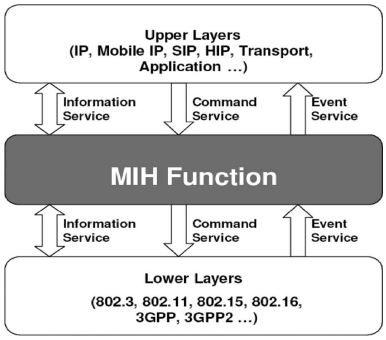


Figura 2.13: MIH *framework* (fonte: [70])

A Figura 2.13 ilustra a interação do *Media Independent Handover Function* (MIHF), entidade nuclear do protocolo IEEE 802.21 MIH, com as camadas do modelo OSI referidas. Pode-se observar que o MIHF fornece três tipos de serviço: *Media Independent Event Service* (MIES), *Media Independent Command Service* (MICS) e *Media Independent Information Service* (MIIS), que facilitam o processo de *handover* entre redes heterogéneas.

- MIES providencia relatórios onde estão incluídas informações como: caraterísticas, qualidade e estados da ligação. O MIES pode reportar eventos, quer estes tenham sido obtidos localmente, quer remotamente. Os eventos mais comuns são *Link Down*, *Link Up*, *Link Detected*, *Link Parameter Reports* e *Link Going Down*. Os protocolos de mobilidade podem utilizar estes eventos para assistir o seu processo de *handover*;
- MICS utiliza as primitivas do MIHF para enviar comandos das camadas superiores (por exemplo: de um protocolo de mobilidade) para as camadas inferiores. Os comandos do MICS são utilizados para determinar o estado das ligações atuais e para executar decisões sobre o processo de mobilidade entre as camadas superiores e as camadas inferiores. Por exemplo, um protocolo de mobilidade pode utilizar o MICS para informar a camada de ligação de dados que vai ocorrer um *handover*, podendo esta preparar-se para este, mesmo antes de este ocorrer;

- MIIS oferece um serviço de descoberta de informação acerca da vizinhança na rede, de forma a facilitar o processo de *handover*. A ideia fundamental é apresentar informações sobre as diferentes tecnologias de acesso disponíveis.

2.7 Segurança em Redes Veiculares

A segurança é um aspeto fulcral em qualquer rede, pois caso os utilizadores não tenham garantia de confidencialidade dos seus dados vão acabar por abandonar a rede e assim esta tende a ser posta de lado. Sendo assim, é necessário que desenvolva uma arquitetura de segurança que providencie comunicações seguras entre os diferentes veículos. De acordo com Raya e Hubaux [71], um sistema de segurança aplicado a redes veiculares deve satisfazer os seguintes requisitos:

- **Autenticação** - Os veículos apenas devem responder a mensagens legítimas, isto é, mensagens geradas por nós legítimos, assim é necessário um sistema de autenticação;
- **Verificação da consistência da informação** - O conteúdo das mensagens deve ser verificado, pois o nó de envio pode ser legítimo, mas a mensagem gerada pode ser falsa;
- **Disponibilidade da rede** - Mesmo que exista um ataque que bloqueie a rede esta deve estar disponível através de meios alternativos;
- **Privacidade** - A privacidade dos dados de um utilizador deve ser garantida contra observadores não autorizados;
- **Restrições temporais** - Devido às altas velocidades dos nós da rede restrições temporais estritas devem ser respeitadas.

Ainda em [71] é proposto um sistema de segurança baseado numa chave de criptografia pública que, segundo os autores, é a melhor solução de segurança para redes veiculares. Outro protocolo de segurança é proposto por Lin et al. [72], integrando técnicas de *Group Signature* (GS) e *Identity* (ID)-*based Signature*. Através de simulações, realizadas em cenário urbano e de autoestrada, os autores mostram que a solução proposta mantém o atraso e as perdas de pacotes bastante baixas, mesmo na presença de uma elevada latência computacional introduzida pelas operações de criptografia. Finamente, Haas et al. [73] testam o desempenho das comunicações com protocolos de segurança. De forma a realizarem testes em larga escala, foi criado um simulador próprio (com mobilidade real de veículos, ao contrário de grande parte dos artigos existentes em que a mobilidade dos veículos é baseada em simuladores,

neste estudo os autores utilizam registos de mobilidade de veículos reais), que pode albergar muito mais veículos que o simulador NS-2. Para validar os resultados obtidos pelo simulador proposto, estes são comparados com resultados obtidos a partir do simulador NS-2 e conclui-se que são semelhantes. Neste estudo são testados dois mecanismos de segurança, *Timed Efficient Stream Loss-tolerant Authentication* (TESLA) e *Elliptic Curve Digital Signature Algorithm* (ECDSA), mostrando as vantagens e as desvantagens de cada um, baseando-se no número de pacotes entregues e na latência dos pacotes enviados em *broadcast*.

2.8 Aplicações e Serviços

Como já foi referido anteriormente, o grande propósito das redes veiculares prende-se com a necessidade de aumentar a segurança nas estradas. Contudo, para que estas redes se tornem atrativas a investidores, é necessário que estas possam disponibilizar aplicações de uso corrente para assim se abrirem novas oportunidades de negócio e, assim, se possa obter uma rápida difusão. Deste modo, para além das aplicações de segurança, espera-se também que os utilizadores possam desfrutar de outros serviços como o acesso à *Internet*, por exemplo.

As aplicações para redes veiculares podem, então, ser divididas em aplicações de segurança, gestão de tráfego rodoviário e aplicações de conforto.

2.8.1 Aplicações de Segurança

As aplicações de segurança, como o próprio nome indica, têm como finalidade aumentar a segurança nas estradas e assim reduzir o número de acidentes de viação e consequentes mortes na estrada. A principal caraterística deste tipo de aplicações é a necessidade de serem transmitidas o mais rapidamente possível e terem como destino uma certa ZOR. Segundo, Kihl [7] as aplicações de segurança podem ser divididas em: *Cooperative Collision Avoidance* (CCA) e *Emergency Warning Message* (EWM).

2.8.1.1 *Cooperative Collision Avoidance*

O objetivo das aplicações CCA é evitar colisões entre veículos, sejam elas colisões em cadeia, frequentes em ambiente de autoestrada, ou colisões frontais, frequentes em ambientes de estradas com dois sentidos de circulação. Para se evitarem as colisões, os veículos, caso estejam preparados, podem travar automaticamente assim que recebem esta mensagem, ou, caso não possuam um mecanismo de travagem automática, mostram uma mensagem de aviso

ao condutor. É de salientar também o facto que estas aplicações podem ser utilizadas quando numa situação pós-colisão, sendo nesse caso a sua utilidade evitar que novos veículos embatam nos veículos já acidentados. Obviamente, para que estas mensagens tenham efeitos práticos, é necessário que sejam entregues em tempo útil: de acordo com Biswas et al. [74], as mensagens de segurança não podem ter uma latência superior a 100 ms. Este tipo de aplicações assenta sobretudo em comunicações V2V, pois comunicações V2I dificilmente podem garantir o tempo de atraso referido anteriormente.

Para se ter uma noção da necessidade destas aplicações durante o ano de 2011, em Portugal, existiram 32541 acidentes de viação, causando 42162 feridos e 689 mortes [75]. Nos últimos tempos a indústria automóvel tem feito um grande esforço no sentido de reduzir estes números através da introdução de uma série de mecanismos de segurança e as autoridades também têm vindo a fazer inúmeras campanhas de sensibilização, mas a verdade é que estes números tendem a não descer. Neste sentido, este tipo de aplicações pode ter um papel fundamental levando a uma redução considerável do número de acidentes.

2.8.1.2 *Emergency Warning Message*

As aplicações de EWM consistem num veículo detetar um acidente, ou condições de perigo na estrada (obras, por exemplo), e enviar uma mensagem a todos os veículos que se encontrem na ZOR desse acontecimento. Este tipo de aplicações requer que as mensagens "permaneçam"nessa determinada zona durante um longo período de tempo, logo, ao contrário das aplicações de CCA, em que o principal tipo de comunicação era V2V, neste tipo de aplicações pode já existir comunicação V2I pois as restrições de latência já não são tão apertadas. A utilização de RSUs pode trazer uma vantagem para este tipo de aplicações, pois desta forma é mais fácil fazer com que as mensagens permaneçam na ZOR.

As EWMs podem ser divididas em dois tipos: instantâneas e permanentes.

- **EWM instantânea** consiste numa mensagem que é gerada por um veículo, por exemplo quando os seus sensores detetam que este fez uma travagem brusca, sendo disseminada para todos os veículos que se encontrem na ZOR. Assim que isto acontece, esta mensagem irá desaparecer;
- As **EWMs permanentes** são mensagens que têm como objetivo avisar os condutores de condições de perigo que se mantêm durante longos períodos de tempo: neste tipo de aplicações é necessário que as mensagens "permaneçam"na ZOR para que sempre que um novo veículo entre nesta zona possa receber a mensagem e tome conhecimento da

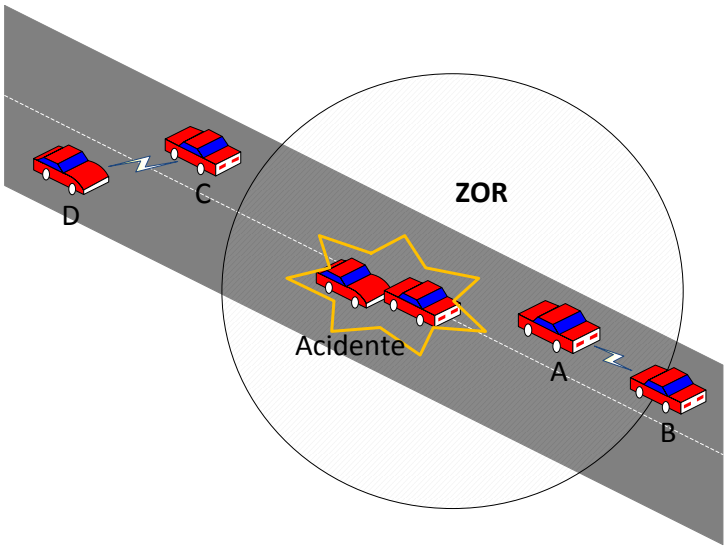


Figura 2.14: Exemplo de *Geocasting* permanente

situação de perigo. Estas aplicações poderão utilizar o método de disseminação *stored geocast*, proposto por Maihofer et al. [76], que basicamente consiste na disseminação da informação para todos os nós que se encontrem na região alvo durante um certo período de tempo. Este tipo de aplicações poderá utilizar infraestruturas, para que deste modo, depois da mensagem de emergência ser gerada, esta seja encaminhada até uma RSU e a partir desse momento, todos os veículos que entrem na zona de alcance, recebem essa mensagem. A Figura 2.14 exemplifica um cenário em que existe uma EWM permanente. Nesta, o veículo A ao detetar que o veículo B está a entrar na ZOR, vai-lhe enviar a mensagem de aviso de perigo. O veículo C, apesar de já não se encontrar na ZOR, possui a mensagem de aviso, pois passou na ZOR. Este ao detetar que o veículo D se encaminha para a esta, deve enviar-lhe a mensagem, otimizando assim o processo de disseminação da EWM.

2.8.2 Aplicações de Gestão de tráfego Rodoviário

As aplicações de gestão de tráfego têm como propósito melhorar a circulação nas estradas, providenciando viagens mais rápidas e reduzindo o congestionamento das vias. Ao nível das necessidades da rede para este tipo de aplicações, estas não têm restrições tão elevadas como as aplicações de segurança em que o atraso ou perdas de mensagens pode resultar em acidentes. Aqui o principal objetivo é providenciar ao condutor informação acerca do tráfego na zona

onde este se encontra ou para onde pretende ir (pressupõe-se neste tipo de aplicações que os carros estão equipados com sistema de posicionamento e navegação GPS e que o condutor definiu nesse equipamento o seu destino), assim são toleráveis tempos de entrega de mensagens mais elevados e perda de pacotes. De acordo com Kihl [7], as aplicações de gestão de tráfego rodoviário podem ser divididas em duas categorias: monitorização de tráfego e assistência em interseções.

2.8.2.1 Monitorização de tráfego

Neste tipo de aplicações as estradas são divididas em vários segmentos. Cada veículo recolhe informações, velocidade por exemplo, sobre o segmento onde de situa e, de seguida, em intervalos de tempo pré-estabelecidos, envia essas informações para a ZOR afetada por esse segmento de estrada. Assim, cada veículo que se encontre nessa zona recebe essa mensagem e guarda-a, podendo agregá-la com a informação sobre o mesmo segmento proveniente de outro veículo. Esta informação será depois utilizada para informar o condutor sobre as condições de tráfego que irá encontrar nesse determinado segmento de estrada, ou pelo sistema de navegação presente no automóvel para melhorar a sua eficiência como é sugerido por Chang et al. [77].

Existem já sistemas de navegação que proporcionam aos condutores informações sobre o estado do trânsito ou sobre o estado da via, recorrendo ao acesso à *Internet* através de rede celular: novamente, segundo [77], estes sistemas ainda carecem das informações provenientes dos próprios veículos.

2.8.2.2 Assistência em interseções

Como é sabido, as interseções são pontos críticos nas estradas, tanto ao nível de acidentes, como ao nível da eficiência do trânsito. Assim, torna-se essencial que se desenvolvam aplicações para melhorar estes pontos críticos. Os estudos realizados nesta área focam-se essencialmente em dois aspetos:

- **Sistemas de aviso de situações perigosas** - estes sistemas alertam para a presença de outros veículos nas imediações das interseções e, no caso de os condutores não tomarem as devidas precauções, estes podem atuar automaticamente. Um sistema deste género é proposto por Benmimoun et al. [78]; neste artigo é também estudado qual o melhor *design* para a interface de interação com o condutor;

- **Semáforos virtuais** - estes sistemas consistem em os semáforos passarem a estar incorporados no próprio veículo, com um sistema deste género. De acordo com Ferreira et al. [79], pode-se conseguir um aumento na eficiência do tráfego na ordem dos 60% em casos de densidades de tráfego bastante elevadas, para além de que possibilitaria também uma redução ao nível dos acidentes. Este sistema tem o inconveniente de necessitar que todos os veículos estejam equipados com um sistema comunicações veiculares e com o próprio sistema de semáforo virtual.

2.8.3 Aplicações de Conforto

O principal objetivo deste tipo de aplicações, como o próprio nome indica, é tornar as viagens mais agradáveis, sobretudo para os passageiros, podendo, no entanto, fornecer também informações aos condutores.

Estas aplicações possibilitam uma série de serviços aos passageiros, por exemplo *Video-on-Demand* (VOD), músicas, noticias, televisão, navegação na *Internet*, etc.. Para além destes serviços poderá também existir a hipótese de se obterem informações sobre restaurantes e hotéis que se encontrem no caminho, mas, para além da simples informação do local onde estes se encontram, como quase todos os equipamentos de navegação GPS já providenciam, os utilizadores podem aqui receber outro tipo de informações adicionais como as ementas disponíveis, fazer reservas (de mesa para jantar ou quarto num hotel), entre outras possibilidades.

As aplicações de conforto baseiam-se sobretudo no acesso à *Internet*, sendo assim necessário que os veículos tenham acesso a esta. Para tal, como já foi referido anteriormente, é necessário que se realizem elevados investimentos em introdução de RSUs ao longo das estradas. No entanto, numa fase inicial, poder-se-á utilizar as redes 3G/4G já existentes para providenciar este acesso e à medida que a penetração das VANETs for aumentando já será mais rentável investir na instalação de RSUs.

2.9 Sumário

Neste capítulo foram apresentados os conceitos essenciais para a compreensão dos principais temas abordados no âmbito desta Dissertação, ou seja, redes veiculares, protocolos de encaminhamento e mobilidade utilizados nas mesmas.

Em relação às redes veiculares foi possível verificar que, apesar de já existirem avanços

muito significativos, existem ainda muitos desafios para serem ultrapassados, entre os quais se destacam avaliações de desempenho em cenário real e integração com outras redes já existentes. Como foi possível compreender ao longo deste capítulo, foi desenvolvida uma nova tecnologia de acesso à rede específica para este tipo de comunicações, sendo que, no entanto, muito poucos estudos a têm em conta. Sabendo que esta tem caraterísticas diferenciadoras em relação a outras normas de comunicação utilizadas, são necessários estudos que mostrem estas diferenças e quais as melhores formas de as aproveitar.

Ao nível de protocolos de encaminhamento para VANETs, verificou-se a existência de um grande número de protocolos propostos, faltando no entanto implementações e estudos práticos destes protocolos, especialmente protocolos baseados na posição geográfica, pois é dado como adquirido que estes são a melhor opção para redes veiculares, contudo, faltam estudos práticos que o comprovem e que mostrem possíveis falhas.

Finalmente, em relação à integração de protocolos de mobilidade em redes veiculares, verificou-se que existem muito poucos estudos que abordem este assunto e ainda menos que tenham em conta a norma IEEE 802.11p, percebendo assim que este é um campo que necessita de grandes avanços nos próximos anos, pois a mobilidade é um fator inerente às redes veiculares e uma gestão eficaz da mesma poderá providenciar uma série de aplicações de conforto, necessárias para uma rápida penetração destas redes.

Capítulo 3

Protocolos de Encaminhamento

3.1 Introdução

Os protocolos de encaminhamento são uma peça fundamental em redes de telecomunicações, pois são estes que definem as rotas efetuadas pelos dados ao longo da rede. Em VANETs, tal como em todos os outros tipos de redes, a eficiência destes é essencial para que o tráfego possa ser encaminhado eficazmente pela rede. No entanto, devido às caraterísticas diferenciadoras das VANETs, torna-se necessário desenvolver novos protocolos, ou adaptar os já existentes para que estes possam ter o comportamento desejado. O estudo sobre protocolos de encaminhamento realizado ao longo desta Dissertação enquadra-se neste último grupo, ou seja, são realizados estudos sobre protocolos já existentes, verificando a sua adaptabilidade a ambientes veiculares.

Durante este capítulo será apresentado o estudo realizado sobre protocolos de encaminhamento, para tal este capítulo será dividido em cinco secções. Na Secção 3.2 serão apresentadas as implementações de protocolos de encaminhamento para redes *ad-hoc* existentes para o sistema operativo *Linux*, bem como as suas principais caraterísticas.

Na Secção 3.3 são apresentados os equipamentos desenvolvidos no âmbito do projeto DRIVE-IN, equipamentos estes utilizados ao longo de todas as experiências realizadas ao longo desta Dissertação.

Na Secção 3.4 são descritas as experiências realizadas de forma a ser possível ajustar os parâmetros dos vários protocolos, para que estes se possam adaptar às necessidades das redes veiculares. São também apresentados os resultados dessas experiências, bem como as principais conclusões que se podem retirar das mesmas.

A Secção 3.5 estuda a capacidade dos protocolos de encaminhamento suportarem a mo-

bilidade dos veículos ao longo do seu movimento entre RSUs, nesta são apresentadas as experiências realizadas e os respetivos resultados.

Finalmente, na Secção 3.6 é feito um pequeno resumo deste capítulo, sendo expostas as principais conclusões que se podem retirar deste.

3.2 Implementações de Protocolos de Encaminhamento para Redes *Ad-Hoc*

Como foi referido no capítulo anterior (ver Secção 2.5), existem muitas propostas de protocolos de encaminhamento para redes *ad-hoc*, sejam elas MANET ou VANET. No entanto, poucos apresentam implementações práticas, existindo também muito poucos estudos sobre o desempenho destes em cenários reais. Para que fosse possível fazer um estudo acerca de protocolos de encaminhamento em VANETs e sobre a sua capacidade de suportar mobilidade em comunicações V2I, foi necessário verificar quais os protocolos de encaminhamento que possuem implementações para o sistema operativo *Linux*. Desta procura resultaram três protocolos, o OLSR, o B.A.T.M.A.N. e o BABEL. Todos estes protocolos são baseados na topologia de rede, no entanto apresentam caraterísticas diferentes, tal como referido anteriormente. Pretendeu-se também estudar o AODV, no entanto, a sua implementação apresenta bastantes problemas, não sendo suficientemente estável, facto também verificado por Abolhasan et al. [54] e Murray et al. [55].

A implementação utilizada do OLSR foi o OLSR *daemon* v0.6.2 [80]. As principais caraterísticas desta implementação são: a variedade de plataformas suportadas (existem versões para os principais sistemas operativos existentes), utiliza poucos recursos e, por fim, é escalável (foram realizados testes com redes de aproximadamente dois mil nós). Outro aspeto interessante desta implementação prende-se com o facto de apresentar um sistema de *link quality*, apesar de este não ser definido pelo protocolo, baseado no algoritmo *Expected Transmission count* (ETX) [81].

O B.A.T.M.A.N. *daemon* v0.3.2 [82] foi a implementação utilizada do protocolo de encaminhamento B.A.T.M.A.N.. Esta é uma implementação do protocolo realizada na camada 3, ou seja, ao nível da camada de rede do modelo protocolar OSI. Apesar do protocolo definir que este deve funcionar na camada 2, utilizou-se esta implementação, pois de acordo com Murray et al. [55], não existem grandes diferenças de desempenho entre as implementações na camada 2 e 3 deste protocolo. O facto de ser um *daemon* traz vantagens no que confere à

sua integração no resto do sistema.

Por fim, foi utilizado o BABEL *daemon* v1.3.0 [83], implementação do protocolo de encaminhamento BABEL. A principal caraterística desta implementação é a utilização de um sistema de *link quality*, tal como o OLSR *daemon* baseado na métrica ETX. Outra característica importante é o facto de esta implementação integrar o sistema de *dual-stack* definido pelo protocolo, isto é, o mesmo pacote pode conter as rotas referentes ao IPv4 e ao IPv6.

3.3 Equipamento utilizado

De forma a ser possível testar os cenários pretendidos neste capítulo e no Capítulo 5, foi necessário criar pequenas *testbeds*. Para as realizar recorreu-se, sobretudo, aos equipamentos desenvolvidos no âmbito do projeto DRIVE-IN. Estes são constituídos pelos componentes descritos de seguida:

- Módulo PCEngines Alix3D3, com um processador de 500 MHz AMD Geode LX800 – arquitetura 32-bits x86, 256 MBytes de memória e ligação *Ethernet*.
- Módulo Wi-Fi compatível com a norma IEEE 802.11p.
- Módulo Wi-Fi compatível com a norma IEEE 802.11b/g.
- Antena L-Com omnidirecional preparada para frequências entre 5.150 e 5.9 *GHz*, com ganho de 5dBi.
- Antena omnidirecional preparada para frequências na gama dos 2.4 *GHz*, com ganho de 5dBi.
- Sistema operativo Linux Debian "squeeze", com a versão 2.6.32 do *kernel* compilado com as opções de suporte aos protocolos de mobilidade.
- *Driver* ath5k modificado para suportar a norma IEEE 802.11p/1609.x [32].
- GPS GlobalTop (MediaTek MT3329).
- *Modem* 3G ZTE MF636 *Universal Serial Bus* (USB).

A principal caraterística deste equipamento é a inclusão de *hardware* e *software* capazes de suportar as normas de comunicação WAVE (apresentadas em 2.3.1), ou seja, a norma IEEE 802.11p e a família de normas IEEE 1609.x. Deste modo, as comunicações utilizando a interface correspondente a estas normas irão ter todas as caraterísticas destas, das quais se destacam:

- Inexistência de autenticação e associação.
- Suporte para o protocolo WSMP.
- Existência de CCH e de SCH e suporte para operações com comutação de canal.

3.4 Adaptações realizadas para integração dos Protocolos de Encaminhamento em VANET

As redes veiculares podem ser definidas como redes *ad-hoc*. No entanto, devido ao facto de os nós da rede serem veículos, estas apresentam uma mobilidade muito superior às redes *ad-hoc* tradicionais. Devido a esta mobilidade, os protocolos de encaminhamento desenvolvidos para MANETs podem não apresentar o mesmo desempenho em VANETs. Deste modo torna-se necessário perceber se os protocolos de encaminhamento disponíveis se conseguem adaptar a esta mobilidade, e quais as configurações necessárias para tal.

Os três protocolos de encaminhamento estudados são protocolos proativos, isto é, são permanentemente trocadas mensagens de controlo que estabelecem todas as rotas possíveis. Como em redes veiculares o tempo de ligação entre veículos será reduzido, torna-se importante perceber qual o impacto que tempo entre envio de pacotes de controlo de topologia tem sobre a deteção de um novo nó na rede e sobre o tempo de reação à quebra de uma ligação. Assim, efetuaram-se testes variando o tempo de envio de mensagens de controlo e mediram-se os respetivos tempos de reação à presença de um novo nó na rede e à quebra de uma ligação. Deste modo, é possível verificar qual o intervalo entre envio de pacotes de topologia apresenta melhor tempo de reação, em função do *overhead* introduzido na rede. É também possível efetuar uma comparação entre os protocolos utilizados, de modo a verificar qual se adapta melhor à elevada mobilidade das redes veiculares.

Para se efetuar o teste de verificação do tempo necessário à descoberta de um novo nó na rede utilizaram-se duas placas com equipamento semelhante ao descrito na secção anterior. Na primeira placa colocou-se o protocolo de encaminhamento sempre em funcionamento, enquanto na outra foi introduzido um fluxo de pacotes ICMP com um intervalo de 1 ms (desta forma é possível ter uma precisão ao milissegundo) destinado à primeira e iniciou-se uma captura de pacotes, recorrendo ao programa *Tshark* [84]. De seguida iniciou-se o protocolo de encaminhamento na placa onde foi iniciado o fluxo de dados, e mediu-se a diferença entre o primeiro pacote ICMP entregue com sucesso e o primeiro pacote de controlo de topologia enviado, sendo possível verificar qual o tempo necessário para que um nó seja

reconhecido na rede.

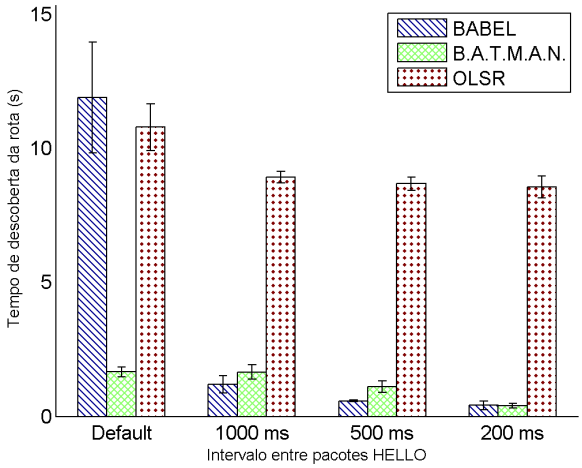


Figura 3.1: Tempo necessário para descoberta de um novo nó na rede em função do intervalo entre envio de pacotes de HELLO

A Figura 3.1 mostra os resultados obtidos a partir do teste descrito anteriormente. O primeiro facto facilmente observável é a grande diferença entre o protocolo OLSR e os restantes. Mesmo com o envio de mensagens HELLO a cada 200 ms, verifica-se que o tempo de deteção de um novo nó na rede não baixa significativamente, mantendo-se sempre em valores de aproximadamente oito segundos. Outro aspeto observável na figura é a grande diferença entre os resultados obtidos quando utilizadas as definições *default* em cada protocolo. É possível verificar que, para o protocolo BABEL, o tempo de descoberta de um novo nó é bastante elevado, pois este na sua configuração *default* envia pacotes de controlo de topologia a cada quatro segundos. Esta definição, como se pode observar pela figura, leva a um tempo de descoberta de um novo nó na rede bastante elevado, o que faz com que esta definição não seja adequada a redes veiculares. No entanto, quando utilizados os intervalos semelhantes aos outros protocolos, nota-se que este apresenta um desempenho superior, ainda que quando comparado com o B.A.T.M.A.N. a diferença seja bastante reduzida. Por fim, pode-se ainda concluir que o intervalo que apresenta melhor relação entre o tempo de descoberta de um novo nó na rede em função do *overhead* introduzido é o intervalo de 500 ms; uma vez que utilizando o intervalo de 200 ms, o *overhead* é mais do que duplicado, o que leva a uma utilização pouco eficiente dos recursos disponíveis.

De forma a ser possível obter o tempo necessário para que os protocolos em estudo detetem uma quebra de ligação numa rota, utilizaram-se quatro placas semelhantes às utilizadas an-

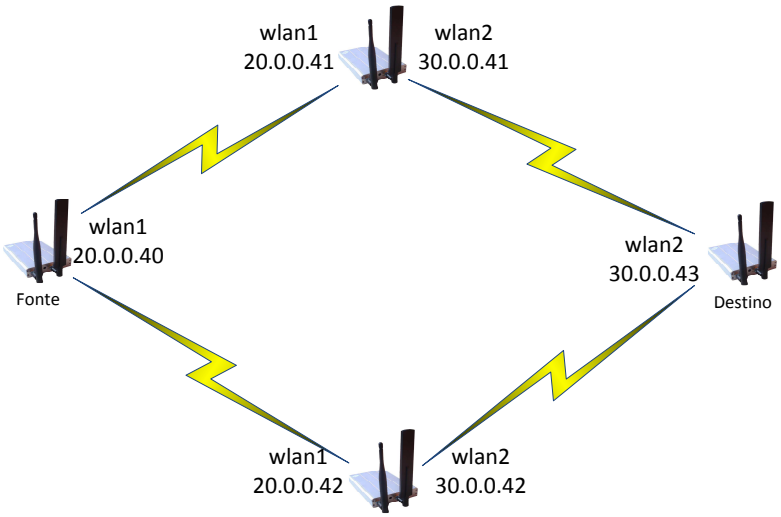


Figura 3.2: Esquematização da *testbed* utilizada para determinar o tempo de reação à quebra de uma rota

teriormente, criando-se assim uma rede conforme esquematizado na Figura 3.2. Deste modo, existem duas rotas possíveis entre a fonte e o destino. Quando uma das rotas é quebrada, o protocolo é obrigado a alterar a rota. Para medir o tempo necessário para o protocolo se aperceber da quebra da rota, introduziu-se um fluxo de dados utilizando o protocolo de transporte *User Datagram Protocol* (UDP), para que não existam retransmissões e se possa perceber qual o tempo efetivo de reação à quebra da rota. Depois de introduzido este fluxo de dados, mediu-se o tempo em que não houve a receção de dados, recorrendo à ferramenta *Tshark*.

Na Figura 3.3 podem-se observar os tempos de reação à quebra de uma rota em função do intervalo entre o envio de pacotes de controlo de topologia, para os vários protocolos de encaminhamento em estudo. Analisando esta figura, verifica-se que o protocolo OLSR apresenta tempos de descoberta de quebra de rota muito elevados, e que estes não são influenciados pela alteração do intervalo entre o envio de pacotes TC. Tal como verificado no teste anterior, neste também se pode perceber que o protocolo OLSR é muito lento a aperceber-se de alterações na topologia da rede, o que faz com que este não seja muito adequado para as redes veiculares. Quanto aos restantes protocolos, é possível verificar que ao contrário do teste anterior, em que o comportamento era semelhante, neste teste o protocolo BABEL mostra um desempenho bastante superior. Mesmo quando utilizado o intervalo de envio de pacotes de controlo de topologia de 500 ms, este apresenta um desempenho superior ao protocolo B.A.T.M.A.N.,

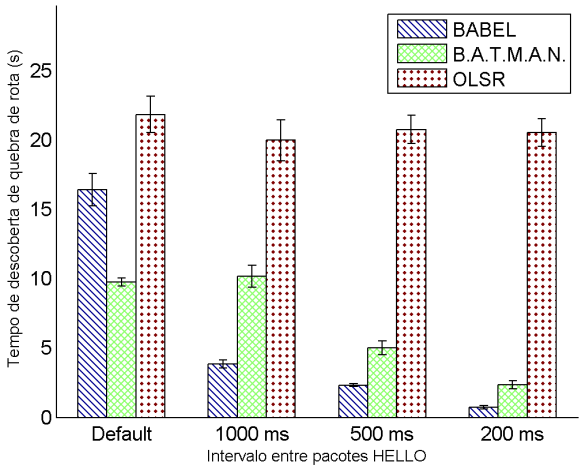


Figura 3.3: Tempo necessário para descoberta da quebra de uma rota em função do intervalo entre envio de pacotes de controlo de topologia

quando este se encontra configurado com um intervalo de 200 ms. Também, ao contrário do teste anterior, verifica-se uma grande diferença nos resultados obtidos utilizando o intervalo de 200 ms em relação aos obtidos com o intervalo de 500 ms, isto em ambos os protocolos. Apesar destes factos, é necessário ter em conta o grande aumento no *overhead* introduzido na rede, sendo para esse feito necessário realizar testes com um grande número de nós na rede para perceber até que ponto este aumento do *overhead* se iria refletir no desempenho da rede.

3.5 Capacidade dos Protocolos de Encaminhamento para responder à necessidade de gestão de mobilidade entre RSUs

Um dos principais objetivos do trabalho realizado ao longo desta Dissertação centra-se no estudo e desenvolvimento de mecanismos de suporte à mobilidade dos veículos entre as diferentes estações fixas existentes. Aproveitando o facto de se estarem a estudar os protocolos de encaminhamento em redes veiculares, e tendo em conta o trabalho realizado por Annese et al. [49], estudou-se a capacidade destes protocolos oferecerem o suporte necessário ao movimento dos veículos entre redes.

Para se realizar o estudo pretendido, fez-se um teste com duas RSUs (que não se encontram em alcance de comunicação) ligadas a um computador, através de *Ethernet*, e um nó móvel que se desloca entre as RSUs, a uma velocidade reduzida (aproximadamente 5 km/h), partindo da zona de alcance da primeira RSU, indo até à segunda e depois voltando para a primeira.

Assim, será de esperar que ocorram dois *handovers* em cada teste efetuado. Para que fosse possível verificar o comportamento dos protocolos ao longo do movimento do MN entre as RSUs, foi introduzido um fluxo de dados entre o computador e a placa móvel. Na Figura 3.4 pode-se observar uma esquematização da *testbed* referida.

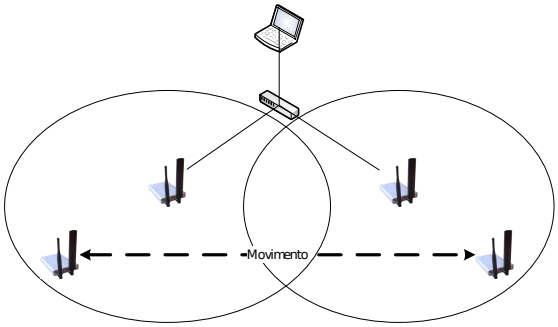
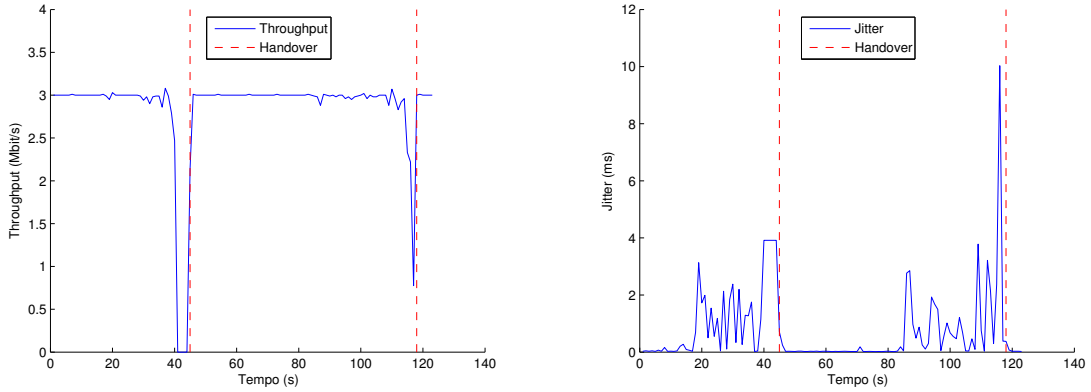


Figura 3.4: Esquematização da *testbed* utilizada

É importante referir que se está a utilizar a tecnologia IEEE 802.11p, e assim que os nós estão em raio de alcance, a comunicação pode-se efetuar de imediato. Deste modo, o único responsável pela rota entre o computador e o MN é o protocolo de encaminhamento. Este teste foi realizado com os três protocolos de encaminhamento em estudo, sendo utilizados os intervalos entre pacotes de anúncio de vizinhos de 500 ms. Desta forma é possível verificar qual o protocolo que apresenta melhor comportamento, sendo estes testes um complemento aos testes realizados na secção anterior.

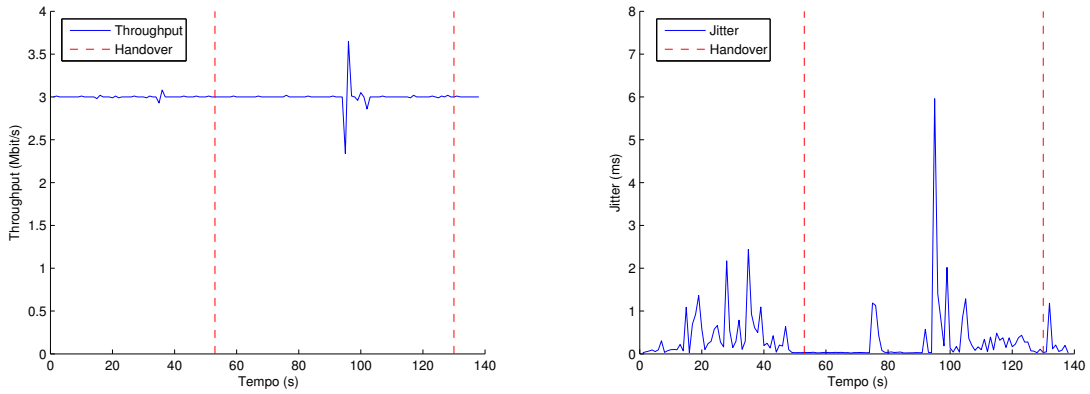


(a) *Throughput* (b) *Jitter*

Figura 3.5: OLSR - Evolução do *Throughput* e *Jitter* ao longo do teste

A Figura 3.5 apresenta a evolução do *throughput* (a) e *jitter* (b) ao longo do teste (gráficos

a azul), enquanto os instantes de *handover* se encontram representados pelas barras verticais (representadas a vermelho). Estes gráficos representam os resultados obtidos quando utilizado o protocolo de encaminhamento OLSR. Nesta figura pode-se verificar que existem períodos de perda de ligação, mesmo sabendo que os raios de comunicação das duas RSUs se sobrepõem em cerca de metade do percurso efetuado pelo MN. Deste modo, pode-se concluir que o protocolo OLSR apenas faz a troca de rota quando se verifica a perda de ligação, não sendo adequado para o tipo de conetividade pretendida. Também analisando o *jitter* se percebe este comportamento, pois este apresenta valores muito elevados antes da troca de RSU e muito baixos logo a seguir, o que indica que a segunda RSU já apresenta melhor qualidade de ligação.

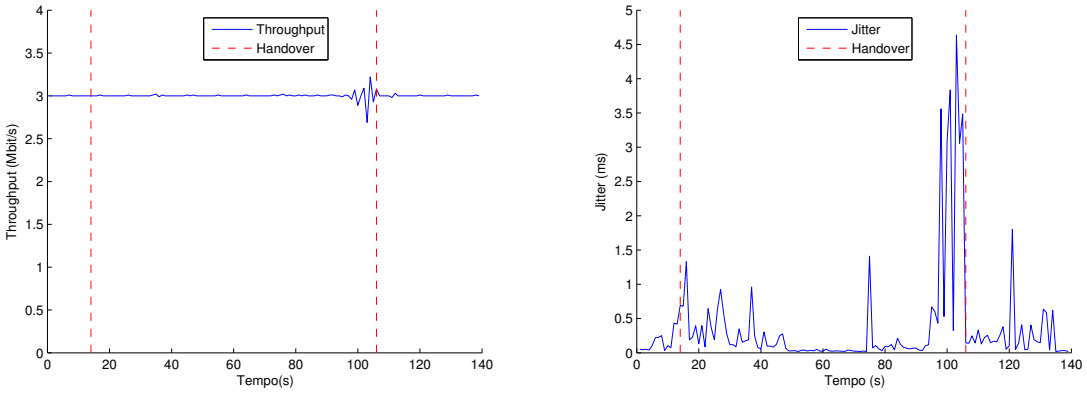


(a) *Throughput* (b) *Jitter*

Figura 3.6: B.A.T.M.A.N. - Evolução do *Throughput* e *Jitter* ao longo do teste

Observando as Figuras 3.6(a) e 3.6(b), referentes à evolução do *throughput* e *jitter*, respetivamente, utilizando o protocolo de encaminhamento B.A.T.M.A.N., é possível observar um comportamento distinto em relação ao verificado anteriormente. Nesta experiência é possível observar que não existem quebras no *throughput* ao longo do teste, o que indica que o protocolo consegue responder atempadamente à perda de qualidade de ligação com a primeira RSU, alterando a rota suficientemente cedo para que não se verifiquem perdas de ligação e consequente perda de pacotes. Analisando o comportamento do *jitter* pode-se também verificar que não existe grande variação quando se efetua a troca de rota, o que confirma que esta foi realizada quando a qualidade de ligação ainda era aceitável.

Na Figura 3.7 encontra-se representada a evolução das métricas *troughput* (a) e *jitter* (b), quando utilizado o protocolo BABEL. Analisando estas métricas é possível verificar que



(a) *Throughput* (b) *Jitter*

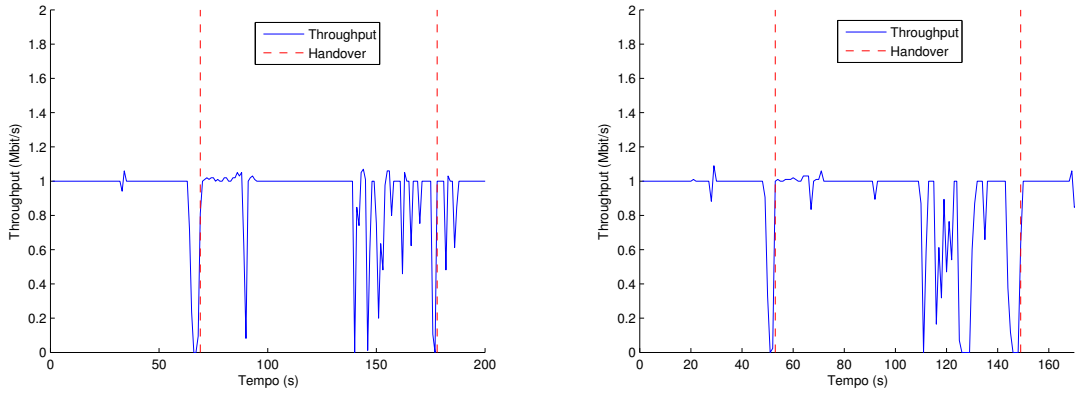
Figura 3.7: BABEL - Evolução do *Throughput* e *Jitter* ao longo do teste

o comportamento do protocolo BABEL é muito semelhante ao apresentado pelo protocolo B.A.T.M.A.N., ou seja, não existem quebras de ligação ao longo do teste. Nota-se apenas uma ligeira instabilidade na ligação nos momentos que precedem o segundo *handover*, que se pode observar em ambos os gráficos. No entanto, verifica-se que o protocolo toma a decisão de alterar a rota antes de existir a perda de ligação, não se verificando assim perda de pacotes ao longo de todo o teste.

Comparando o desempenho dos três protocolos durante este teste, pode-se concluir que o protocolo OLSR apresenta um desempenho inferior, que somado ao comportamento observado na secção anterior, verifica-se que não se adapta a redes veiculares, pois leva muito tempo até estabelecer uma rota para um novo nó na rede, e apenas altera uma rota quando esta é quebrada. Em relação aos restantes protocolos, B.A.T.M.A.N. e BABEL, verificou-se que apresentam um desempenho muito similar tanto no teste apresentado nesta secção como no apresentado na secção anterior, o que leva a concluir que ambos se podem adaptar a VANETs, faltando no entanto realizar testes utilizando veículos, pois aí devido às velocidades mais elevadas estes comportamentos podem-se alterar.

Tendo em conta que o BABEL foi o protocolo que apresentou melhor desempenho em todos os testes apresentados ao longo desta secção, escolheu-se este teste para se efetuarem testes num cenário real. Estes testes foram realizados utilizando a mesma topologia do teste anterior, ou seja, a topologia apresentada na Figura 3.4. No entanto, devido à distância entre as duas RSUs, a ligação *Ethernet* foi alterada por uma ligação IEEE 802.11g. A metodologia utilizada para realizar este teste foi semelhante à utilizada nos testes anteriores, assim a única

variável entre estes testes é a velocidade a que o MN se move. Deste modo é possível perceber o impacto do aumento da velocidade no comportamento do protocolo.



(a) Velocidade de 50 Km/h

(b) Velocidade de 70 Km/h

Figura 3.8: BABEL - Evolução do *Throughput* ao longo do teste em cenário real veicular

A Figura 3.8 apresenta a evolução do *throughput* nos testes realizados com o protocolo BABEL em cenário real, para as velocidades de 50 Km/h e 70 Km/h. Como se pode observar nas Figuras 3.8(a) e 3.8(b) o *throughput* apresenta bastantes quebras ao longo do teste realizado, existindo alguns momentos de quebra de ligação, especialmente nos momentos que antecedem o segundo *handover*. Deste modo pode-se concluir que, embora com mobilidade reduzida o protocolo BABEL tome a decisão de efetuar *handover* antes de se perder completamente a ligação, quando a velocidade se torna mais elevada este já não apresenta o mesmo comportamento, existindo perdas de ligação nos momentos que antecedem o *handover*. Este comportamento torna-se mais evidente com o aumento da velocidade, como se pode comprovar comparando estas figuras. Quando o teste é realizado à velocidade de 70 Km/h os tempos de perda de ligação são superiores aos tempos de perda de ligação obtidos a partir do teste realizado a 50 Km/h.

Para além deste comportamento os protocolos de encaminhamento apresentam também uma série de lacunas no que respeita à gestão de mobilidade. De entre estas lacunas destacam-se as seguintes:

- Não suportam mobilidade entre redes diferentes, isto é, não conseguem garantir a continuidade do endereço de IP.
- Não suportam mobilidade entre diferentes tecnologias de acesso à rede.

- Necessitam que todas as entidades da rede utilizem o mesmo protocolo de encaminhamento, mesmo as entidades pertencentes ao *core* da rede.

Face às limitações apresentadas e aos resultados obtidos em cenário veicular real, pode-se concluir que os protocolos de encaminhamento não são adequados para fazer a gestão da mobilidade entre as várias RSUs. Deste modo torna-se necessário a utilização de protocolos capazes de efetuar esta gestão de forma mais eficaz, para que se possam obter transições entre as várias RSUs de forma rápida e transparente.

3.6 Conclusões

Neste capítulo foi apresentado o trabalho desenvolvido na área de protocolos de encaminhamento para redes VANETs. Numa primeira fase foram expostos os protocolos em estudo e as razões para a sua escolha, sendo também apresentadas as principais caraterísticas de cada uma das implementações utilizadas. Foi também apresentado o material utilizado ao longo das experiências realizadas ao longo desta Dissertação.

De seguida foram apresentados os estudos realizados para se poder perceber qual a adaptabilidade de cada protocolo a redes VANETs. Através destes testes foi possível verificar que o protocolo BABEL apresenta um desempenho superior aos restantes. Observou-se também que o OLSR dificilmente se poderá utilizar nestas redes, pois apresenta tempo de deteção de alterações na topologia da rede na ordem das dezenas de segundos, o que em redes veiculares é incomportável.

O último estudo realizado neste capítulo prende-se com verificação da capacidade dos protocolos de encaminhamento para responder à mobilidade dos veículos entre as várias RSUs existentes. Através deste estudo foi possível verificar que os protocolos B.A.T.M.A.N. e BABEL apenas se podem adaptar a este cenário se a velocidade dos MNs for bastante reduzida, pois para as velocidades de 50 Km/h e 70 Km/h obtiveram-se tempos de perda de ligação bastante elevados. Mais uma vez, neste teste o protocolo OLSR apresentou um desempenho bastante inferior, confirmando assim as conclusões anteriores de que este protocolo não é aplicável a VANETs.

Capítulo 4

Gestão de Conectividade e Protocolos de Mobilidade

4.1 Introdução

Para que os utilizadores das redes veiculares possam ter acesso à *Internet* e consequentes aplicações de conforto, é necessário fazer com que os veículos se possam a ligar às estações fixas presentes ao longo das estradas. No entanto, devido à elevada mobilidade dos veículos, estes permanecem muito pouco tempo no alcance de cada RSU, sendo então imperativo desenvolver sistemas de gestão de mobilidade para que os veículos se possam mover entre RSUs sem perder ligação. O trabalho desenvolvido nesta área, durante esta Dissertação, pretende estudar e desenvolver mecanismos capazes de providenciarem *handover* rápido e transparente, quando os veículos se movem entre as várias RSUs. Pretende-se também verificar quais as tecnologias de acesso à rede que possibilitam este movimento com o mínimo de tempo de perda de ligação. Para isso, foram estudados dois protocolos de mobilidade: o MIPv6 e o PMIPv6, pois estes dois protocolos apresentam implementações para o sistema operativo em uso e, apesar de ambos terem o objetivo de suportar a mobilidade ao nível da camada de rede, a forma como o fazem é completamente distinta, sendo assim possível perceber qual das abordagens se adapta melhor aos cenários em estudo. Utilizaram-se três tecnologias de acesso à rede, o IEEE 802.11p, o IEEE 802.11g e o 3G. A primeira foi desenvolvida especificamente para comunicações veiculares, e implementada por Ameixieira et al. [32] no âmbito do projeto no qual esta Dissertação se insere, enquanto as restantes são as tecnologias de acesso à rede (sem fios) mais comuns hoje em dia. Assim será possível desenvolver mecanismos que integrem

diversas tecnologias; será também possível comparar o desempenho de cada uma durante o processo de mobilidade e qual a sua adaptabilidade a comunicações entre veículos.

No entanto, os protocolos de mobilidade apenas operam ao nível da camada de rede, sendo também necessário efetuar o *handover* ao nível da camada de ligação. Para tal, foi necessário desenvolver um mecanismo que monitoriza as redes existentes, determinando quais as que oferecem melhor qualidade de ligação e que efetue a devida ligação com essas redes. Este mecanismo terá também de ser integrado com os protocolos de mobilidade, pois cada protocolo tem as suas necessidades particulares.

Neste capítulo é explicado todo o processo de funcionamento das implementações dos dois protocolos de mobilidade utilizados, o MIPv6 e o PMIPv6. São também apresentadas as alterações realizadas nas duas implementações de forma a obter um melhor desempenho, bem como todas as configurações efetuadas para que o sistema utilizado suporte os protocolos de mobilidade. Será também apresentado o gestor de mobilidade desenvolvido.

Este capítulo será então dividido em cinco secções. A Secção 4.2 apresenta a arquitetura que se pretende estudar, bem como a interação existente entre as várias entidades envolvidas no processo de mobilidade. Na Secção 4.3 será explicada a implementação do protocolo MIPv6 e as alterações da implementação utilizadas, bem como o programa desenvolvido para fazer a ligação entre o gestor de mobilidade e o protocolo. A Secção 4.4 será semelhante à secção anterior mas para o caso do protocolo PMIPv6. Numa primeira fase será explicado o funcionamento da implementação do protocolo, seguidamente serão expostas as lacunas existentes e as alterações introduzidas para fazer face a essas lacunas. Na Secção 4.5 será apresentado o gestor de mobilidade implementado e, finalmente, na Secção 4.6 é apresentado um breve resumo deste capítulo.

4.2 Arquitetura em Estudo

Considerando que hoje em dia existem várias tecnologias de acesso à rede disponíveis, um dos objetivos do trabalho desenvolvido durante desta Dissertação centra-se no desenvolvimento e avaliação do processo de *handover*, tanto entre rede homogéneas, como entre redes heterogéneas, num ambiente veicular.

A Figura 4.1 exemplifica a arquitetura que se pretende estudar, ou seja, uma arquitetura em que os veículos comunicam entre si, utilizando comunicações através da norma IEEE 802.11p, e comunicam também com as várias estações fixas presentes ao longo das estradas, através de vários tipos de tecnologia, como se pode observar através da figura. Como se

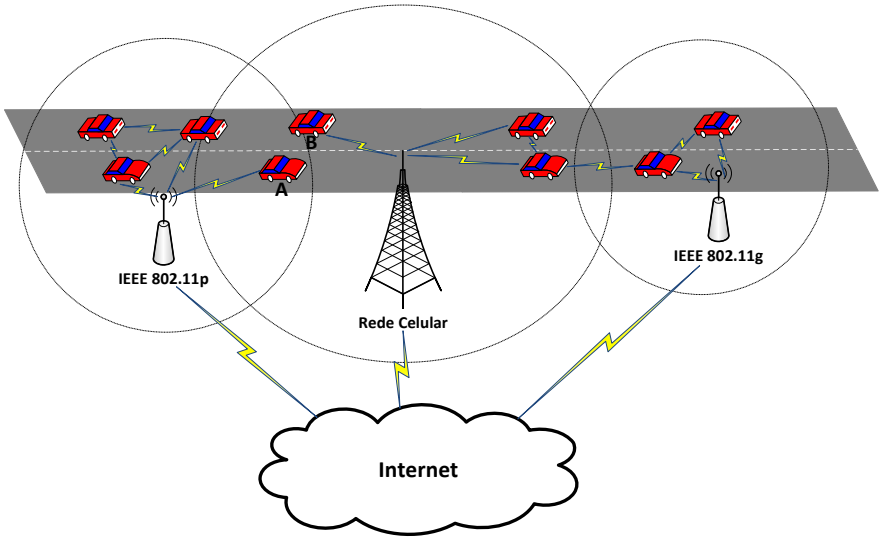


Figura 4.1: Exemplo da arquitetura das VANETs que se pretende estudar

pode observar na Figura 4.1 o veículo A encontra-se no alcance de uma RSU equipada com a tecnologia IEEE 802.11p. No entanto, está prestes a sair do alcance desta e, deste modo, é necessário efetuar o *handover* para a tecnologia 3G de forma a não perder a ligação com a *Internet*. Já o veículo B encontra-se na situação inversa, e tendo em conta que a ligação 3G apresenta maior latência e menor *bitrate*, é conveniente que este quando entre no alcance de um rede IEEE 802.11p efetue o *handover* para esta. Tendo em conta esta necessidade, o principal objetivo desta Dissertação passa pelo desenvolvimento de mecanismos capazes de efetuarem esta transição de forma rápida e transparente, quer esta seja entre estações fixas equipadas com a mesma tecnologia – *handover* intra-tecnologia –, quer esta seja entre estações fixas equipadas com tecnologias diferentes – *handover* inter-tecnologia.

Deste modo, o equipamento utilizado (ver Secção 3.3) possui três tecnologias de acesso à rede, o IEEE 802.11p, o IEEE 802.11g e o 3G, sendo assim possível estudar o comportamento durante o *handover* entre qualquer uma destas tecnologias, de acordo com os seguintes cenários:

- IEEE 802.11p $\Rightarrow$ IEEE 802.11p, com e sem comutação de canal. A comutação de canal utilizada segue o esquema representado na Figura 2.4(a);
- IEEE 802.11g $\Rightarrow$ IEEE 802.11g;
- IEEE 802.11p $\Leftrightarrow$ IEEE 802.11g;

- IEEE 802.11p ⇔ 3G;
- IEEE 802.11g ⇔ 3G.

Para que se possa efetuar o *handover* entre redes é necessário utilizar um protocolo de mobilidade que trate de todos os aspetos relativos à mudança de rede. Neste sentido foram utilizados dois protocolos o MIPv6 e o PMIPv6. Deste modo, é possível perceber qual das abordagens seguidas pelos protocolos se adapta melhor a VANETs.

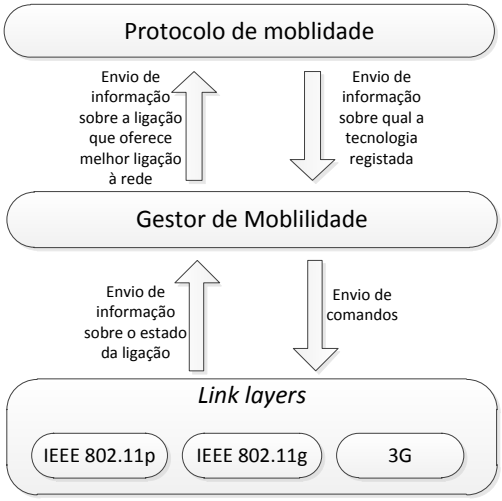


Figura 4.2: Arquitetura em estudo

Os protocolos de mobilidade apenas efetuam o *handover* ao nível da camada de rede, isto é, na camada de IP. Assim, é necessário utilizar o mecanismo que desencadeie o *handover* ao nível da camada de ligação de dados e que faça a ligação com o protocolo de mobilidade utilizado. Neste sentido, desenvolveu-se um Gestor de Mobilidade que monitoriza a qualidade de ligação das redes existentes, efetua a ligação com a rede que oferecer melhor qualidade de ligação e comunica com o protocolo de mobilidade, desencadeando o *handover* ao nível da camada MAC. A Figura 4.2 esquematiza esta comunicação entre o gestor de mobilidade e os *link layers* das várias tecnologias, bem como a interação com o protocolo de mobilidade utilizado. Esta figura representa a arquitetura ao nível do MN, pois é neste que se efetua o processo de escolha da rede que oferece melhor qualidade de ligação. É também neste que se inicia todo o processo de *handover*.

Através da Figura 4.2 pode-se observar que a arquitetura em estudo é similar à arquitetura introduzida pelo protocolo IEEE 802.21 MIH (ver Figura 2.13), apresentando conceptu-

almente as mesmas funções. No entanto, não se utilizou este protocolo uma vez que não existe nenhuma implementação deste integrando a tecnologia IEEE 802.11p, sendo assim necessário proceder à implementação de raiz. Outro fator que levou à não utilização deste foi o facto de a implementação utilizada do protocolo PMIPv6 não estar preparada para trabalhar com este protocolo, sendo assim também necessário proceder à sua implementação. Deste modo, optou-se pelo desenvolvimento de um Gestor de Mobilidade simplificado, sendo a introdução deste protocolo um possível trabalho futuro.

4.3 MIPv6

De forma a ser possível testar o protocolo MIPv6 foi necessário recorrer a uma implementação deste em *Linux*. Existem algumas implementações deste protocolo para este sistema operativo, sendo que a escolha recaiu sobre a implementação *USAGI-patched Mobile IPv6 for Linux* [85], já que esta é uma evolução de implementações mais antigas, tendo portanto, correções de *bugs* e novas funcionalidades, como o suporte para o protocolo NEMO [86]. A versão utilizada foi a *USAGI-patched Mobile IPv6 for Linux* (UMIP) 0.4.

4.3.1 Funcionamento

Antes de se poder proceder a uma avaliação do protocolo é necessário perceber o seu funcionamento, isto é, é necessário proceder a uma análise do seu processo de funcionamento tendo em conta a arquitetura que se pretende estudar. Como se pretendem estudar dois tipos de *handover*: entre redes homogéneas e entre redes heterogéneas, torna-se importante perceber o comportamento do protocolo em cada uma destas situações.

Um aspeto crítico num protocolo de mobilidade é a sua capacidade de detetar o movimento dos MNs, sendo que o protocolo MIPv6 define que esta é realizada pelo próprio MN. Assim, durante esta subsecção, a análise efetuada será para o UMIP implementado no MN, focando-se no processo de decisão de *handover*.

4.3.1.1 Funcionamento do UMIP implementado no MN

O UMIP utiliza os pacotes RA enviados pelos diversos *routers* existentes para fazer a deteção do movimento, tal como o protocolo MIPv6 especifica. Através da receção destas mensagens, o MN terá acesso a uma série de informações como: o prefixo da rede à qual pertence o *router* que enviou a mensagem; se o MN se encontra na sua HN ou numa FN; o

tempo desde o ultimo RA recebido de forma não solicitada; e detalhes sobre o seu HA.

Depois de recebido o RA, o UMIP começa por verificar se o endereço *link local* da interface de onde a mensagem é proveniente é válido, caso não seja, este pacote é descartado e o programa volta à sua fase inicial.

Caso passe esta verificação, o passo seguinte é verificar se o *router* registado na interface que recebeu o RA (*default router*) corresponde ao *router* que enviou o RA. Se os dois *routers* coincidirem é atualizada a informação referente a este e o programa volta à fase inicial, caso não coincidam, a informação relativa à interface é atualizada, sendo definido o novo *router* como *default router*.

O passo seguinte é verificar se o MN se encontra ligado à sua HN, se tal acontecer o MN vai-se permanecer ligado a esta sem ter em conta as outras ligações presentes. Se o MN não tiver ligação com a sua HN, é verificada a existência de ligação em alguma interface do MN. Caso esta exista, é dada uma preferência a esta interface e se o RA tiver sido recebido através de outra é automaticamente descartado. Caso o MN não tenha ligação em nenhuma interface, ou a interface em que está ligado corresponde à interface de que recebeu o RA, é invocada a função *mn_get_iface* para obter a nova interface, seguindo-se a atualização do CoA e nova verificação da igualdade entre a interface atual e a interface determinada. Caso estas interfaces coincidam, o processo de *handover* é ignorado e o programa volta à fase inicial; caso as interfaces sejam diferentes procede-se à realização do *handover*.

4.3.2 Limitações e melhorias no UMIP

Tendo em conta o funcionamento do UMIP, no que diz respeito à forma como este determina a necessidade de ocorrer um *handover*, percebe-se que este apresenta algumas lacunas, das quais se destacam:

- Não permite a utilização de mais de um CoA por interface;
- É dada sempre preferência pela HN. Mesmo que existam outras redes com melhor qualidade de ligação, o MN irá sempre ligar-se à sua HN;.
- Não permite a realização de *handover make-before-break*, ou seja, é necessário perder a ligação com a rede atual para serem consideradas novas redes.

Durante o trabalho desenvolvido ao longo desta Dissertação não foi efetuada qualquer alteração no UMIP, sendo no entanto utilizada uma versão modificada por Capela et al. [87], que dá resposta às limitações apresentadas. As principais funcionalidades introduzidas são:

- Capacidade de intervir no processo de escolha da interface para a qual se pretende realizar *handover*;
- Foi retirada a preferência pela HN, deste modo esta é tratada de forma igual a uma FN;
- Capacidade de comunicação com uma entidade externa, através de um processo de comunicação "cliente-servidor"baseado em *sockets*.

Tendo em conta esta comunicação, foi necessário desenvolver um mecanismo capaz de comunicar com o UMIP, indicando-lhe qual a interface para a qual este deve efetuar o *handover*. Este mecanismo funciona integrado com o gestor de mobilidade desenvolvido e apresentado na Secção 4.5. Este força o UMIP a efetuar *handover* para a interface pretendida.

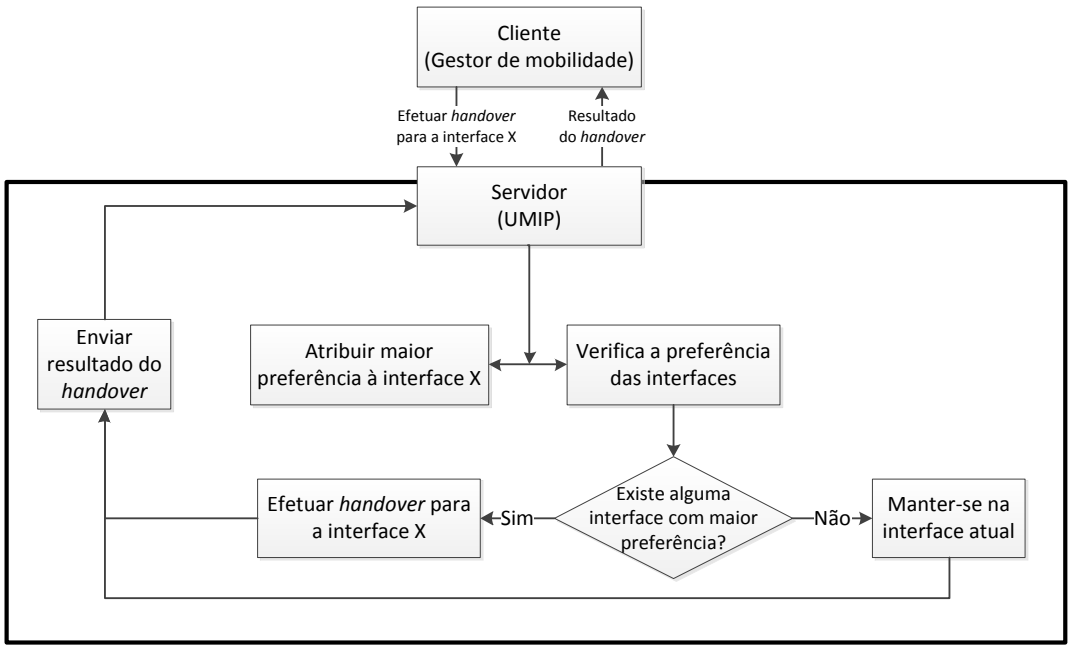


Figura 4.3: Diagrama de funcionamento do mecanismo que permite forçar o *handover* para a interface escolhida (adaptado de [87])

Como se pode observar na Figura 4.3, a decisão de desencadear um *handover* entre redes heterogéneas começa no Gestor de Mobilidade. Este, depois de determinar que uma interface oferece melhor qualidade de ligação à rede que a interface atual, utiliza o mecanismo desenvolvido para efetuar a comunicação com o UMIP, indicando-lhe para que interface deve realizar o *handover*. Este, depois de receber a informação acerca da interface para a qual

deve efetuar *handover*, utiliza um sistema de preferências, atribuindo a maior preferência à interface indicada, realizando assim o *handover* para esta. Depois de concluído este processo, o UMIP envia uma mensagem a informar se o *handover* foi bem-sucedido.

4.4 PMIPv6

Para ser possível testar o protocolo PMIPv6 foi necessário recorrer a uma implementação em *Linux* deste protocolo. A implementação utilizada foi a *OpenAirInterface Proxy Mobile IPv6* (OAI PMIPv6) [88], uma implementação *open source* baseada na implementação do MIPv6 apresentada na secção anterior. A versão utilizada do OAI PMIPv6 foi a 0.4.1.

4.4.1 Funcionamento

Antes de se poder passar a uma análise do desempenho do protocolo foi primeiro necessário perceber o funcionamento da implementação utilizada, de modo a ser possível detetar possíveis lacunas, bem como a melhor forma para as ultrapassar. Assim, durante esta secção será explicado o processo de funcionamento da implementação do protocolo PMIPv6 utilizada. Primeiro será explicado o funcionamento dos MAGs, pois o processo de gestão de mobilidade inicia-se nestes, e seguidamente será explicado o funcionamento do LMA.

4.4.1.1 Funcionamento do MAG

Um dos processos mais importantes de um protocolo de mobilidade é a deteção do movimento dos nós, ou seja, um protocolo para ser eficaz tem de ser capaz de detetar o movimento dos MNs sem muito atraso, para minimizar o tempo de perda de ligação. O protocolo PMIPv6 define que a entidade responsável por este processo é o MAG. O OAI PMIPv6 apresenta duas formas de detetar este movimento: uma é através de mensagens de associação e desassociação geradas pelos *Access Point*s (APs) Cisco Aironet 1100 series (esta implementação foi realizada para uma *testbed* que utilizava este APs); a outra forma de detetar o movimento é através de mensagens de RS. Assim, quando o MAG inicia, a primeira operação que este realiza, depois das devidas inicializações, é iniciar as capturas referidas. O OAI PMIPv6 baseia todas as suas operações numa máquina de estados finitos, responsável por todas as decisões e ações realizadas pelo programa. Deste modo, o segundo passo do programa é iniciar esta máquina de estados finitos.

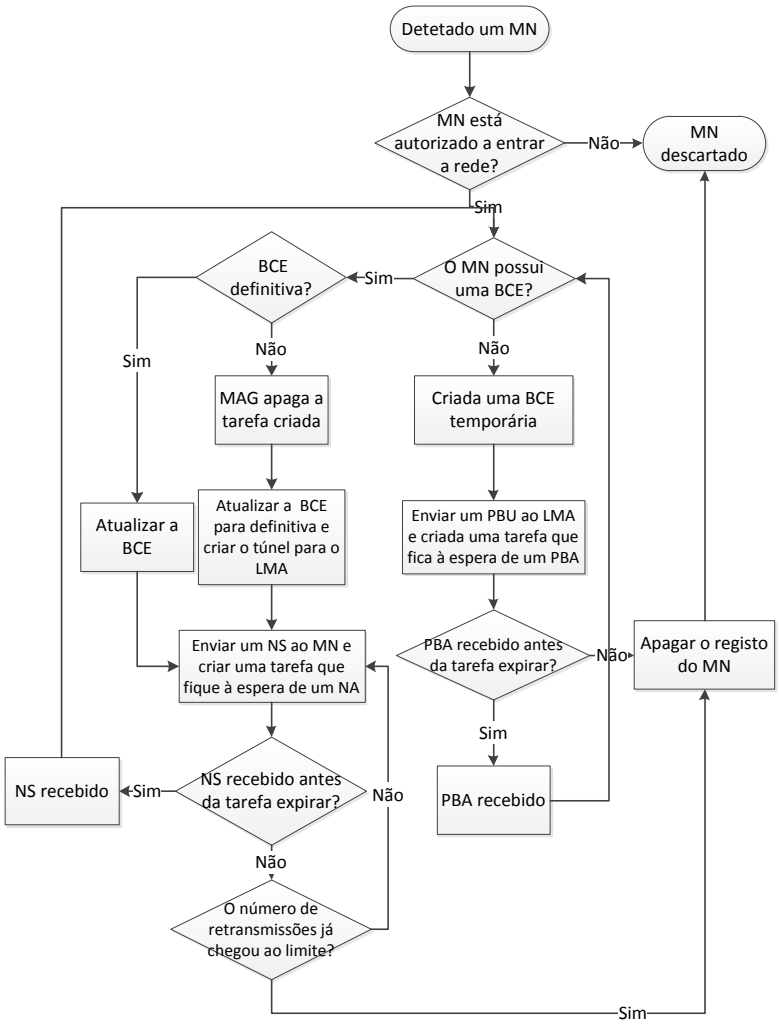


Figura 4.4: Diagrama de fluxo do funcionamento MAG

Depois de realizadas as inicializações, o programa fica à espera até detetar o primeiro pacote, através das capturas iniciadas anteriormente. Quando isto acontece, a máquina de estados finitos, implementada pelo módulo *pmip_fsm.c*, faz o tratamento deste pacote. Esta começa por verificar o MN-ID para verificar se o MN já possui uma BCE. A partir desta informação o programa pode seguir três caminhos diferentes:

- Se o MN não possui uma BCE é desencadeado o processo de registo;
- Se o MN possui uma BCE temporária, o MAG finaliza o processo de registo criando o túnel e as respetivas rotas para o MN;

- Se o MN possui uma BCE definitiva, o MAG atualiza o registo do MN.

Quando o MN não possui uma BCE, significa que o MN foi detetado pela primeira vez e é necessário que se faça todo o processo de registo imposto pelo protocolo. Para tal, o OAI PMIPv6 começa por verificar se o MN tem autorização para entrar na rede, utilizando o programa freeradius-client-1.1.6 [89]. Se o MN passar esta verificação é criada uma BCE temporária. Para realizar esta operação é chamada a *mag_pmip_md* que preenche todos os campos da BCE definidos pelo protocolo. Assim que esta operação é concluída, é invocada uma nova função *mag_start_registration* que é responsável por enviar a mensagem PBU para o LMA; depois de esta ser enviada, é criada uma tarefa que fica à espera da mensagem PBA durante um intervalo de tempo pré-definido. Se o PBA não for recebido dentro desse tempo a BCE é apagada.

Assim que o PBA é recebido, o programa volta à máquina de estados finitos, mas agora como o MN possui uma BCE temporária, o MAG vai começar por apagar a tarefa criada, para que a BCE não seja apagada; de seguida vai invocar a função *mag_end_registration*. Esta função começa por alterar a BCE para definitiva, cria uma tarefa que irá verificar periodicamente se o MN ainda se encontra no seu alcance, através de mensagens de *Neighbor Solicitation* (NS). Para finalizar o processo de registo do MN é criado o túnel entre o MAG e o LMA, e de seguida é invocada a função *mag_kickoff_ra* que envia um pacote RA ao MN contendo o seu HNP. Nesta altura está concluído o registo do MN.

A partir do momento em que o MN tem uma BCE definitiva, o MAG, devido à tarefa criada anteriormente, vai verificar periodicamente se o MN ainda se encontra no seu alcance. Para tal é enviado um pacote de NS ao MN, utilizando a função *ndisc_send_ns*. De seguida é criada uma tarefa que fica à espera de receber a resposta por parte do MN, ou seja, fica à espera de uma mensagem *Neighbor Advertisement* (NA). Caso tal não aconteça dentro de um certo tempo, pré-determinado, o processo é repetido um número de vezes configuradas pelo utilizador. Se mesmo assim não for recebida uma resposta, o registo do MN é apagado, ou seja, é apagada a BCE, é decrementado o número de utilizadores do túnel (se for zero este é apagado), é removida a rota para o MN e finalmente é enviado um PBU ao LMA informando-o que o MN já não se encontra ao alcance do MAG. Caso o MAG receba o pacote do MN, o programa volta à máquina de estados finitos, sendo que desta vez a BCE é definitiva. Neste caso é chamada a função *mag_end_registration_no_new_tunnel* cujo procedimento é em tudo idêntico à utilizada quando a BCE era temporária (*mag_end_registration*), apenas diferindo na criação do túnel e da rota para o MN, que não são necessárias.

4.4.1.2 Funcionamento do LMA

No protocolo PMIPv6, o LMA é a entidade responsável pela gestão da mobilidade. Este mantém registo com a localização atual de cada MN. A implementação do LMA, no OAI PMIPv6, baseia o seu funcionamento no módulo *pmip_fsm.c*, ou seja, na máquina de estados finitos.

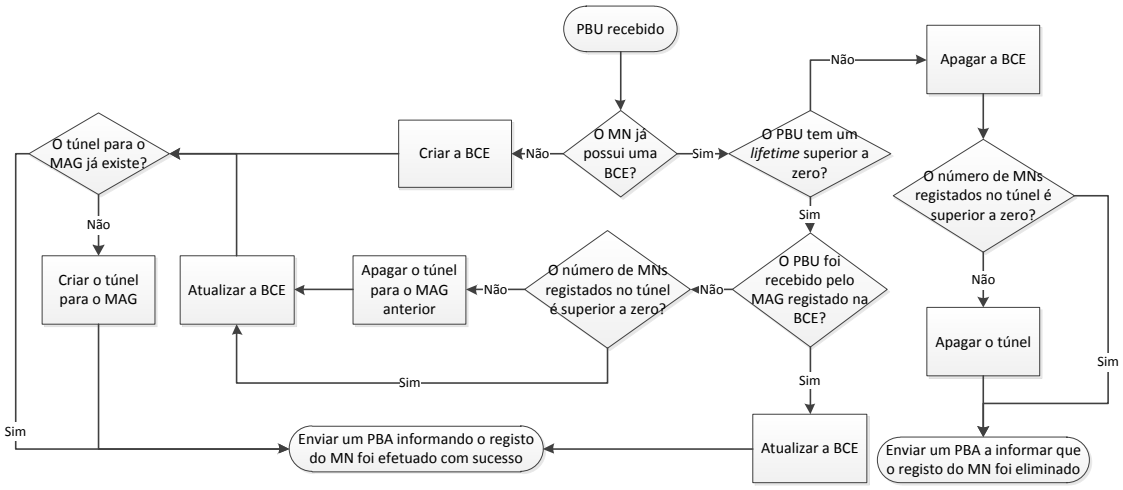


Figura 4.5: Diagrama de fluxo do funcionamento LMA

Quando o LMA é iniciado são efetuadas as devidas inicializações e de seguida é iniciada uma captura de pacotes PBU, pois estes são os únicos que o LMA necessita de receber (Figura 4.5). Depois de efetuada esta inicialização, o LMA fica em espera até receber o primeiro PBU. Quando isto acontece, o programa passa para o módulo que implementa a máquina de estados finita e aí vão existir dois comportamentos possíveis:

- Se o MN que despoletou o envio do PBU não possui uma BCE, o LMA procede ao seu registo;
- Se o MN possui uma BCE, o LMA apenas atualiza o seu registo.

Quando o LMA recebe um PBU com a informação de um MN que não possui uma BCE, o OAI PMIPv6 começa por criar essa BCE com as informações especificadas pelo protocolo PMIPv6. De seguida cria o túnel para o MAG que enviou e, para finalizar o processo de registo do MN, é enviado um PBA para o MAG.

Assim que o LMA recebe um pacote PBU e verifica que o MN que gerou o envio desse pacote possui uma BCE, o programa começa por verificar se o MAG que enviou o PBU é o mesmo que se encontrava guardado na BCE do MN. Caso seja, o LMA envia uma PBA ao MAG e efetua uma atualização nos seus registos. Se tal não acontecer, o LMA começa por apagar os registos que tinha, ou seja, apaga o túnel para o MAG anterior e de seguida apaga a BCE. De seguida, o programa efetua os mesmos passos que verificados no caso em que não existia BCE.

4.4.2 Modificações Efetuadas no OAI PMIPv6

Depois de percebido e testado o funcionamento da implementação do protocolo PMIPv6 utilizada, percebeu-se que esta tinha algumas limitações para cenários que se pretendiam estudar, estas são:

- Não possui qualquer tipo de mecanismo capaz de lidar com interfaces *sit* (IPv6-em-IPv4), necessárias no cenário em estudo devido à ligação 3G utilizada apenas suportar IPv4;
- Não possui um mecanismo de verificação da tecnologia de acesso à rede utilizada pelo MN;
- Falta uma opção de *optimistic handover*, que pode aumentar a eficiência do processo de *handover*;
- O LMA, quando deteta que um MN se moveu entre MAGs, tem um comportamento bastante ineficiente, pois primeiro apaga o túnel, depois o registo, para depois voltar a criar um novo registo e um novo túnel.

Face a estas limitações foram introduzidas alterações na implementação do protocolo PMIPv6 para que estas deixassem de existir. De seguida serão apresentadas as alterações introduzidas.

4.4.2.1 Modificações efetuadas para integração de interfaces *sit* com o OAI PMIPv6

A primeira falha detetada no OAI PMIPv6, quando utilizada uma interface *sit*, foi o facto de quando este recebe uma mensagem de RS através desta interface, necessária para iniciar todo o processo de registo no domínio do protocolo, o programa apresenta uma mensagem de erro e termina a sua execução. Este erro ocorre devido à não existência de MAC *address*

nas interfaces *sit*. Foi então necessário criar uma exceção na função *nd_get_l2addr*, que recebe como parâmetro de entrada o índice da interface e devolve qual o seu MAC *address*, para que quando a interface utilizada for do tipo *sit*, esta função possa indicar que se trata de uma interface deste tipo.

Depois de corrigida esta falha, o programa passou a conseguir receber os pacotes RS através de interfaces *sit*. No entanto, detetou-se que quando o MAG tenta verificar se o MN ainda se encontra no seu alcance, enviando para tal mensagens NS, o MN não responde a esta mensagem. Isto ocorre, pois este tipo de mensagens é utilizada pelo protocolo IPv6 para fazer a descoberta de nós vizinhos. No entanto, como as interfaces *sit* são utilizadas para encaminhar pacotes IPv6 através de redes que apenas suportem IPv4, criando um túnel entre dois endereços de IP para tal, não faz sentido estas suportarem o protocolo de descoberta de nós vizinhos utilizado pelo protocolo IPv6.

Sabendo que a rede 3G tem uma cobertura ampla, quase todo o território português se encontra coberto por esta rede, e como se pretende utilizar esta tecnologia quando não existir mais nenhuma disponível, optou-se por retirar esta verificação do programa, ou seja, o MAG vai proceder ao envio da mensagem PBU, para que o LMA atualize o registo do MN sem verificar se o MN ainda se encontra no seu alcance. O retirar desta verificação vai acabar por reduzir a redundância e o *overhead* introduzido pelo programa, pois como referido, o MN vai estar quase sempre no alcance do MAG. Como a interface 3G é utilizada apenas quando não existe outra forma de acesso à rede, mesmo que o MN não esteja numa área com cobertura da rede 3G, o que vai acontecer neste caso é que os pacotes destinados ao MN, em vez de serem descartados quando chegam ao LMA, serão descartados quando chegam ao MAG.

Para retirar esta verificação foi necessário criar uma exceção na função *pmip_timer_bce_expired_handler*. Assim, depois de criada uma verificação da interface utilizada pelo MAG para comunicar com o MN, foi introduzida uma condição que, caso esta seja *sit*, é invocada a função *mag_force_update_registration*, que como o nome indica irá fazer uma atualização ao registo sem que faça a troca das mensagens NS e NA.

Ainda em relação à integração de interfaces *sit*, como com a alteração anterior o MAG vai enviar periodicamente mensagens a informar o LMA que o MN se encontra no seu alcance, foi necessário desenvolver um mecanismo que faça com que o LMA, depois de verificar que o MN se ligou à rede utilizando outra tecnologia que não o 3G, crie um *timeout* durante o qual o LMA não vai aceitar mensagens PBU que indiquem que a tecnologia de acesso à rede do MN é o 3G. Deste modo, como o MAG não recebe a resposta do LMA, vai apagar o registo daquele

MN e a partir deste momento, quando o MN pretender voltar a utilizar a tecnologia 3G, terá de efetuar um pedido. Se este *timeout* não fosse criado, o LMA iria alternar entre a rede 3G e a outra rede. Para efetuar esta alteração no programa foi necessário criar um campo extra na estrutura *pmip_entry_t*, estrutura que implementa a BC, que indica se o próximo PBU recebido, indicando que a tecnologia de acesso à rede é 3G, pode ser aceite. Assim quando o LMA recebe uma mensagem PBU a informar que o MN pretende aceder à rede através de outra tecnologia que não o 3G, e a tecnologia de acesso à rede guardada na BCE é o 3G, esta variável é igualada a zero, indicando que o próximo PBU recebido que contenha a informação de acesso à rede 3G será descartado. Após este processo, na próxima vez que a BCE for atualizada, esta variável será igualada a 1 e a partir daí o LMA vai voltar a aceitar registos da tecnologia 3G.

4.4.2.2 Modificações efetuadas para integração de um sistema de verificação da tecnologia de acesso à rede

Para que muitas das alterações referidas anteriormente fossem possíveis, foi necessário existir uma verificação da tecnologia de acesso à rede que o MN se encontra a utilizar. Esta verificação não se encontra presente no OAI PMIPv6 sendo que o campo do pacote PBU *Access Technology Type option*, especificado pelo PMIPv6 como obrigatório, era sempre preenchido com o valor referente à tecnologia IEEE 802.11.

De modo a ser possível ultrapassar esta limitação, foi alterada a função *mh_send_pbu*, função responsável pela criação e respetivo envio das mensagens PBU, para que esta, através do índice da interface que o MAG está a utilizar para comunicar com o MN, possa saber qual a tecnologia que está a ser utilizada. Depois de efetuada esta verificação, foi criada uma condição que, em função da tecnologia de acesso, invoca a função *mh_create_opt_access_technology_type* (função que preenche o campo referido) passando como argumento o valor correspondente ao *Access Technology Type* (especificado pelo protocolo) referente a cada tecnologia.

Depois de enviada a informação acerca da tecnologia de acesso utilizada é necessário que o LMA guarde essa informação. Para tal, foi criado um novo campo na estrutura *pmip_entry_t*, denominado *access_technology*. Finalmente, para concluir este processo de verificação da tecnologia de acesso à rede, foi alterada a função *lma_update_binding_entry*, fazendo com que o campo criado anteriormente seja preenchido com a informação existente na mensagem recebida.

4.4.2.3 Modificações efetuadas para integração de um sistema de *optimistic handover*

Antes de serem explicadas as alterações introduzidas para a integração de um sistema de *optimistic handover*, é importante definir o que se entende por este sistema. Assim, um sistema de *optimistic handover* consiste na criação e uso do túnel assim que o PBU é enviado, isto é, sem ser necessário esperar pela receção do PBA. Este mecanismo permite uma redução da latência de *handover*, pois assim que o LMA recebe o PBU e estabelece o túnel para o MAG, pode começar a encaminhar de imediato os pacotes destinados aos MN, não sendo necessário esperar que o MAG receba o PBA para o fazer.

Para implementar este sistema foi necessário efetuar uma série a modificações no programa, a primeira das quais foi a criação de uma nova opção de configuração do MAG, denominada *MAGOptimisticHandover*. Assim, se o utilizador pretender utilizar esta opção terá de incluir no ficheiro de configuração do programa a indicação *MAGOptimisticHandover Enable*. Caso omita este campo ou o coloque como *Disable*, este não será tido em conta e o programa funciona na sua forma original. Depois de criada esta opção passou-se para a implementação do sistema propriamente dito.

Relembrando o funcionamento do MAG, explicado em 4.4.1.1, quando um novo MN era detetado era chamada a função *mag_start_registration*, que iniciava o processo de registo. Para se obter o mecanismo de *handover* otimista, alterou-se esta função para que, caso a opção referida anteriormente esteja ativa, a função comece por criar o túnel para o LMA e de seguida a rota para o MN. A partir deste ponto esta função continua com o seu processo original. Para evitar que quando o MAG receba a resposta do LMA crie um novo túnel, foi criada uma *flag* na estrutura *pmip_entry_t*, denominada *tunnel_already_created*. Assim, quando o túnel é criado na função *mag_start_registration*, esta *flag* é definida com o valor 1 (correspondente a verdadeiro), para que quando seja recebida a mensagem do LMA se evite a criação de um novo túnel.

4.4.2.4 Modificações efetuadas no LMA para tornar o *handover* mais eficiente

Tal como explicado anteriormente (ver 4.4.1.2), quando o LMA percebe que um MN se moveu entre MAGs, apaga o túnel e o registo referente a esse MN, para de seguida criar um novo registo e um novo túnel. Este procedimento não apresenta problemas num cenário de *handover* entre redes homogéneas com associação. No entanto, nos cenários que se pretendem estudar durante esta Dissertação este procedimento levará a um aumento da latência de

handover.

Para fazer face a este problema foi alterada a função *lma_update_binding_entry*, passando o túnel para o novo MAG a ser criado nesta. Depois de este ser criado, a função retoma o seu funcionamento original, ou seja, apaga o túnel para o MAG anterior e de seguida atualiza os registos. Na implementação original, a criação do novo túnel não é realizada nesta função. Assim, para que se evite a criação de um novo túnel, quando a função que originalmente o faria for invocada, foi utilizada a *flag* referida em 4.4.2.3 (não irá existir qualquer conflito, pois o programa ou executa como LMA ou como MAG, nunca os dois em simultâneo) para indicar que o túnel já foi criado. Desta forma foi criada uma verificação na função que criava o túnel originalmente, para que esta apenas o crie se a *flag* estiver definida com o valor correspondente a falso.

4.5 Gestor de Mobilidade

Durante o seu movimento os veículos podem encontrar várias RSUs. Este gestor de mobilidade tem como principal objetivo escolher a ligação que oferece melhor qualidade de sinal e efetuar a ligação a esta rede, ao nível da camada de ligação de dados. Como a *testbed* utilizada suporta três tecnologias de acesso à rede diferentes, o gestor de mobilidade vai também escolher e efetuar a ligação com a rede que oferecer melhor qualidade de ligação, no caso das tecnologias acesso IEEE 802.11p e IEEE 802.11g. No caso do 3G assume-se que existe sempre ligação com a rede e esta é utilizada apenas quando nenhuma das outras está disponível, pois o 3G tem uma latência muito superior e largura de banda mais baixa, não sendo de todo apropriada a comunicações veiculares.

Este gestor de mobilidade foi programado em *Linux Shell Script*, pois esta permite uma maior rapidez e eficiência já que a grande parte das ações realizadas por este mecanismo são chamadas ao sistema do *Linux*.

O processo de funcionamento do gestor de mobilidade desenvolvido pode ser dividido em três fases: a fase de procura, a fase de decisão e a fase de ligação, as quais serão explicadas de seguida. Este processo de funcionamento pode ser observado através dos diagramas de fluxo esquematizados nas Figuras 4.6 e 4.7.

4.5.1 Fase de procura

O objetivo desta fase é determinar qual a rede, denominada FN na terminologia proposta no protocolo MIPv6 (por cada tecnologia disponível), que oferece melhor qualidade de ligação. Para tal é iniciada uma captura de pacotes na interface IEEE 802.11p utilizando o programa *Tshark* [84]. No futuro a necessidade de utilizar o *Tshark* pode ser substituída pela utilização da informação proveniente nas mensagens WSA, recebidas no CCH. No entanto, na altura em que este gestor de mobilidade foi desenvolvido esta funcionalidade ainda não se encontrava disponível, tendo-se optado por esta abordagem. Para realizar esta captura foi criada uma interface monitor, pois só com estas interfaces monitor é possível ter acesso ao *Received Signal Strength Indicator* (RSSI) dos pacotes. O *Tshark* é ativado executando o seguinte comando:

- *sudo tshark -i mon1 -f icmp6 -t -T fields -E separator= -e frame.time -e radiotap.dbm_ant signal -e wlan.sa >wlan1_scan.txt*

O significado de cada um dos parâmetros é o seguinte:

- ***-i mon1*** - Indica a interface na qual se quer fazer a captura, neste caso é a interface *mon1* que está ligada à interface física *wlan1*;
- ***-f icmp6*** - Filtra apenas os pacotes ICMP6 já que nos interessa saber que redes emitem pacotes RA, que são um tipo específico do protocolo ICMP;
- ***e -T fields -E separator=*** - Faz com que os vários *outputs* do programa venham separados por espaços de forma a facilitar a leitura do ficheiro de texto mais adiante;
- ***-e frame.time*** - Cria um *output* com o instante em que o pacote foi capturado;
- ***-e radiotap.dbm_antsignal*** - Cria um *output* com o RSSI do pacote recebido;
- ***-e wlan.sa*** - Cria um *output* com o MAC *address* de quem enviou o pacote;
- ***>wlan1_scan.txt*** - Envia o *output* do programa para um ficheiro de texto chamado *wlan1_scan.txt*.

Quanto à interface IEEE 802.11g (correspondente à *wlan2* nos equipamentos utilizados), o processo de procura foi realizado utilizando o seguinte comando: *iw wlan2 scan > wlan2_scan.txt*. Este comando procurar todas as redes disponíveis, guardando a informação obtida no ficheiro *wlan2_scan.txt*. De entre as informações guardadas destacam-se: o *Service Set IDentifier* (SSID) da rede e o RSSI, que serão utilizados nas fases seguintes.

4.5.2 Fase de decisão

O objetivo desta fase é tomar a decisão de qual a rede que oferece melhor ligação (tendo em conta o RSSI) por cada uma das duas tecnologias, e no caso de existir ligação através das duas interfaces, decidir também qual a que oferece melhor qualidade de sinal. Para atingir este propósito foi desenvolvido um *script* em linguagem AWK que analisa os ficheiros de texto obtidos na fase anterior.

Este *script* é invocado duas vezes, uma para cada interface, através dos comandos:

- *next_wlan1 = $(awk -f next_FN.awk wlan1_scan.txt)*
- *next_wlan2 = $(awk -f next_FN.awk wlan2_scan.txt)*

Este *script* irá devolver para as variáveis *next_wlan1* e *next_wlan2* qual a rede que oferece melhor qualidade de sinal. O *script* começa por verificar quantas redes diferentes existem, verificando quantos MAC *address* (SSIDs no caso da tecnologia IEEE 802.11g) diferentes existem no ficheiro obtido na primeira fase. A partir deste ponto o *script* tem um comportamento diferente conforme a tecnologia. Para o IEEE 802.11p, sabendo quantas redes existem, cria igual número de *arrays* com dez posições onde irá guardar os valores de RSSI dos últimos dez pacotes recebidos de cada rede. Depois de estes *arrays* estarem preenchidos é feita a média dos valores contidos nos *arrays* e de seguida comparado para verificar qual a maior. Assim que este passo está concluído, o *script* devolve o MAC *address* da rede correspondente ao valor determinado anteriormente. Para o IEEE 802.11g, como cada rede têm a informação do RSSI correspondente, o *script* apenas irá comparar estes valores e determinar o maior, devolvendo o SSID correspondente.

Depois de obtido este valor, o programa principal vai proceder à verificação da rede atual em cada uma das interfaces. Caso não exista ligação ou o valor devolvido pelo *script* AWK seja diferente do valor obtido, o programa vai verificar se existe ligação em ambas as interfaces. Caso nenhuma destas condições se verifique, o programa volta à fase de procura.

Se existir ligação em ambas as interfaces, volta-se a correr o *script* AWK para determinar qual a interface que oferece melhor ligação (esta informação será utilizada na fase seguinte), e de seguida o programa passa para a fase de ligação. Caso exista ligação apenas numa interface ou em nenhuma, o programa passa diretamente para a fase de ligação.

Como referido, o processo de decisão da rede que oferece melhor qualidade de ligação é realizado tendo em conta a força do sinal, sendo que no futuro este pode ser melhorado para incluir outros fatores, como por exemplo, o *bitrate* da ligação, a taxa de utilização da rede ou

preferência dos utilizadores

4.5.3 Fase de ligação

Esta fase tem como objetivo efetuar a ligação ao nível da camada MAC com as redes determinadas previamente e garantir que, se existir mais que uma tecnologia de acesso à rede disponível em simultâneo, o protocolo de mobilidade utilizado utiliza a tecnologia que oferece a melhor qualidade de ligação à rede. Devido às caraterísticas de cada um dos protocolos de mobilidade, esta fase do gestor de mobilidade irá ter comportamentos diferentes consoante o protocolo de mobilidade que se esteja a utilizar.

4.5.3.1 MIPv6

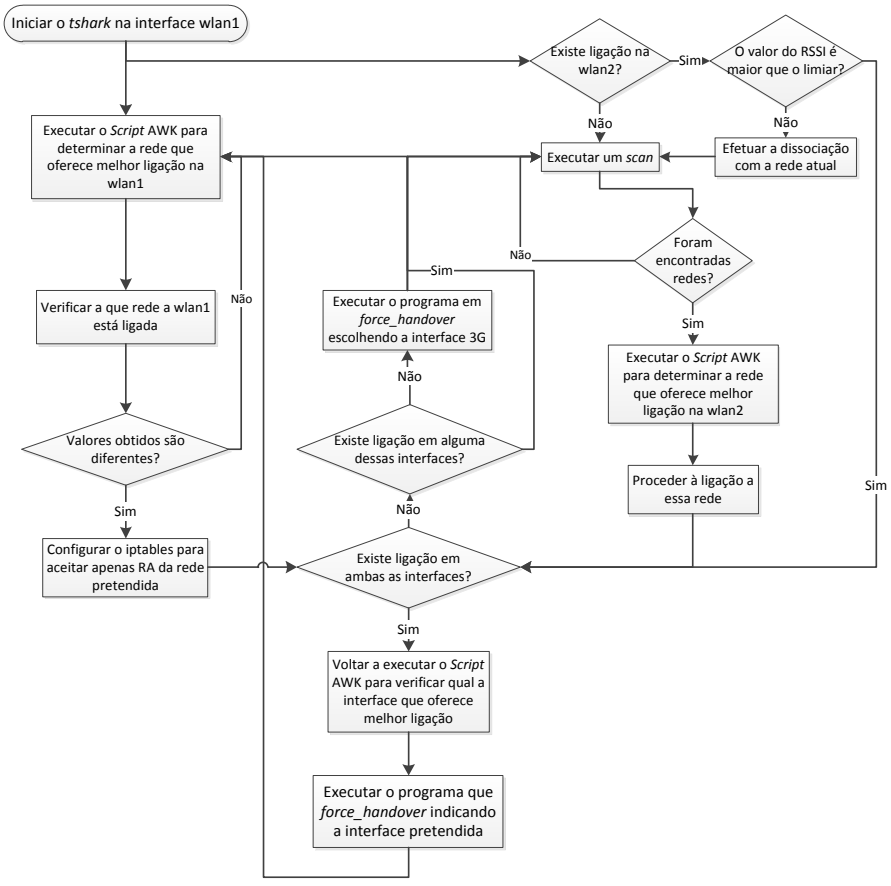


Figura 4.6: Diagrama de fluxo do Gestor de Mobilidade funcionando conjuntamente com MIPv6

O processo de ligação com as redes determinadas na fase anterior é diferente para cada uma das tecnologias. No IEEE 802.11g, como existe associação, é necessário efetuar a desassociação da rede antiga e aí associar à nova. Para tal utilizam-se os comandos do *Linux* apropriados. No IEEE 802.11p, como não existe associação, desde que se esteja no raio de comunicação existe comunicação. No entanto, é necessário garantir que o protocolo MIPv6 apenas regista um CoA, pois a implementação utilizada não suporta mais de um CoA na mesma interface. Desta forma, bloqueiam-se os pacotes de RA de todas as redes exceto a que foi obtida na fase anterior; estes pacotes são utilizados por este protocolo para verificar que existe uma FN à qual se pode ligar. Para tal utilizou-se a ferramenta *Iptables* do *Linux*. Se existir ligação nas duas interfaces é utilizado o programa, descrito em 4.3.2, para forçar o HA a registar o CoA (rede) que oferece melhor qualidade de ligação. Caso não exista ligação em nenhuma das interfaces anteriormente referidas, este programa irá forçar o MIPv6 a utilizar a ligação 3G.

4.5.3.2 PMIPv6

Assim que é determinada qual a rede que oferece melhor ligação é necessário proceder à ligação com essa rede. Mais uma vez este processo é distinto para as duas tecnologias presentes. Caso a tecnologia de acesso à rede determinada no fase anterior seja IEEE 802.11g, a ligação física com a rede é feita utilizando o mesmo processo que se utilizou no caso do protocolo de mobilidade o MIPv6; caso esta seja IEEE 802.11p não é necessário tomar qualquer medida pois a implementação utilizada não apresenta qualquer problema se o MN estiver ligado a mais de uma rede.

Com o PMIPv6, de forma a se obter mobilidade entre as diversas tecnologias foi necessário replicar os *link local* das três interfaces de acesso à rede utilizada para que os diversos MAGs "vissem"as várias interfaces do mesmo MN como pertencentes ao mesmo MN, pois a implementação do protocolo utilizada retira o MN-ID a partir do *link local*. Sendo assim, o PMIPv6 guarda a informação das várias interfaces na mesma BCE, e é então necessário fazer com que o MN apenas registe no domínio do protocolo a interface pela qual obtém melhor acesso à rede. Para tal, utilizando a informação obtida na fase anterior, é enviado um pacote de RS utilizando a ferramenta *ndisc6* [90] pela interface (IEEE 802.11g, IEEE 802.11p ou 3G) que o MN pretende aceder à rede. De seguida faz-se um *timeout* suficiente para que o LMA receba a informação e atualize o MAG a que o MN está ligado. Passado este *timeout*, utilizando a ferramenta *Iptables*, bloqueiam-se os pacotes de NS enviados pelo MAG periodicamente para

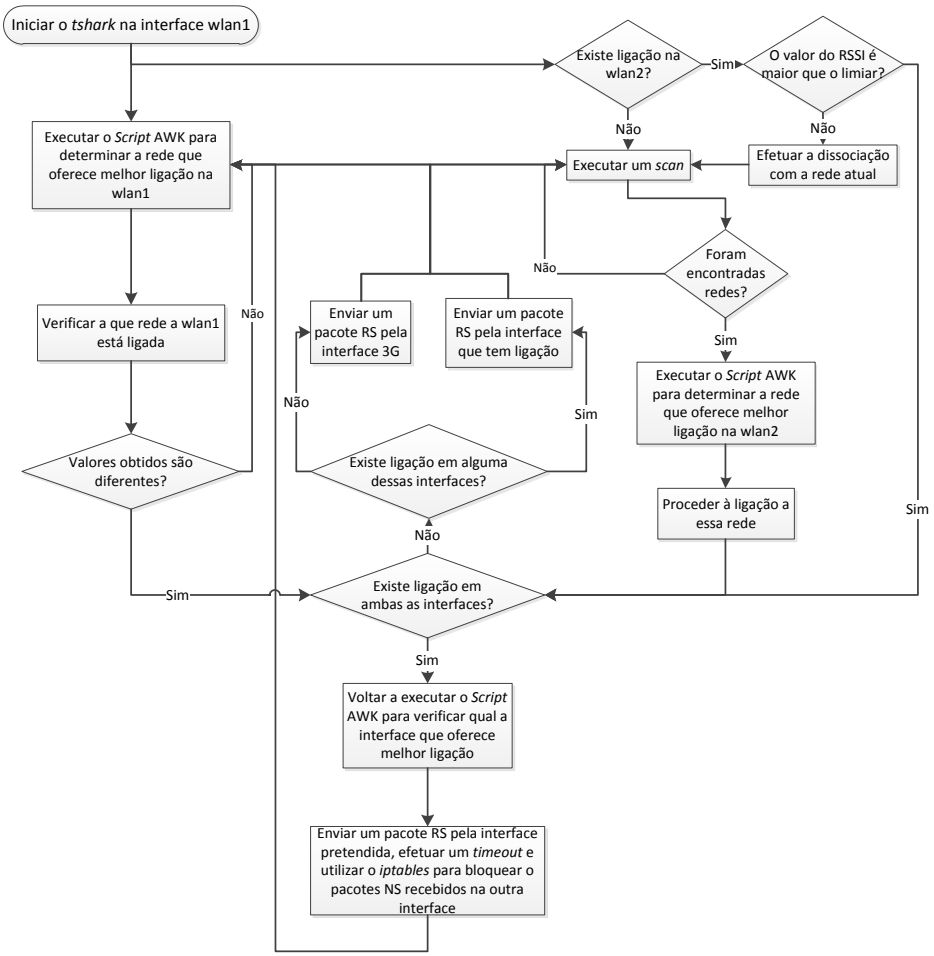


Figura 4.7: Diagrama de fluxo do Gestor de Mobilidade funcionando conjuntamente com PMIPv6

saber se o MN ainda está no seu alcance. Este passo é necessário, pois caso contrário, o MN iria responder ao MAG e este voltava a informar o LMA que o MN estava novamente no seu alcance, e a interface de acesso à rede ficaria em permanente troca até que uma delas deixasse de ter ligação. Tal como no protocolo MIPv6, o MN apenas utiliza o 3G caso não exista ligação com nenhuma das outras tecnologias.

4.6 Sumário

Neste capítulo foram apresentados todos os desenvolvimentos realizados ao nível de protocolos de mobilidade. Numa primeira fase definiu-se a arquitetura que se pretende estudar.

De seguida foram apresentados os protocolos de mobilidade utilizados, descrito o seu funcionamento e apontando pontos que deveriam ser melhorados para poderem funcionar em ambiente veicular de forma otimizada e suportando o IEEE 802.11p. Numa fase seguinte foram descritas as modificações efetuadas.

Por fim foi descrito o gestor de mobilidade implementado, sendo detalhado o seu processo de funcionamento em conjunto com os dois protocolos de mobilidade utilizados, para que seja efetuada a ligação à melhor interface e rede, no sentido de otimizar o processo de comunicação numa rede veicular.

Capítulo 5

Avaliação dos Protocolos de Mobilidade

5.1 Introdução

Depois de desenvolvidos os mecanismos capazes de suportar mobilidade transparente em ambiente veicular, considerando a mobilidade entre as diferentes tecnologias: IEEE 802.11p, IEEE 802.11g e 3G, é importante analisar o seu desempenho. Deste modo, neste capítulo serão apresentados todos os desenvolvimentos necessários para proceder a essa avaliação. Para atingir este objetivo, este capítulo encontra-se dividido em cinco secções.

Na Secção 5.2 são descritas as *testbeds* utilizadas para testar os protocolos de mobilidade, em laboratório e em ambiente veicular. Nesta secção será também apresentado o equipamento utilizado nestas *testbeds*. A Secção 5.3 descreve as métricas que se pretendem obter, de forma a ser possível efetuar a caraterização do processo de *handover*, bem como a metodologia utilizada para a obtenção destas métricas. Na Secção 5.4 são apresentados os resultados obtidos, e é também feita uma análise e discussão dos mesmos. Finalmente, a Secção 5.5 expõem as principais conclusões dos desenvolvimentos realizados neste capítulo.

5.2 *Testbed*

Como foi referido anteriormente, o trabalho desenvolvido no âmbito desta Dissertação pretende avaliar o desempenho dos mecanismos de mobilidade desenvolvidos, com base nos protocolos MIPv6 e PMIPv6, em redes veiculares. Na Secção 4.2 foi descrita a arquitetura que se pretende estudar, e de seguida irão ser apresentadas as várias *testbeds* implementadas

para se poder realizar essa avaliação.

5.2.1 Equipamento utilizado

A arquitetura que se pretende estudar engloba quatro entidades fundamentais em ambos os protocolos. Uma unidade central (denominada HA ou LMA, conforme o protocolo de mobilidade seja o MIPv6 ou o PMIPv6, respetivamente) responsável pela gestão de todo o processo de mobilidade, bem como do encaminhamento do tráfego para o MN. Duas RSU que permitem que o MN se ligue à rede, e finalmente o próprio MN.

Como HA/LMA foi utilizado um PC Toshiba Satellite L755 com sistema operativo UBUNTU 12.04, utilizando a versão 3.2.0-9 do *kernel* do *Linux*, compilado com as opções de suporte aos protocolos de mobilidade ativas. Este encontra-se também equipado com um módulo Wi-Fi TP-Link TL-WN722N e antena preparada para frequências na gama dos 2.4 GHz, com ganho de 4 dBi.

Para as RSUs e MN foram utilizadas as unidades apresentadas anteriormente (ver Secção 3.3), com o suporte das três tecnologias referidas anteriormente.

5.2.2 *Testbed* utilizada para testar o MIPv6

De forma a ser possível efetuar uma avaliação do MIPv6 torna-se necessário desenvolver uma *testbed* capaz de suportar os vários tipos de *handover* que se pretendem estudar. Para tal recorreu-se ao equipamento referido anteriormente e implementou-se a *testbed* esquematizada na Figura 5.1.

Como se pode observar na Figura 5.1 esta *testbed* é composta por várias redes distintas:

- A *Home Network*, rede à qual o MN pertence. Nesta rede encontra-se também o seu HA;
- A rede onde se encontra o CN e por onde o HA comunica com as RSU. Esta rede simula a *Internet* numa rede real;
- As restantes redes são as FNs que proporcionam o acesso ao MN através das várias tecnologias presentes.

Uma das RSU tem três FNs distintas, uma para cada tipo de tecnologia de acesso utilizada, enquanto a outra apenas tem duas, pois como a comunicação através do 3G se efetua do *modem* 3G presente na RSU para a *Base Station* (BS) e daí para o MN, desde que tanto a

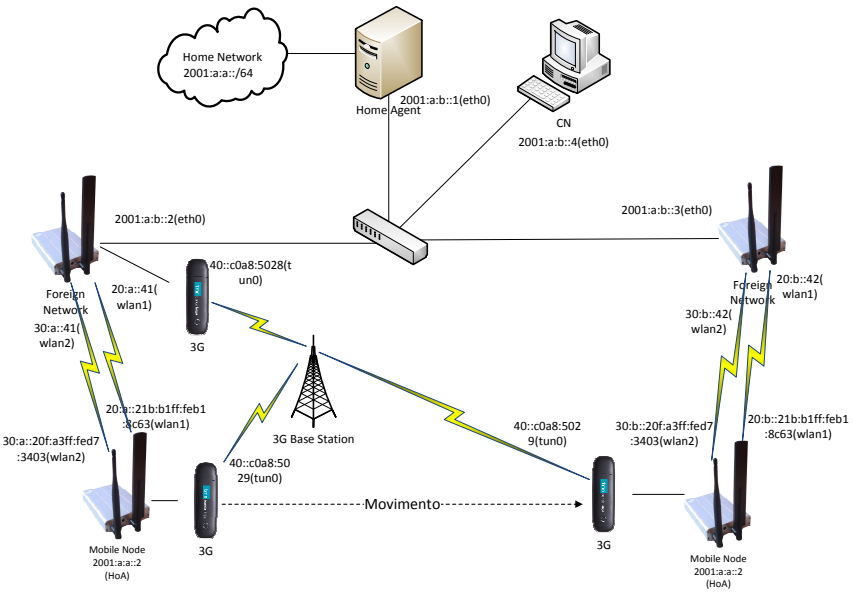


Figura 5.1: Esquema da *testbed* implementada para testar o MIPv6

RSU e o MN estejam no raio de cobertura de uma BS do operador utilizado, irão ter sempre ligação mesmo que estejam em ligados BS diferentes.

Através desta *testbed* podem-se realizar vários tipos de *handover*, tanto *handover* inter-tecnologia como *handover* intra-tecnologia. Assim é possível fazer uma avaliação do comportamento dos mecanismos de mobilidade nos diferentes tipos de *handover*, pois um mecanismo pode ter um bom comportamento em *handovers* entre tecnologias de acesso diferentes, mas mau em *handovers* entre a mesma tecnologia de acesso, ou vice-versa.

Outro aspeto importante desta *testbed* é o facto de suportar a norma IEEE 802.11p/1609.X, dado que não existem estudos do comportamento desta conjuntamente com protocolos de mobilidade. Devido às suas caraterísticas particulares, os resultados e conclusões obtidas com outras tecnologias não podem ser extrapolados para esta tecnologia, a qual irá também criar uma série de novos desafios aos protocolos de mobilidade como se pode verificar ao longo deste capítulo.

5.2.3 *Testbed* utilizada para testar o PMIPv6

Tal como na secção anterior, também para testar o protocolo PMIPv6 foi necessário criar uma *testbed* capaz de fornecer dados sobre os vários tipos de *handover* que se pretendem estudar. A Figura 5.2 esquematiza esta *testbed*, onde se podem observar as várias entidades

que compõem este protocolo.

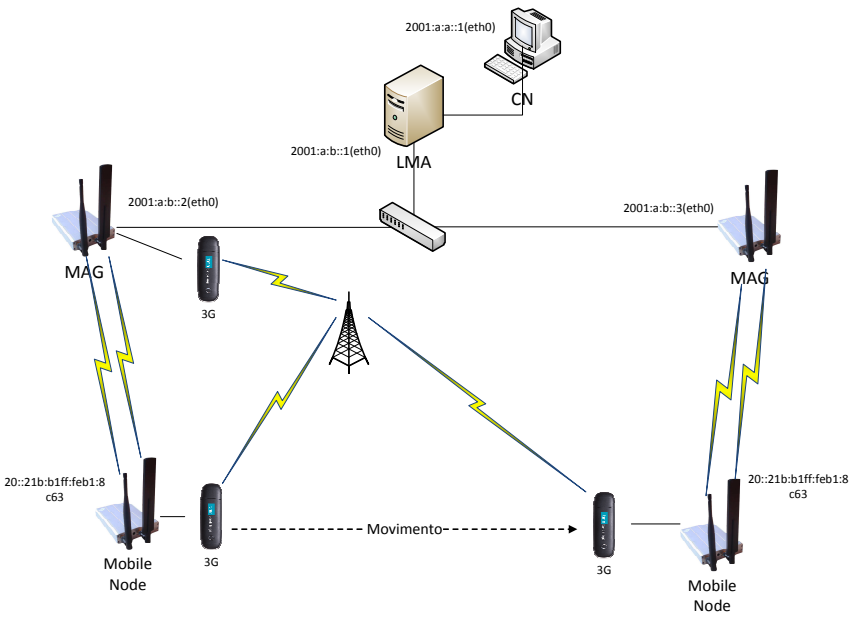


Figura 5.2: Esquema da *testbed* implementada para testar o PMIPv6

Esta *testbed* é em tudo idêntica à que foi utilizada para testar o MIPv6, diferindo apenas nos aspetos relacionados com o funcionamento dos protocolos de mobilidade. Assim, podem-se realizar as mesmas experiências que as da *testbed* anterior. Desta forma será possível fazer uma comparação válida entre os dois protocolos, pois como o equipamento é o mesmo, a única modificação encontra-se nos mecanismos de mobilidade.

Na Figura 5.2 pode-se observar que esta *testbed* é constituída por três redes distintas, sendo esta a principal diferença ao nível do esquema para a *testbed* referida anteriormente.

- A rede pela qual o CN comunica com o LMA, que simula a *Internet* num cenário real;
- A rede que liga o LMA aos vários MAGs existentes no domínio do PMIPv6;
- Por fim, a HN do MN.

A principal diferença entre esta *testbed* e a esquematizada na Figura 5.1 prende-se com o facto de no protocolo PMIPv6 não haver necessidade de existir uma HN no LMA. Neste, ao contrário do que acontece no MIPv6, o mecanismo de mobilidade guarda a informação sobre o MN-HNP dos vários MNs que estão autorizados a entrar no domínio do PMIPv6. Assim que um MAG deteta um MN, será enviado um pacote RA especificamente para aquele MN.

Deste modo, não há a necessidade de existir a HN que existia anteriormente, nem as várias FNs pois o MN comunica com as RSUs através do *link local*.

5.2.4 *Testbed* utilizada para testar o PMIPv6 em cenário veicular

Um dos grandes objetivos do trabalho desenvolvido no âmbito desta Dissertação é poder avaliar qual o desempenho dos mecanismos de mobilidade desenvolvidos em ambiente de redes veiculares. Para tal, como foi referido anteriormente, foram escolhidos dois protocolos de mobilidade para efetuar esta avaliação. Dos testes efetuados em ambiente controlado aos dois protocolos utilizando as *testbeds* referidas nas secções anteriores conclui-se que o protocolo PMIPv6 é o que apresenta melhor desempenho na grande maioria dos testes realizados, como se pode observar na Secção 5.4.3. Deste modo, escolheu-se o PMIPv6 para testes em cenário veicular. Optou-se por este caminho, pois realizar uma *tested* num ambiente veicular envolve uma logística bastante grande, e devido ao facto do MIPv6 não tirar proveito das caraterísticas da norma IEEE 802.11p, testar o MIPv6 numa *testbed* veicular não traria vantagens.

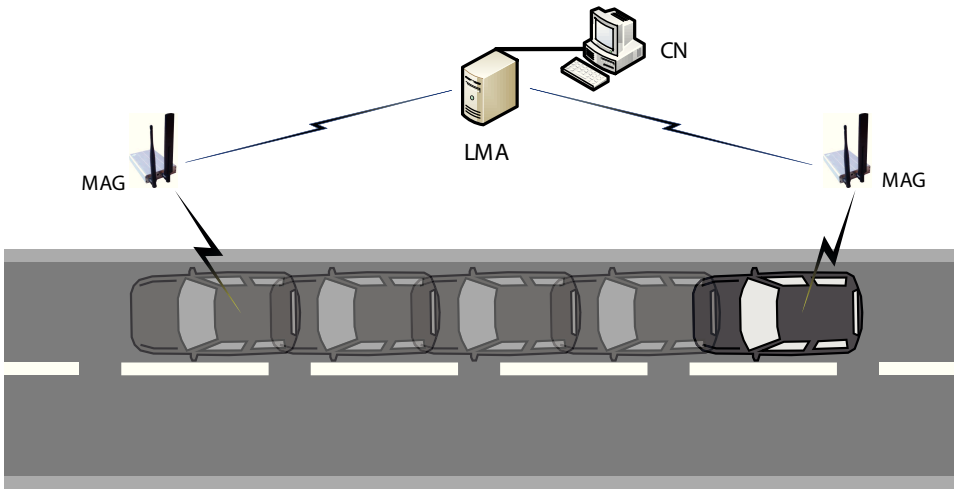


Figura 5.3: Esquema da *testbed* implementada para testar o PMIPv6 em ambiente veicular

Para se poder testar o PMIPv6 num cenário veicular foi necessário adaptar a *testbed* utilizada anteriormente. A grande diferença reside no facto de em ambiente laboratorial se recorrer à ligação *Ethernet* para ligação entre o LMA e os dois MAGs utilizados. Em ambiente veicular, devido à distância entre as RSUs, que suportam os MAGs, e também devido à necessidade de existir um *switch* e consequente alimentação, substitui-se a ligação *Ethernet* por uma ligação IEEE 802.11g. Deste modo será possível testar os cenários de *handover* entre redes IEEE 802.11p.

A Figura 5.3 esquematiza a *testbed* utilizada. Nesta podem-se observar as referidas alterações. É também possível observar a distância entre as RSUs, correspondente a 400 metros. Definiu-se este valor, pois é o valor máximo com que se consegue obter uma boa comunicação entre os MAGs e o LMA. Importa ainda referir que como se definiu o *bitrate* de 12 Mbit/s nas interfaces IEEE 802.11p, estas apresentam um alcance de comunicação máximo de aproximadamente 400 metros. Assim, quando o veículo se encontra na zona compreendida entre as duas RSUs, pode comunicar com ambas, enquanto na parte inicial e final dos testes apenas apresenta comunicação com uma delas.

(a) Montagem das RSUs (b) Montagem da OBU

Figura 5.4: Imagens da montagem das RSUs e OBU

Por fim, para se poder colocar em prática esta *testbed*, foi utilizado um automóvel Fiat Bravo, no qual foi instalada uma OBU, sendo que esta e a respetiva antena foram colocadas no interior do veículo, mais precisamente sobre a bagageira como se pode observar Figura 5.4(b). Quanto às RSUs, estas foram colocadas sobre um tripé, utilizando uma bateria como fonte de energia, como pode ser observado na Figura 5.4(a)

5.2.5 Configurações Necessárias

Depois de idealizadas as *testbed* e escolhido o material para as realizar, foi necessário proceder à sua configuração. Tendo em conta que toda a comunicação presente é baseada em IPv6, o primeiro aspeto a ter em conta foi garantir que todas as entidades presentes utilizam o *kernel* do *Linux* com as opções de suporte IPv6 ativas. Ainda em relação ao suporte de IPv6, foi necessário garantir que o HA/LMA faz o reencaminhamento, utilizando para tal os comando apropriado.

Como o protocolo MIPv6 necessita que as FNs existentes procedam ao envio de pacotes RA, foi necessário utilizar a ferramenta *Router Advertisement Daemon* [91]. Quando utilizado o protocolo PMIPv6, como é o próprio que trata do envio dos RAs, não é necessário utilizar esta ferramenta.

O passo seguinte nas configurações foi a configuração do próprio UMIP ou OAI PMIPv6. Para tal utilizaram-se ficheiros de configuração apropriados, em que as principais configurações realizadas foram ao nível das interfaces utilizadas e dos respetivos endereços.

Para finalizar o processo de configuração foram criados *scripts* que atribuem os endereços de IP às respetivas interfaces, configuram as rotas necessárias e por fim iniciam os programas necessários.

Tabela 5.1: Parâmetros utilizados na configuração das ligações sem fios utilizadas

Parâmetro	**Interface IEEE 802.11p**	**Interface IEEE 802.11g - RSU** 1	**Interface IEEE 802.11g RSU 2**
Canal	174	11	6
Frequência	5.870 GHz	2.463 GHz	2.437 GHz
Bitrate	12 Mbit/s	Adaptativo	Adaptativo
Largura de Banda	10 MHz	20 MHz	20 MHz
TxPower	23 dBm	20 dBm	20 dBm

Em termos de configurações das interfaces sem fios, foram utilizados os parâmetros apresentados na Tabela 5.1. Nas interfaces IEEE 802.11p, em termos de *bitrate*, optou-se pelo valor de 12 Mbit/s devido às razões apresentadas na secção anterior. A largura de banda imposta pela norma, como já foi referido em 2.3.1 é de 10 *MHz*. Por fim definiu-se o TxPower de 23dBm pois é o máximo permitido pela norma.

Nas interfaces que utilizam a norma IEEE 802.11g utilizaram-se canais diferentes para as duas RSUs presentes para minimizar as colisões existentes. Quanto aos restantes parâmetros utilizaram-se as definições mais usuais neste tipo de ligações.

5.3 Metodologia e Métricas

Estando definida a arquitetura que se pretende estudar e as *testbeds* que o possibilitam, o próximo passo é definir as métricas que se pretendem obter, sendo estas as seguintes:

- Tempo de latência do processo *handover*;
- Número de pacotes perdidos durante o processo de *handover*;
- Latência antes, durante e depois do momento de *handover*;
- *Throughput* antes, durante e depois do momento de *handover*;
- *Jitter* antes, durante e depois do momento de *handover*.

Através destas métricas pode-se obter uma caraterização bastante completa do processo de *handover*. A latência de *handover* será a métrica mais importante, pois esta define o tempo de quebra de ligação quando o MN se move de uma rede para outra. O número de pacotes perdidos será também um fator importante, pois este será um complemento da informação obtida através da latência de *handover*. As restantes métricas permitiram retirar conclusões sobre o efeito do processo de *handover* na *Quality of Service* (QoS) oferecida aos utilizadores. Estas métricas possibilitarão também retirar conclusões acerca do desempenho de cada uma das tecnologias estudadas e da sua adaptabilidade para redes veiculares.

Para se obterem as métricas referidas foi necessário gerar tráfego entre o CN e o MN. Para tal recorreu-se à ferramenta *Iperf* [92]. Esta permite a geração de tráfego, utilizando os protocolos de transporte: *Transmission Control Protocol* (TCP) e UDP. Durante todos os testes realizados nesta Dissertação, o tráfego gerado foi enviado recorrendo ao protocolo de transporte UDP, pois como não existe controlo sobre os pacotes entregues, não irão existir retransmissões de dados. Assim, pode-se ter uma noção exata das métricas que se pretendem obter sem que o protocolo de transporte tenha efeito sobre estas. Para além deste aspeto, a ferramenta *Iperf*, quando utilizado este protocolo de transporte, fornece estatísticas com três das métricas que se pretendem obter, sendo estas: o número de pacotes perdidos, o *throughput* e o *jitter*.

Faltam no entanto obter duas das métricas pretendidas, relacionadas com a latência de *handover*. Para tal recorreu-se à ferramenta *Tshark* para capturar os pacotes, tanto na fonte como no recetor. Tendo acesso à informação dos pacotes recebidos, determinar a latência de *handover* é um processo bastante simples, bastando simplesmente fazer a diferença entre o primeiro pacotes recebido através da nova rede com o último recebido pela rede antiga. Para determinar a latência dos pacotes é necessário comparar a informação obtida na fonte e no recetor. Este processo encerra uma grande dificuldade: o sincronismo dos relógios. Para fazer face a esta dificuldade recorreu-se à ferramenta *PTPd* [93], que implementa o protocolo *Precision Time Protocol* (PTP), desenvolvido para providenciar coordenação temporal bastante precisa entre máquinas ligadas em rede. Correll et al. [94] demonstram que esta tem

um desvio máximo na ordem dos 10 μs, sendo suficiente para a medida que se pretendem efetuar, pois a latência dos pacotes será sempre da ordem dos milissegundos, pelo menos cem vezes superior ao erro introduzido pela sincronização dos relógios.

Depois de definidas as métricas que se pretendem obter e as ferramentas necessárias para tal, desenvolveram-se dois *scripts* para automatizar todo o processo. Para a fonte desenvolveu-se um *script* denominado *sender.sh* que, quando invocado, inicia uma captura na interface *eth0* (ou *wlan1* no caso das experiências realizadas em cenário veicular), espera cinco segundos para que o *Tshark* possa ser iniciado e por fim inicia o *Iperf*. Para o recetor desenvolveu-se também um *script*, denominado *receiver.sh*, que segue o mesmo procedimento do *script* anterior, mas em que a iniciação do *Tshark* é feita consoante o tipo de teste que se pretende realizar, ou seja, se por exemplo se pretende efetuar um teste de *handover* entre IEEE 802.11p e IEEE 802.11g, é necessário iniciar o *Tshark* nas respetivas interfaces. Estes *scripts* são ativados utilizando os seguintes comandos:

- *sh sender.sh [IPv6 do destino] [bitrate pretendido] [Nome do teste]*
- *sh receiver.sh [Tipo de teste] [Nome do teste]*

Após obter os resultados, foi necessário proceder à sua análise. Para tal elaborou-se um programa para a ferramenta *MATLAB* [95]. Este programa lê os relatórios produzidos pelo *Tshark* e pelo *Iperf*, tanto na fonte como no recetor, e realiza as operações necessárias para a obtenção das métricas pretendidas.

Por fim, é importante referir que todas as métricas foram obtidas utilizando cinco e dez repetições do mesmo teste, no caso dos testes realizados em ambiente veicular e laboratorial, respetivamente. Os intervalos de confiança apresentados são de 95%.

5.4 Resultados

Antes de se apresentarem os resultados obtidos, é importante realçar que por uma questão de visualização dos gráficos não foram adicionados os nomes completos dos cenários testados mas apenas abreviaturas. A Tabela 5.2 faz a correspondência entro o cenário testado e a abreviatura utilizada nos gráficos que se seguem. Esta correspondência será válida durante todo este documento.

Tabela 5.2: Correspondência entre os cenários em estudo e as referências utilizadas nos gráficos

Nome atribuído	**Cenário**
PtoP	IEEE 802.11p ⇒ IEEE 802.11p
PtoP alt	IEEE 802.11p ⇒ IEEE 802.11p (com comutação de canal)
GtoG	IEEE 802.11g ⇒ IEEE 802.11g
PtoG	IEEE 802.11p ⇒ IEEE 802.11g
GtoP	IEEE 802.11g ⇒ IEEE 802.11p
Pto3G	IEEE 802.11p ⇒ 3G
3GtoP	3G ⇒ IEEE 802.11p
Gto3G	IEEE 802.11g ⇒ 3G
3GtoG	3G ⇒ IEEE 802.11g

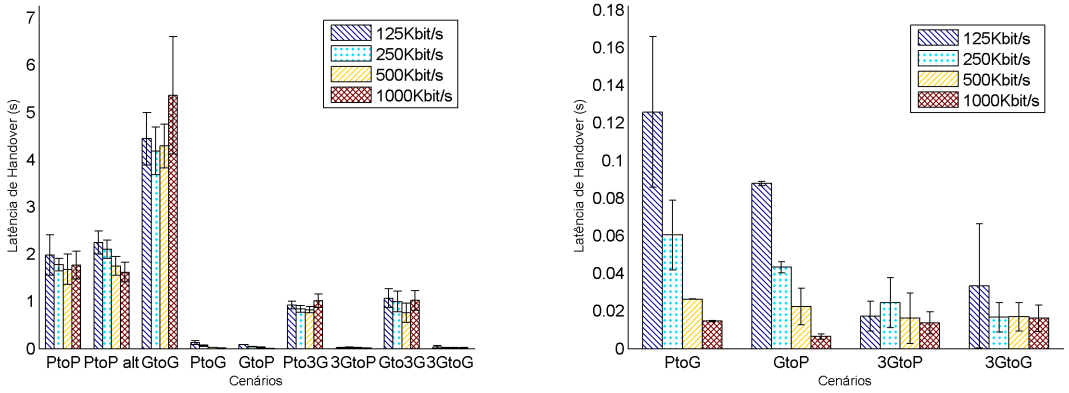
5.4.1 Resultados obtidos com o Protocolo MIPv6

Nesta secção serão apresentadas as métricas obtidas, para as diversas situações de *handover* em estudo, utilizando o protocolo de mobilidade MIPv6. Inicialmente serão apresentados os valores referentes à latência de *handover* e ao número de pacotes perdidos durante o mesmo, e seguidamente serão apresentadas as restantes métricas.

5.4.1.1 Latência de *Handover*

Tal como referido anteriormente, a latência de *handover* é a medida mais importante para caraterizar o processo de *handover*, pois esta define o tempo de perda de ligação quando se efetua o processo de movimentação entre redes. A Figura 5.5 mostra os valores da latência de *handover* obtidos para os diferentes cenários em teste. Na Figura 5.5(a) encontram-se os valores de todos os cenários testados, enquanto na figura 5.5(b) foram retirados os cenários: PtoP, PtoP alt ,GtoG ,Pto3G e Gto3G, para que se possa ter uma ideia mais precisa dos tempos referentes aos restantes cenários.

A Figura 5.5(a) mostra a latência de *handover* nos vários cenários estudados em função do tráfego introduzido na rede, representado pelas várias barras correspondentes a cada cenário. Analisando esta figura pode-se observar que existe uma latência de *handover* da ordem de dois segundos para o cenário de *handover* entre duas redes com tecnologia IEEE 802.11p, quer esta esteja a funcionar em modo contínuo, quer funcione em modo alternado. Este



(a) Todos os cenários

(b) Cenários PtoG, GtoP, 3GtoP e 3GtoG

Figura 5.5: MIPv6 - Latência de *Handover*

tempo *handover* (na ordem dos segundos) explica-se devido ao facto do protocolo MIPv6 não suportar vários CoA na mesma interface, logo para que se efetue o *handover* entre redes homogéneas é necessário apagar o registo da rede antiga e seguidamente esperar que o MIPv6 detete uma nova rede e proceda ao registo de um novo CoA no respetivo HA. A Figura 5.6 mostra toda a troca de mensagens necessária quando o MN efetua o movimento entre redes homogéneas. Todo este processo leva algum tempo a decorrer, explicando-se assim que a latência de *handover* nestes cenários seja de alguns segundos. Outro comportamento que se pode observar através dos cenários referidos anteriormente é o facto de a latência de *handover* não sofrer grande alteração quando a comunicação é efetuada em modo alternado, em relação ao caso de comunicação em modo contínuo. Tal demonstra que é possível obter comunicações de aplicações de lazer no SCH com qualidade, sem no entanto afetar as comunicações de segurança, sendo este um aspeto essencial das comunicações veiculares.

Observando o cenário IEEE 802.11g ⇒ IEEE 802.11g, verifica-se que a latência de *handover* neste caso é mais elevada do que nos cenários anterior. Isto explica-se pois nesta tecnologia, para além do processo referido anteriormente, é ainda acrescentado o tempo necessário para que se proceda à desassociação com a rede antiga e associação com a nova rede. Neste cenário verifica-se também que os diferentes valores de tráfego não têm grande influência na latência de *handover*, não se verificando um comportamento linear com a variação de tráfego inserido na rede.

Passando agora para os cenários IEEE 802.11p ⇒ IEEE 802.11g e IEEE 802.11g ⇒ IEEE 802.11p, visualizando a Figura 5.5(b), pode-se observar que a latência de *handover* é mais

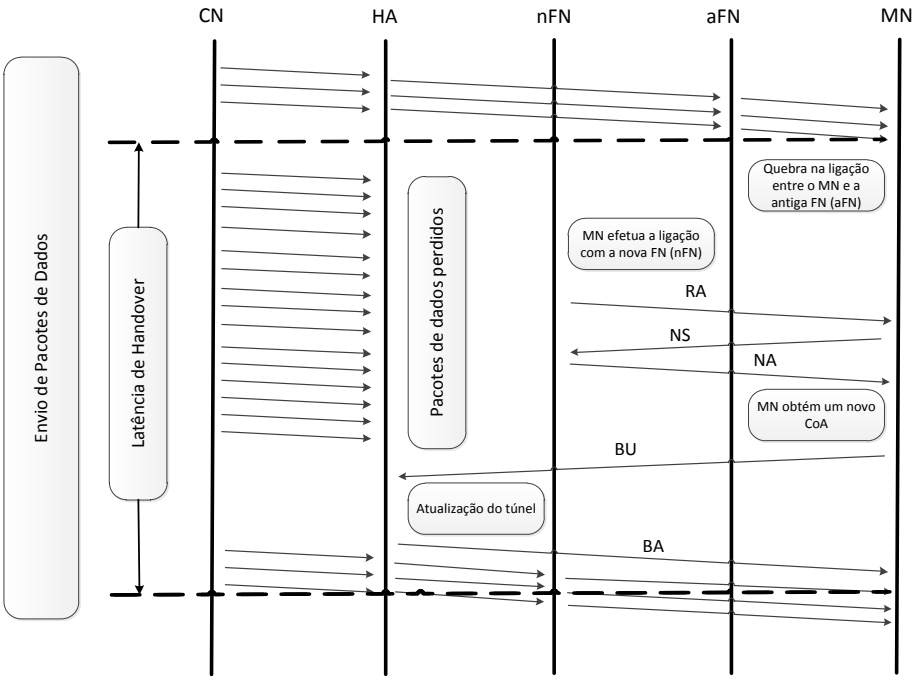


Figura 5.6: MIPv6 - Troca de mensagens durante o *handover* entre redes homogéneas

pequena caso o *handover* se efetue de uma rede com tecnologia IEEE 802.11g para uma rede IEEE 802.11p do que no cenário inverso. Tal deve-se ao facto de a latência ser mais elevada na ligação IEEE 802.11g. Observando ainda a Figura 5.5(b) conclui-se que a latência de *handover* neste dois cenários é bastante pequena, na ordem das dezenas de milissegundos. Este resultado deve-se ao facto de, ao contrário do que acontecia nos cenários anteriores, neste caso, como o *handover* se efetua entre redes heterogéneas, ser possível ter um CoA em cada rede sendo então apenas necessário ao MN informar o HA de qual pretende utilizar. A Figura 5.7 esquematiza a troca de mensagens existente quando se efetua um *handover* entre redes heterogéneas, através da qual se pode perceber que todo o processo de deteção de uma nova rede e de aquisição de um CoA nesta se procede enquanto ainda existe ligação com a rede anterior. Só depois de todo este processo estar concluído é enviado o BU a informar o HA que se pretende alterar o CoA; deste modo quase não existe tempo de perda de ligação durante o movimento entre redes. Ainda para os mesmos cenários, observa-se que a latência de *handover* é inversamente proporcional ao tráfego introduzido na rede, isto explica-se pois a latência de *handover* é medida através da diferença entre o primeiro pacote recebido pela nova rede e o último recebido pela rede antiga. Como se referiu anteriormente, o tempo de perda de ligação entre redes heterogéneas é bastante pequeno, logo quanto maior for o tráfego

introduzido menor é o intervalo entre pacotes enviado, e consequentemente menor irá ser a latência de *handover*.

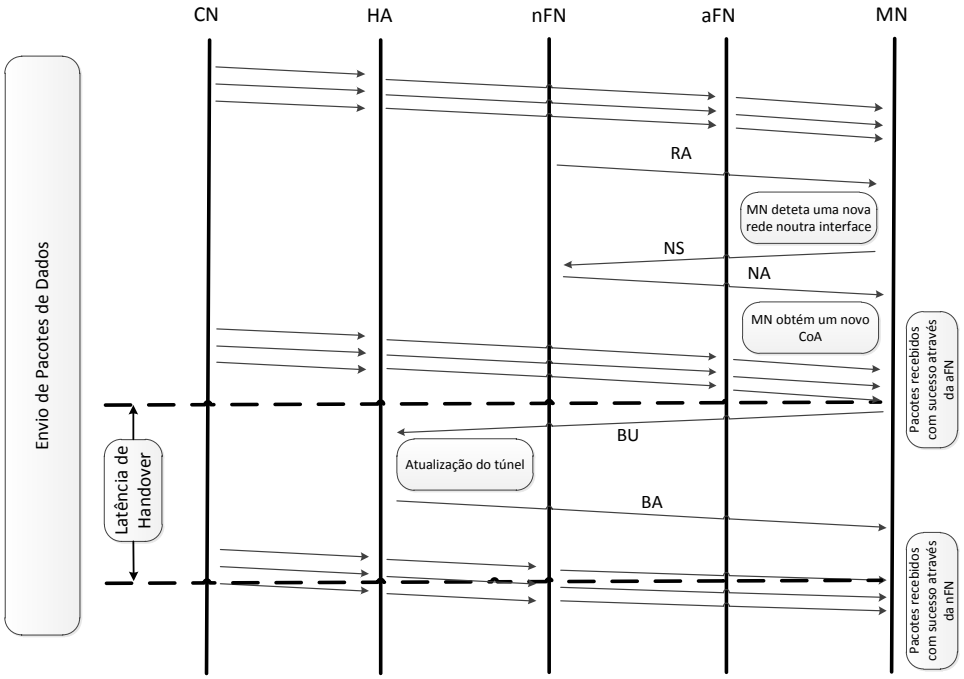


Figura 5.7: MIPv6 - Troca de mensagens durante o *handover* entre redes heterogéneas

Quanto aos restantes cenários, envolvendo a tecnologia de acesso à rede 3G, verifica-se que caso o *handover* se processe de uma rede que utilize tecnologia IEEE 802.11p ou IEEE 802.11g para uma rede que utilize 3G, a latência de *handover* é bastante superior ao caso em que o *handover* se processe de forma inversa. Isto deve-se ao facto de a ligação 3G apresentar uma latência bastante grande, na ordem das centenas de milissegundos, enquanto as ligações IEEE 802.11 apresentam latências bem mais baixas. Em relação ao efeito do tráfego inserido na rede sobre a latência de *handover*, verifica-se que quando este ocorre de IEEE 802.11 para 3G, a latência de *handover* diminui com o aumento do tráfego, tal como acontecia nos cenários explicados anteriormente. Neste caso nota-se ainda que para o tráfego de 1000 Kbit/s acontece um aumento, pois quando se utilizou este valor de tráfego verificou-se que a ligação 3G utilizada não tem capacidade para o mesmo, existindo perda de pacotes de consequente variação no *throughput*. Quando o *handover* se faz de uma rede 3G para uma rede IEEE 802.11 verifica-se que a variação do valor do tráfego não influencia a latência de *handover*; isto acontece pois devido ao valor elevado da latência desta ligação, quando se dá o *handover* para uma rede IEEE 802.11, os primeiros pacotes recebidos por esta interface chegam primeiro

que os últimos pacotes recebidos pela interface 3G.

5.4.1.2 Pacotes perdidos durante o processo de *Handover*

A informação relativa ao número de pacotes perdidos durante o processo de *handover* é um complemento à informação referida anteriormente, pois o número de pacotes perdidos está diretamente ligado à latência de *handover*. Tendo em conta que não é possível definir momentos de início e fim para o processo de *handover*, a informação relativa aos pacotes perdidos será apresentada em valor absoluto, isto é, serão apresentados os valores de pacotes perdidos entre o primeiro pacote recebido pela nova rede e o último recebido pela rede antiga. Tal será válido para todas as informações relativas a pacotes perdidos presentes ao longo deste documento.

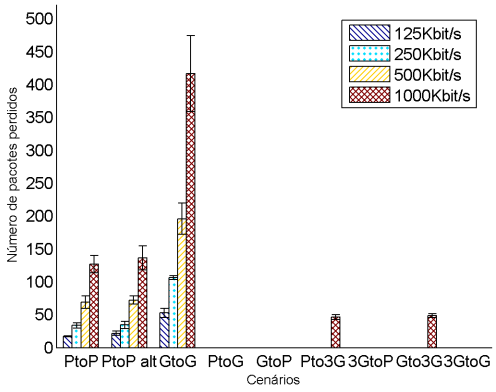
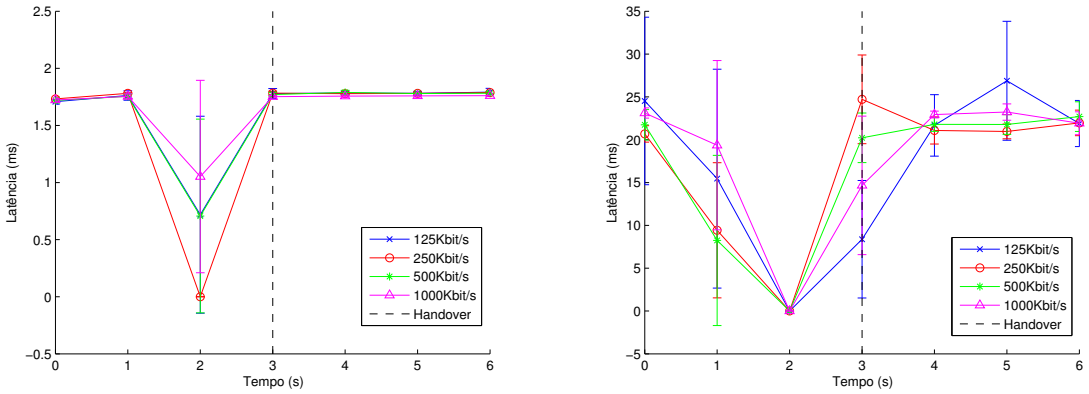


Figura 5.8: MIPv6 - Número de pacotes perdidos durante o *handover*

Através da análise da Figura 5.8 pode-se observar que existem perdas de pacotes bastante significativas nos cenários de *handover* entre redes homogéneas. Verifica-se também que o número de pacotes perdidos é diretamente proporcional ao aumento do tráfego introduzido na rede, facto que era esperado, pois o aumento do tráfego leva a um aumento do número de pacotes e consequente ao aumento do número de pacotes perdidos quando existe perda de ligação.

Outro aspeto que se pode observar na figura 5.8 é a existência de perda de pacotes quando se dá o *handover* de uma rede IEEE 802.11 para uma rede 3G, quando utilizado o *bitrate* de 1000 Kbit/s. Isto acontece devido às mesmas razões apresentadas anterior para o aumento da latência de *handover* nestas situações, sendo esta informação sobre a existência de perda de pacotes nestes cenários, a confirmação do argumento utilizado anteriormente.

5.4.1.3 Latência



(a) Modo contínuo

(b) Modo alternado

Figura 5.9: MIPv6 - Latência durante o *handover* de IEEE 802.11p ⇒ IEEE 802.11p

Para se poder perceber completamente as figuras referentes às métricas: latência, *throughput* e *jitter*, convém referir que nestas estão representados os valores da latência durante sete segundos: durante os primeiros três segundos todos os pacotes são recebidos através da rede antiga; no quarto segundo os pacotes são recebidos através das duas redes, ou seja, o *handover* ocorre durante este segundo; e nos restantes três segundos os pacotes são já todos recebidos pela nova rede. Esta descrição é válida para todas as figuras que serão apresentadas ao longo desta secção e da Secção 5.4.2, nos gráficos referentes às métricas: latência, *throughput* e *jitter*. É feita uma exceção aos gráficos correspondentes ao cenário de *handover* entre IEEE 802.11g ⇒ IEEE 802.11g, que devido ao elevado tempo de perda de ligação foi necessário aumentar o intervalo de tempo mostrado. Deste modo, nos gráficos correspondentes a este cenário, os primeiros sete segundos correspondem à ligação com a rede antiga, no oitavo segundo ocorre o *handover*, e os restantes três correspondem à ligação com a nova rede.

Na Figura 5.9 encontra-se ilustrada a latência durante o *handover* correspondente ao cenário IEEE 802.11p ⇒ IEEE 802.11p: em 5.9(a) está representada esta latência quando esta tecnologia se encontra a funcionar em modo contínuo, enquanto em 5.9(b) está representado o caso em que esta tecnologia se encontra em modo alternado. Na Figura 5.9(a) pode-se observar que a latência apresenta um valor sempre bastante semelhante durante todo o teste; apenas no segundo antes de ocorrer *handover* existe uma diferença, pois como a latência de *handover* neste cenário é de cerca de 1.5 a 2 segundos, e como os valores apresentados neste gráfico foram obtidos através de vários testes, existem testes em que existiu a chegada

de pacotes no segundo anterior a ocorrer o *handover*, enquanto noutro tal não aconteceu. Assim justifica-se o comportamento apresentado no gráfico, de existir uma diminuição da latência no segundo anterior ao *handover*. Através desta figura é também possível observar que a variação do valor do tráfego introduzido não tem influência no valor da latência, pois a ferramenta utilizada para gerar o tráfego utiliza sempre pacotes com tamanho 1470 Bytes de dados. Outro facto que se pode observar neste gráfico são os intervalos de confiança serem bastante apertados, o que revela a qualidade desta ligação, pois mostra que não existe grande diferença entre a latência dos diversos pacotes recebidos.

Observando a Figura 5.9(b), é possível verificar que quando a tecnologia IEEE 802.11p se encontra a funcionar em modo alternado, existe um aumento na latência dos pacotes recebidos, facto que é facilmente compreensível, pois como esta interface comuta entre o SCH e o CCH a cada 50 ms, só existem 50 ms com serviço ativo e 50 ms sem serviço. Logo, quando um pacote chega a esta rede e esta se encontra a transmitir no CCH, este pacote terá de esperar que se faça a comutação para o SCH. Este tempo de espera será refletido na latência final do pacote, levando ao aumento verificado em relação ao cenário em que esta tecnologia se encontra em modo de funcionamento contínuo.

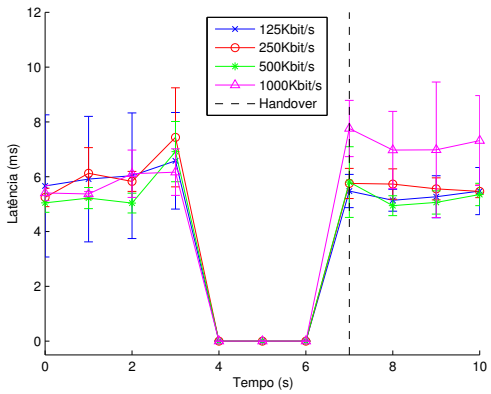
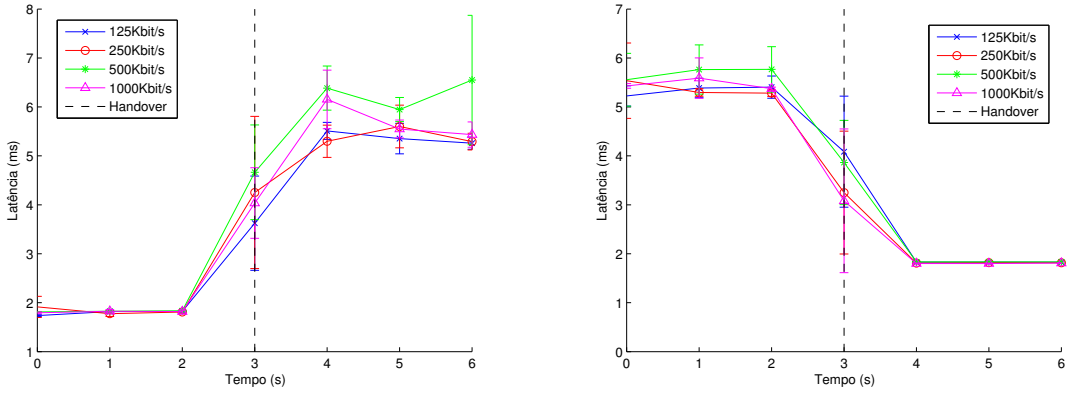


Figura 5.10: MIPv6 - Latência durante o *handover* de IEEE 802.11g ⇒ IEEE 802.11g

A Figura 5.10 mostra a latência durante no cenário *handover* IEEE 802.11g ⇒ IEEE 802.11g. Através desta pode-se verificar que enquanto existem pacotes recebidos a latência mantém um valor relativamente constante, verificando-se apenas um ligeiro aumento no segundo em que ocorre a perda de ligação com a rede antiga; tal pode ficar a dever-se ao facto da qualidade da ligação já ter sofrido uma quebra. Outro comportamento que se verifica é um aumento da latência nos momentos seguintes ao *handover*, quando utilizado o *bitrate* de

1000 Kbit/s. Isto deve-se ao elevado número de pacotes que se tentam transmitir logo que volta a existir ligação, levando a um aumento no tempo nas várias filas de espera existentes, e consequente aumento da latência.

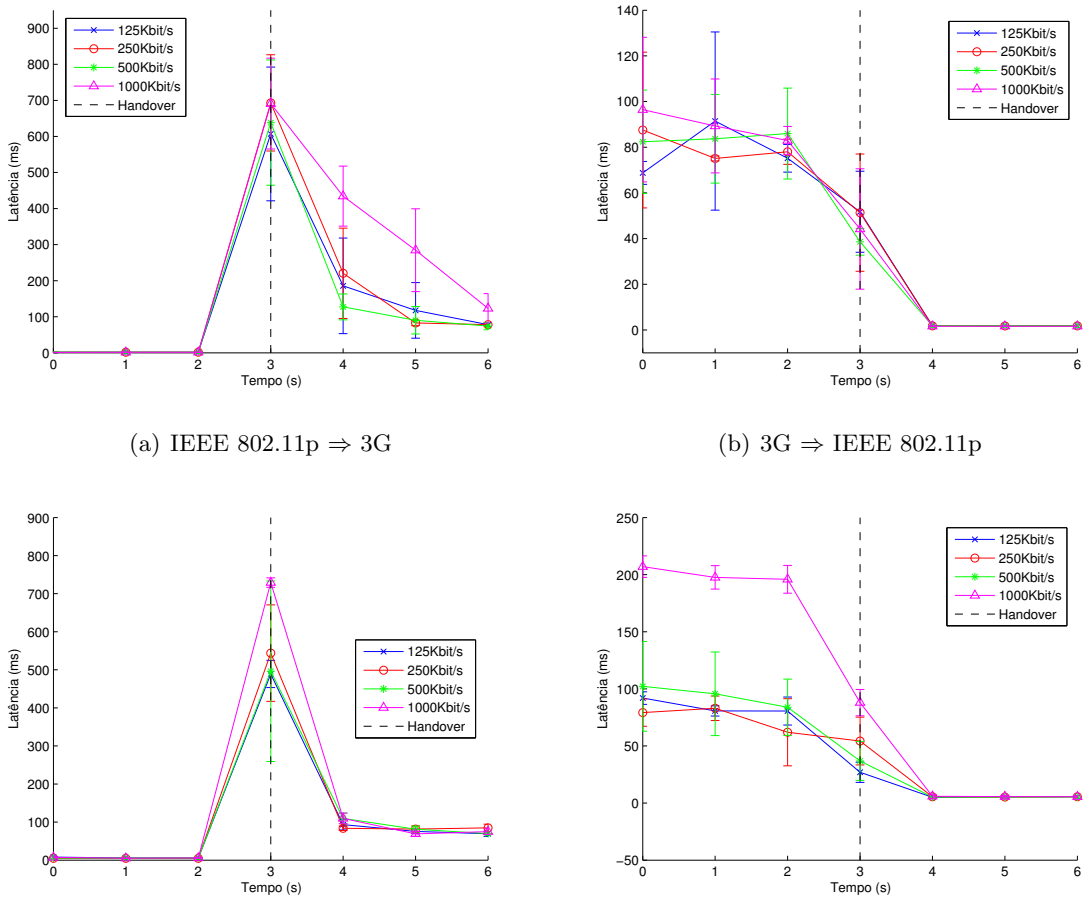


(a) IEEE 802.11p ⇒ IEEE 802.11g (b) IEEE 802.11g ⇒ IEEE 802.11p

Figura 5.11: MIPv6 - Latência durante o *handover* entre IEEE 802.11p e IEEE 802.11g

Na Figura 5.11 estão representados os valores da latência para os casos de *handover* entre IEEE 802.11p ⇒ IEEE 802.11g (a) e IEEE 802.11g ⇒ IEEE 802.11p (b). Analisando estes resultados, observa-se que ambos são bastante similares. Quando os pacotes são recebidos através da interface IEEE 802.11p verifica-se uma latência de cerca de 2 ms, à semelhança do que acontecia na Figura 5.9(a). No instante em que ocorre o *handover* verifica-se que a latência apresenta um valor intermédio, pois são recebidos pacotes através das duas interfaces. Quando apenas existe ligação com a interface IEEE 802.11g, a latência é mais elevada, apresentando valores entre os 5 e os 6 ms.

A Figura 5.12 mostra a latência nos vários cenários envolvendo a tecnologia 3G. Em 5.12(a) e 5.12(c) podem-se observar os cenários IEEE 802.11p ⇒ 3G e IEEE 802.11g ⇒ 3G, respetivamente. Estas figuras são bastante similares, notando-se o mesmo comportamento em ambas. Como o *handover* é feito de uma rede IEEE 802.11 para 3G, a latência começa por ser bastante pequena antes do momento de *handover*; no segundo em que ocorre o *handover* esta aumenta bastante, chegando mesmo a valores próximos dos 700 ms para nos segundos seguintes ao *handover* estabilizar aproximadamente em 100 ms. Este comportamento deve-se ao facto de na ligação 3G não ser possível efetuar a reserva de recursos, ou seja, quando se dá o *handover* para esta rede, esta não está preparada para receber os dados, logo os primeiros pacotes recebidos através desta rede vão sofrer uma latência bastante grande, pois têm de



(a) IEEE 802.11p ⇒ 3G

(b) 3G ⇒ IEEE 802.11p

(c) IEEE 802.11g ⇒ 3G

(d) 3G ⇒ IEEE 802.11g

Figura 5.12: MIPv6 - Latência durante o *handover* entre redes IEEE 802.11 e 3G

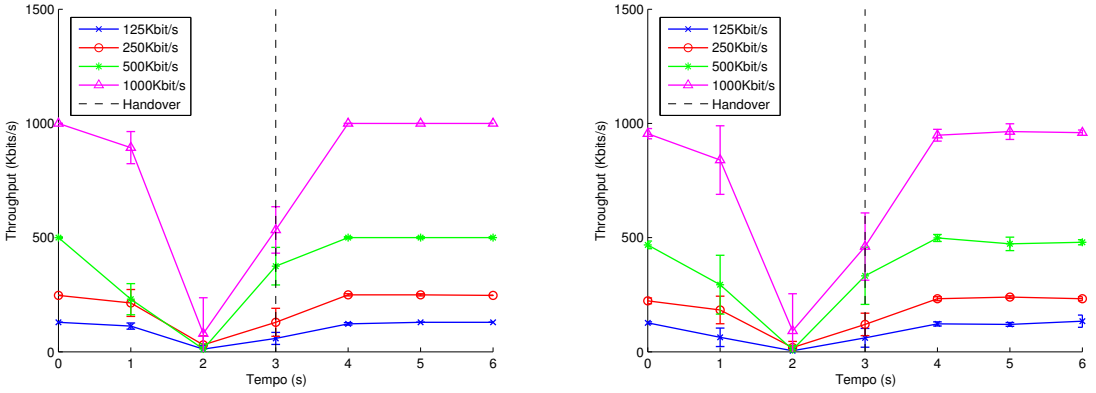
esperar que lhe sejam atribuídos recursos e uma rota até ao seu destino. Um aspeto que merece também ser realçado é o facto de a ligação 3G utilizar uma rede pública, logo todos os testes realizados, envolvendo a mesma, estão sujeitos ao congestionamento existente nesta rede.

Nas Figuras 5.12(b) e 5.12(d) estão representados os cenários 3G ⇒ IEEE 802.11p e 3G ⇒ IEEE 802.11g, respetivamente. Analisando estas figuras observa-se que têm um comportamento similar, facto que era esperado, pois em ambas está representado o *handover* de uma rede 3G para uma rede IEEE 802.11. Estas imagens apresentam o comportamento esperado, ou seja, até ao segundo em que se dá o *handover* a latência apresenta um valor elevado (aproximadamente 100 ms); no segundo em que ocorre o *handover* esta tem um valor intermédio, pois os pacotes chegam através das duas redes, e nos momentos seguintes ao *handover* a

latência estabiliza em valores de poucos milissegundos, como era caraterística das redes IEEE 802.11. A discrepância entre os valores da latência nas curvas correspondentes ao *bitrate* de 1000 Kbit/s, nas presentes em (b) e (d), fica-se a dever às caraterísticas da ligação 3G, não estando esta diferença entre as curvas relacionada com o cenário de *handover* em estudo.

Através da Figura 5.12 é possível verificar que as ligações 3G não são adequadas para comunicações de segurança em VANETs, pois como foi referido anteriormente (ver 2.8.1.1) a latência em comunicações de segurança não deve ultrapassar os 100 ms, o que não pode ser garantido pelas ligações 3G como se pode ver nesta figura.

5.4.1.4 *Throughput*



(a) Modo contínuo

(b) Modo alternado

Figura 5.13: MIPv6 - *Throughput* durante o *handover* de IEEE 802.11p ⇒ IEEE 802.11p

Nas Figuras 5.13(a) 5.13(b) encontram-se as representações do *throughput* nos cenários de *handover* IEEE 802.11p ⇒ IEEE 802.11p, em modo contínuo e em modo alternado, respetivamente. Como se pode observar nestas figuras, existe uma quebra no valor do *throughput* nos segundos antes de ocorrer o *handover*, tal encontra-se de acordo com o esperado.

A Figura 5.14 ilustra o *throughput* durante o *handover* de IEEE 802.11g ⇒ IEEE 802.11g. Nesta pode-se verificar a perda de ligação referida anteriormente, de aproximadamente quatro segundos. Verifica-se também que mesmo nos instantes anteriores à perda de ligação total, já existe uma certa quebra no *throughput* e, em contrapartida, logo no segundo seguinte ao segundo em que se receberam os primeiros pacotes através da nova rede (correspondente ao valor 8 no eixo horizontal da figura), o valor do *throughput* já se encontra completamente reestabelecido. Comparando esta figura com a Figura 5.13, é possível verificar que, mesmo

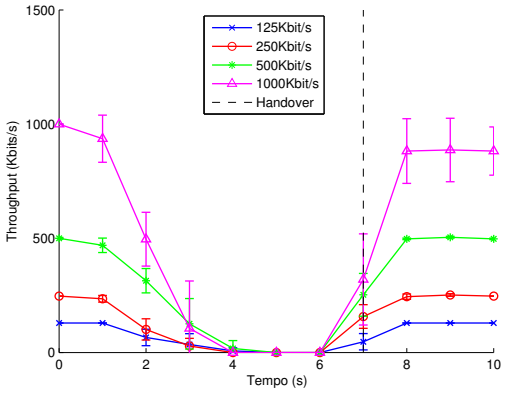
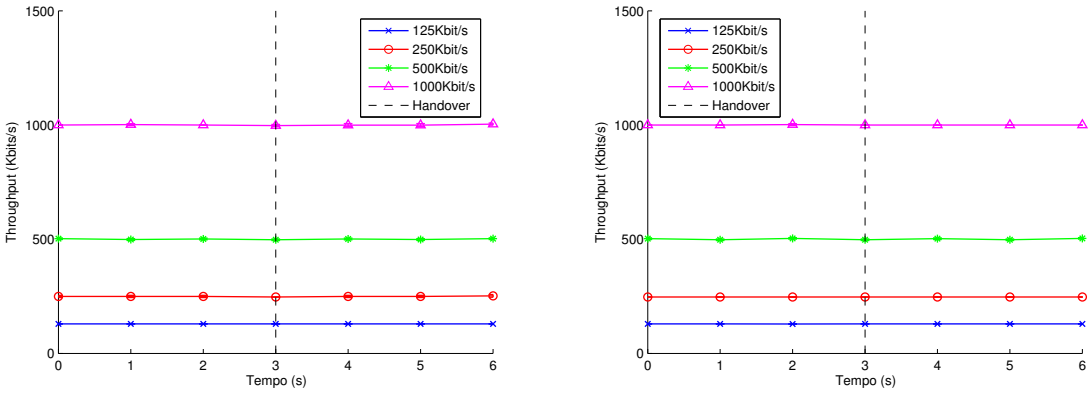


Figura 5.14: MIPv6 - *Throughput* durante o *handover* de IEEE 802.11g ⇒ IEEE 802.11g

existindo tempo de perda de ligação em ambos os casos, no caso em que se utiliza a tecnologia IEEE 802.11p a quebra no *throughput* é muito menor à que ocorre no cenário envolvendo a tecnologia IEEE 802.11g. Este facto explica as vantagens da não existência de associação, pois essa é a grande diferença entre estes cenários.



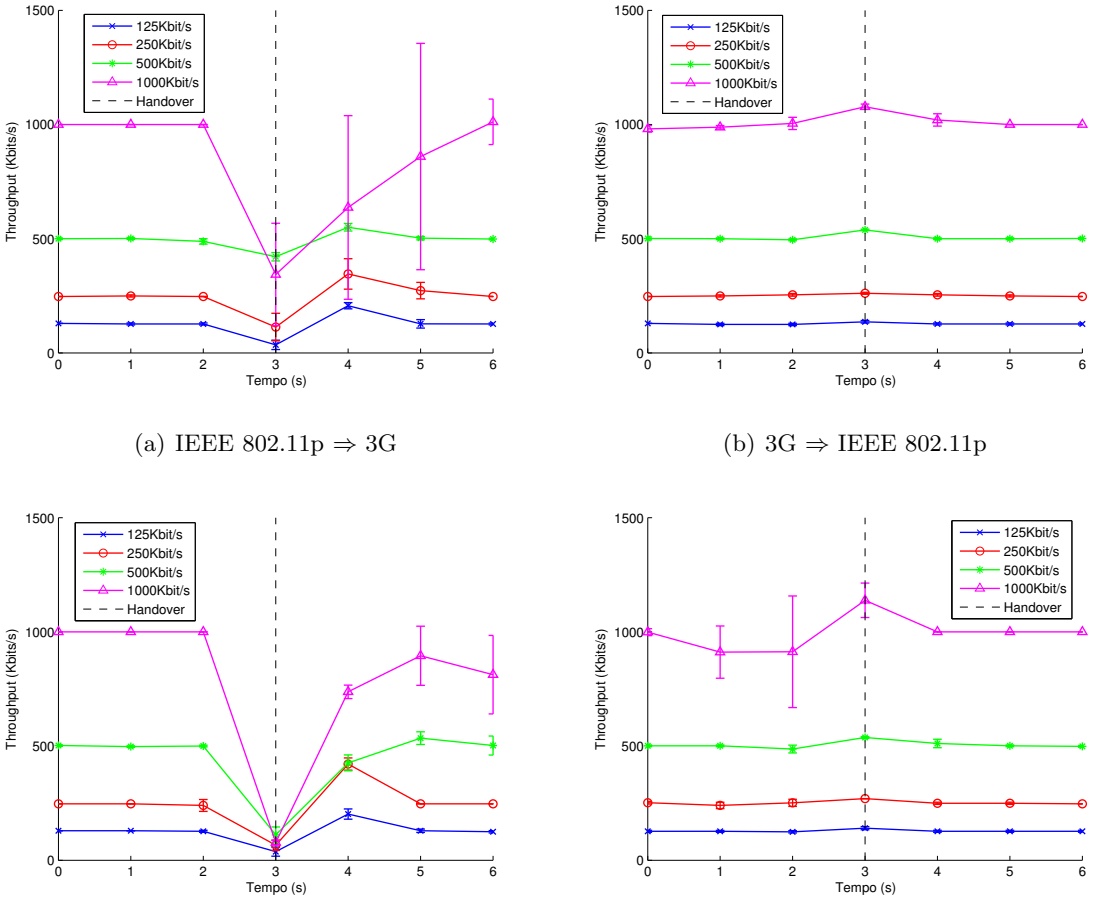
(a) IEEE 802.11p ⇒ IEEE 802.11g

(b) IEEE 802.11g ⇒ IEEE 802.11p

Figura 5.15: MIPv6 - *Throughput* durante o *handover* entre IEEE 802.11p e IEEE 802.11g

Através da análise da Figura 5.15, onde se encontra ilustrado o *throughput* nos cenários de *handover* entre IEEE 802.11p ⇒ IEEE 802.11g e vice-versa, pode-se verificar que não existem quaisquer alterações nas várias curvas, tanto num cenário como no outro. Este facto corresponde ao esperado, pois não existe qualquer perda de pacotes durante o processo de *handover* e a latência de *handover* corresponde, aproximadamente, ao tempo de espaçamento dos pacotes. Conjugando todas estas informações pode-se classificar o *handover* correspondente a

estes dois cenários como *seamless*, ou seja, é um *handover* sem quaisquer perdas.



(a) IEEE 802.11p ⇒ 3G

(b) 3G ⇒ IEEE 802.11p

(c) IEEE 802.11g ⇒ 3G

(d) 3G ⇒ IEEE 802.11g

Figura 5.16: MIPv6 - *Throughput* durante o *handover* entre redes IEEE 802.11 e 3G

A Figura 5.16 mostra o comportamento do *throughput* ao longo dos vários testes efetuados utilizando a tecnologia 3G. Em (a) e (c) nota-se um comportamento semelhante, pois em ambas se apresenta o *throughput* de uma rede IEEE 802.11 para uma rede 3G. Analisando estas figuras, é possível observar uma quebra no valor do *throughput* no instante em que se dá o *handover*; tal deve-se ao mesmo facto enunciado em 5.4.1.3 para explicar o aumento na latência aquando do *handover* nestes cenários, ou seja, esta quebra no *throughput* deve-se ao facto de não ser possível efetuar qualquer reserva de recursos na ligação 3G antes de se fazer o *handover* para este. Assim, quando o *handover* acontece, a ligação não está preparada para receber os dados, levando algum tempo até ao estabelecimento da ligação.

Analisando as Figuras 5.16(b) e 5.16(d) correspondentes aos cenários de *handover* de uma

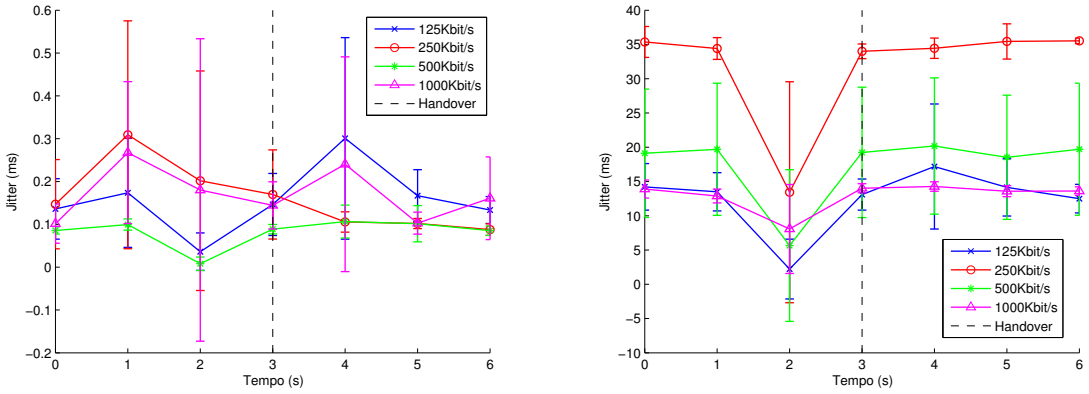
rede 3G para uma rede IEEE 802.11, é possível verificar uma ligeira variação nas curvas no momento em que ocorre o *handover* (ligeiro aumento). Este facto numa primeira análise parece estranho, mas pode-se explicar devido à diferença de latência entre as ligações 3G e IEEE 802.11. Como a latência da ligação 3G é de aproximadamente 100 ms (como se pôde verificar em 5.4.1.3), os pacotes enviados nos últimos 100 ms do segundo anterior ao que ocorreu *handover* irão chegar ao MN já durante o segundo em que ocorre o *handover*. A partir do momento em que efetua o *handover* para a rede IEEE 802.11, a latência dos pacotes passa a ser bem mais baixa, logo quase todos os pacotes enviados no segundo em que ocorre o *handover* são recebidos ainda nesse mesmo segundo. Isto leva a um aumento no número de pacotes recebidos no segundo em que se efetua o *handover* levando a um consequente aumento do *throughput*.

Outro aspeto que se pode observar através dos vários gráficos presentes na Figura 5.16 é a instabilidade no *throughput* quando é utilizado o *bitrate* de 1000 Kbit/s. Tal não seria de esperar, pois a ligação 3G recorre à tecnologia *High-Speed Packet Access* (HSPA), capaz de suportar *bitrates* até 7.2 Mbit/s. Esta instabilidade pode-se ficar a dever a dois fatores: à baixa qualidade do sinal no local onde se efetuou os testes (durante a realização dos mesmos foi-se verificando a intensidade do sinal e numa escala de 1 a 99, a intensidade do sinal situou-se sempre entre os 15 e os 25, nunca se verificando valores fora desta gama), e ao facto da ligação utilizar uma rede pública, logo está dependente do número de utilizadores presentes em cada instante, e da quantidade de recursos que cada um utiliza.

5.4.1.5 *Jitter*

A Figura 5.17 mostra as curvas do *jitter* no cenário de *handover* entre redes que utilizam a tecnologia IEEE 802.11p. Através de (a) pode-se observar que, quando esta tecnologia se encontra a trabalhar em modo contínuo, o *jitter* é sempre bastante pequeno, inferior a 1 ms, não se notando qualquer comportamento diferenciador no momento em que ocorre o *handover*. Quando esta tecnologia se encontra em modo alternado, os valores do *jitter* são bastante mais elevados, como se pode observar na Figura em 5.17(b); este comportamento era esperado devido à alternância, já referida anteriormente, entre o SCH e o CCH o que leva a uma irregularidade na chegada dos pacotes e, consequentemente, a um aumento no valor do *jitter*.

Um facto interessante que se nota nesta figura é a variação do valor do *jitter* não ser proporcional à variação do valor do *bitrate*. Observando a figura percebe-se que para o *bitrate*



(a) Modo contínuo

(b) Modo alternado

Figura 5.17: MIPv6 - *Jitter* durante o *handover* de IEEE 802.11p ⇒ IEEE 802.11p

Tabela 5.3: Correspondência entre o *bitrate* e o intervalo entre pacotes

Bitrate	**Intervalo entre pacotes**
125 Kbit/s	94.08 ms
250 Kbit/s	47.04 ms
500 Kbit/s	23.52 ms
1000 Kbit/s	11.76 ms

de 125 Kbit/s, o *jitter* apresenta valores em torno de 15 ms, tal como para 1000 Kbit/s, ou seja, para o menor e para o maior *bitrate*, respetivamente. O facto interessante surge quando se verifica que para o *bitrate* de 250 Kbit/s o *jitter* apresenta um valor bastante mais elevado. Para que se possa perceber a razão deste acontecimento é necessário ter em conta que o programa utilizado para gerar tráfego utiliza sempre pacotes com 1470 Bytes de dados, e para conseguir diferentes *bitrates* varia o número de pacotes enviados. Assim sendo, e tendo em conta dos valores os vários *bitrates* utilizados, calcularam-se os intervalos entre pacotes - a Tabela 5.3 relaciona cada *bitrate* com o respetivo intervalo entre envio de cada pacote.

Tendo em conta o tempo entre pacotes, e recorrendo à Figura 5.18, é possível perceber o fator que leva às discrepâncias verificadas anteriormente. Quando se utiliza o *bitrate* de 125 Kbit/s, irão ser enviados pacotes a cada 94.08 ms. Quando o primeiro pacote chega à RSU, que se encontra a transmitir em modo alternado, se esta se encontrar no canal SCH o pacote é transmitido (como esquematizado na Figura 5.18). Caso a RSU esteja no CCH, o pacote

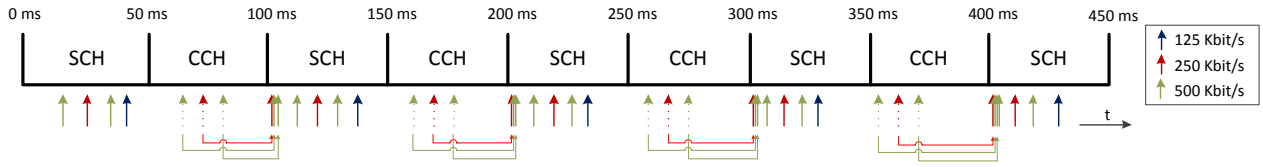


Figura 5.18: Esquema de transmissão em modo alternado

fica em fila de espera até que se efetue a troca de canal, e quando esta ocorrer é enviado. O segundo pacote, como é enviado aproximadamente 94 ms depois, tem uma probabilidade de cerca de 94% de encontrar o mesmo canal ativo que o pacote que o antecedeu encontrou, desta forma explica-se o valor do *jitter* obtido.

Para o *bitrate* de 250 Kbit/s, os pacotes são enviados com um espaçamento de 47.04 ms; deste modo quando um pacote chega à RSU tem apenas uma probabilidade de 6% de encontrar o mesmo canal ativo que o pacote que o precedeu encontrou. Assim, na grande parte dos casos os pacotes serão transmitidos seguindo o esquema ilustrado na figura 5.18, ou seja, quando o SCH se encontra ativo são enviados dois pacotes, o que se encontrava em fila de espera, e o que chegou durante o período de tempo em que o canal esteve ativo. Este esquema de envio irá causar um grande aumento no *jitter*, pois dois pacotes chegam com um intervalo muito pequeno entre si, sendo depois necessário esperar bastante até que voltem a chegar mais dois pacotes.

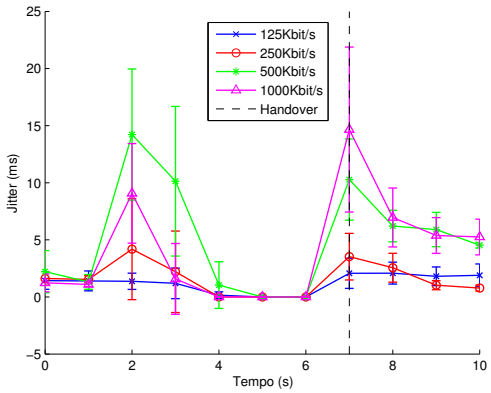
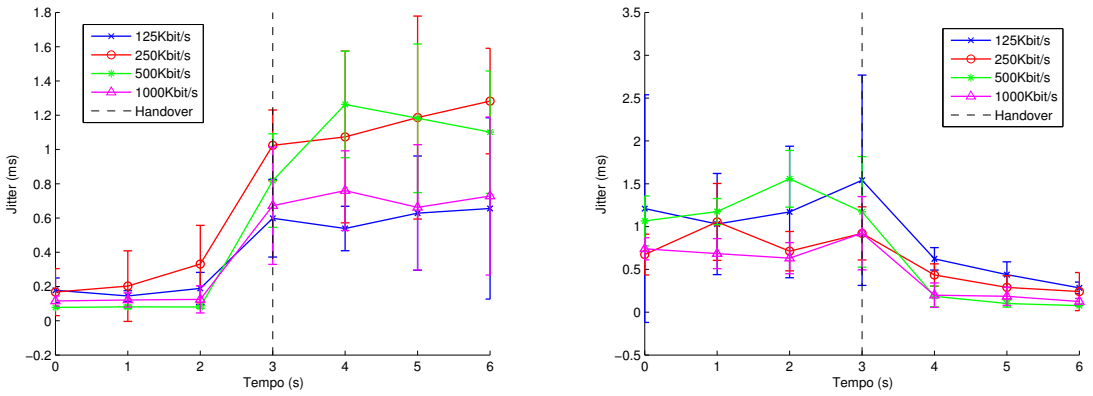


Figura 5.19: MIPv6 - *Jitter* durante o *handover* de IEEE 802.11g ⇒ IEEE 802.11g

Para os *bitrates* mais elevados, o valor do *jitter* tenderá a baixar, como se verifica nos resultados obtidos, pois como o intervalo entre pacotes é cada vez menor, maior será a pro-

babilidade de um pacote encontrar a RSU a transmitir no mesmo canal que o pacote que o precedeu encontrou. O *jitter* terá o seu valor máximo, nas condições testadas, quando utilizado o *bitrate* de 235.2 Kbit/s, pois neste caso o intervalo entre pacotes será de 50 ms, igual ao período de comutação do canal: um pacote quando chega terá uma probabilidade teórica igual a zero de encontrar a estação a transmitir no mesmo canal que o pacote que o precedeu.



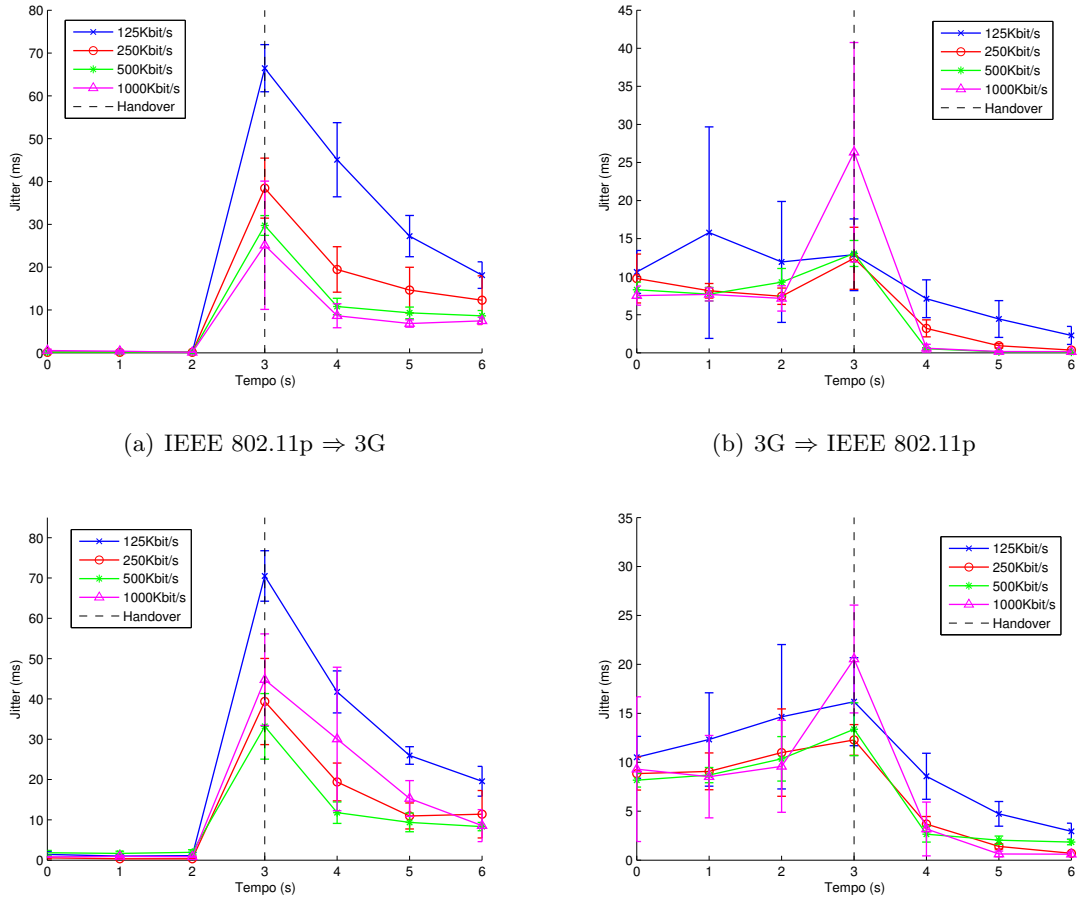
(a) IEEE 802.11p ⇒ IEEE 802.11g (b) IEEE 802.11g ⇒ IEEE 802.11p

Figura 5.20: MIPv6 - *Jitter* durante o *handover* entre IEEE 802.11p e IEEE 802.11g

Na Figura 5.19 está representada a variação o *jitter* durante o *handover* de IEEE 802.11g ⇒ IEEE 802.11g. Nesta pode-se observar que para os *bitrates* mais elevados, o valor do *jitter* apresenta dois picos, um nos momentos que antecedem a perda de ligação com a rede antiga e outro nos instantes seguintes ao *handover*. Este comportamento era esperado, pois nos instantes referidos verifica-se perda de pacotes, logo irá existir uma maior variação entre a chegada dos mesmos o que leva a este aumento no valor do *jitter*. Para o *bitrate* mais baixo, 125 Kbit/s, este comportamento não se verifica, pois como o intervalo entre a chegada de pacotes já é bastante grande quando se recebem todos os pacotes envidados, quando se perdem alguns não irá ter tanta influência como quando se utilizam *bitrates* mais elevados.

A Figura 5.20 mostra o comportamento do *jitter* durante o *handover* entre redes IEEE 802.11, IEEE 802.11p ⇒ IEEE 802.11g em (a) e IEEE 802.11g ⇒ IEEE 802.11p (b). Observando estas figuras nota-se que estas exibem um comportamento muito similar ao verificado para a latência (ver Figura 5.11). Enquanto o MN recebe os dados através da rede IEEE 802.11p, o valor do *jitter* é bastante pequeno, e este apresenta um aumento quando os dados são recebidos através da rede IEEE 802.11g.

Através da Figura 5.21 é possível observar a variação do *jitter* durante os vários cenários



(a) IEEE 802.11p ⇒ 3G

(b) 3G ⇒ IEEE 802.11p

(c) IEEE 802.11g ⇒ 3G

(d) 3G ⇒ IEEE 802.11g

Figura 5.21: MIPv6 - *Jitter* durante o *handover* entre redes IEEE 802.11 e 3G

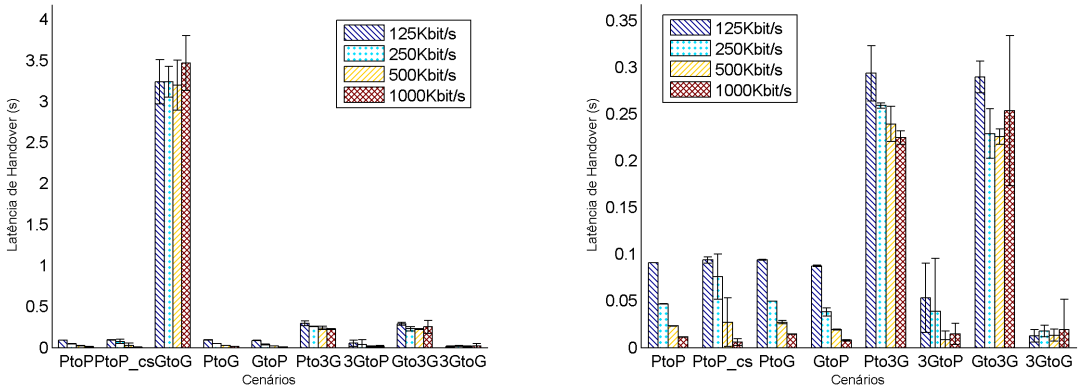
de *handover* que envolvem a tecnologia 3G. Esta figura, tal como sucedia na anterior, é muito similar à Figura 5.12. Quando o *handover* ocorre de uma rede IEEE 802.11 para uma rede 3G, (a) e (c), verifica-se um grande pico no momento do *handover*, seguido de uma estabilização nos instantes seguintes; tal é mais uma vez explicado devido ao facto de não ser possível efetuar reserva de recursos na ligação 3G. Nos cenários de *handover* de 3G para IEEE 802.11 verifica-se também um pico no momento em que ocorre *handover*; tal deve-se ao elevado *jitter* apresentado pela ligação, juntando ainda a diferença entre a chegada dos pacotes imposta pelo próprio *handover*, pois como os pacotes recebidos através da rede IEEE 802.11 têm uma latência muito menor vão provocar uma alteração no intervalo de chegada dos mesmos.

5.4.2 Resultados obtidos com o Protocolo PMIPv6

Nesta secção serão apresentados os resultados relativos aos vários cenários de *handover* testados utilizando o protocolo PMIPv6. Esta secção terá uma estrutura em tudo similar à anterior e, sempre que pertinente, irá ser feita uma comparação entre os resultados apresentados e os resultados referentes ao protocolo MIPv6.

A Tabela 5.2 continua a ser válida nesta subsecção, em todos os gráficos em que o eixo dos *xx* seja referente a cenários.

5.4.2.1 Latência de *Handover*



(a) Todos os cenários

(b) Cenários PtoP, PtoP alt, PtoG, GtoP, Pto3G, 3GtoP, Gto3G e 3GtoG

Figura 5.22: PMIPv6 - Latência de *Handover*

Na Figura 5.22 podem-se observar os valores da latência de *handover* referentes aos vários cenários testados. Em 5.22(a) podem-se observar todos os cenários, enquanto em 5.22(b) foi retirado o cenário IEEE 802.11g ⇒ IEEE 802.11g para que se possa ter uma melhor noção dos valores referentes aos restantes cenários.

Observando esta figura é facilmente percetível que a latência de *handover* no cenário IEEE 802.11g ⇒ IEEE 802.11g é bastante superior às restantes; isto acontece devido à necessidade de se ter de efetuar a desassociação com a rede antiga e a associação com a nova rede. Na Figura 5.23 encontra-se esquematizado o processo de troca de mensagens durante o *handover* referente a este cenário, através do qual é possível perceber todo o processo de *handover*, e consequentemente a razão para este cenário apresentar uma latência de *handover* bastante grande.

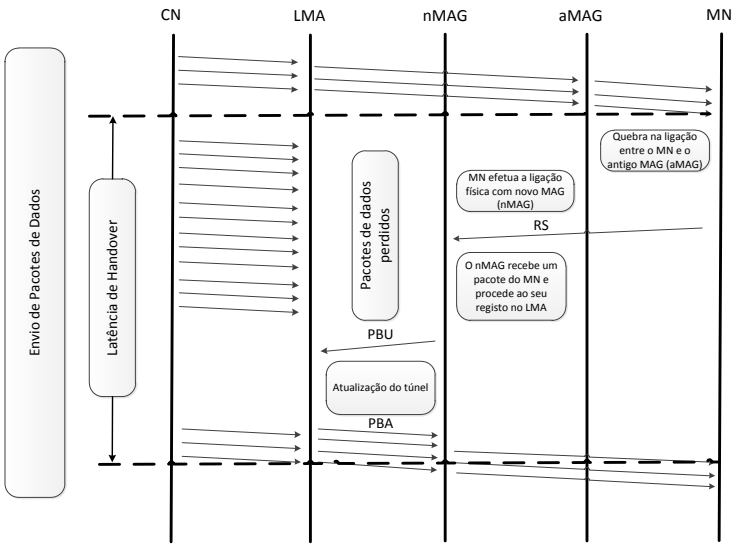


Figura 5.23: PMIPv6 - Troca de mensagens durante o *handover* entre redes IEEE 802.11g

Analisando os cenários de *handover* entre redes IEEE 802.11p (tanto em modo contínuo, como em modo alternado) verifica-se que a latência de *handover* é bastante baixa, apresentado valores similares aos obtidos nos cenários de *handover* entre redes heterogéneas IEEE 802.11. Isto acontece devido à inexistência de associação nesta tecnologia e ao facto do protocolo PMIPv6 conseguir tirar partido deste facto. Como não existe associação, a partir do momento que o MN entre no raio de cobertura da nova rede já pode comunicar com esta, enquanto ainda se encontra a receber pacotes de dados através da rede antiga. Assim que o gestor de mobilidade desenvolvido (ver Secção 4.5) deteta que a nova rede oferece melhor ligação que a rede atual é enviado um pacote de sinalização para esta nova rede, a solicitar que seja efetuado o *handover* para esta; mesmo durante o envio deste, o MN continua a ter ligação e a receber dados através da rede antiga. A nova rede (ou novo MAG, seguindo a terminologia do protocolo PMIPv6), ao receber este pacote de sinalização, vai fazer todas as operações necessárias para encaminhar o tráfego para o MN (estas operações foram explicadas com detalhe em 4.4.2) e seguidamente irá informar o LMA que o MN se encontra no seu alcance, fazendo assim com que o tráfego para este seja encaminhado através do novo MAG. Este processo encontra-se esquematizado na Figura 5.24. Desta forma, apesar de se tratar de um *handover* entre redes homogéneas, e utilizando apenas uma interface, é possível realizar *handover* em tudo semelhante ao que se processa entre rede heterogéneas.

Passando para os cenários de *handover* entre redes IEEE 802.11g e IEEE 802.11p verifica-

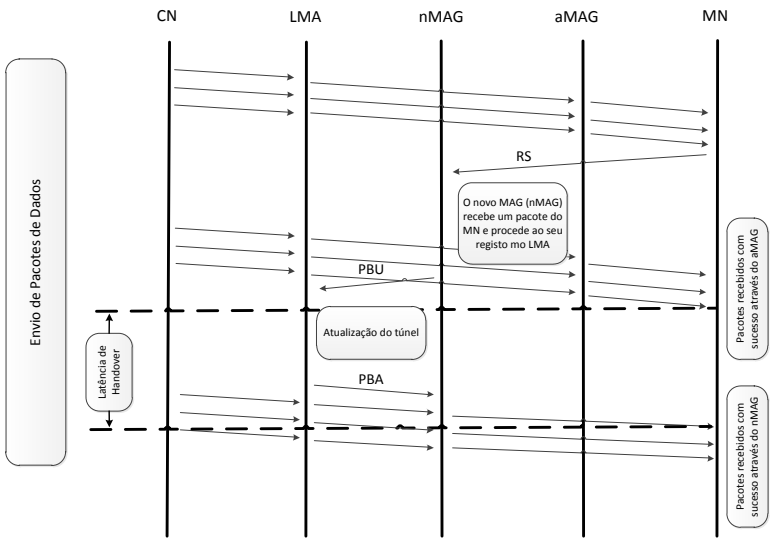


Figura 5.24: PMIPv6 - Troca de mensagens durante o *handover* entre redes IEEE 802.11p

se que a latência de *handover* quando este é efetuado de IEEE 802.11g para IEEE 802.11p é ligeiramente inferior ao cenário inverso. Tal explica-se devido ao atraso da ligação IEEE 802.11p ser ligeiramente inferior, o que faz com que o primeiro pacote recebido através da nova rede leve menos tempo a chegar que o último recebido através da rede antiga.

Finalmente, nos cenários envolvendo a tecnologia 3G, verifica-se o comportamento esperado, ou seja, a latência de *handover* é mais baixa quando este se processa de uma rede 3G para uma rede IEEE 802.11 e é menor quando este se efetua de forma inversa. Este facto ocorre devido às diferenças de latência entre as ligações.

Comparando os cenários 802.11p ⇒ 3G e 802.11g ⇒ 3G, verifica-se uma discrepância quando se introduz na rede tráfego com o *bitrate* de 1000 Kbit/s; no segundo caso verifica-se um aumento da latência de *handover*, quando seria de esperar o inverso. No entanto, observando o intervalo de confiança, vê-se que este é bastante grande o que indica uma grande variação dos vários valores obtidos, consequência da ligação 3G utilizada ser uma rede pública, logo partilhada por diversos utilizadores e estando dependente de vários fatores incontroláveis para quem faz uso desta.

Analisando os cenários 3G ⇒ 802.11p e 3G ⇒ 802.11g, nota-se que a variação do valor do *bitrate* utilizado não produz uma variação correspondente na latência de *handover*. Isto deve-se ao facto de, quando se efetua do *handover* nestes cenários, os primeiros pacotes recebidos pela nova rede, IEEE 802.11g ou IEEE 802.11p, chegarem antes dos últimos que são recebidos

através do 3G, e a latência de *handover* neste caso ser calculada através da diferença entre o primeiro pacote recebido pela interface IEEE 802.11g/IEEE 802.11p e o pacote recebido na ordem correta pela interface 3G. Deste modo, a latência de *handover* não terá grande alteração com a variação do *bitrate*, pois a variação deste apenas irá alterar o número de pacotes recebidos fora de ordem.

5.4.2.2 Pacotes perdidos durante o processo de *Handover*

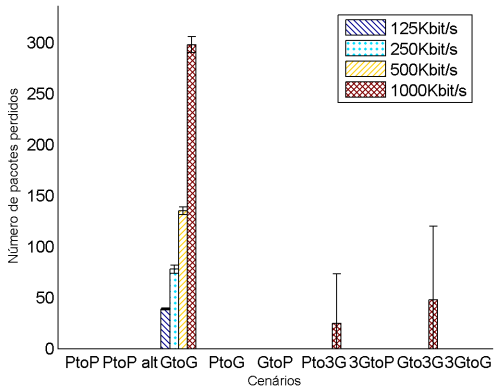


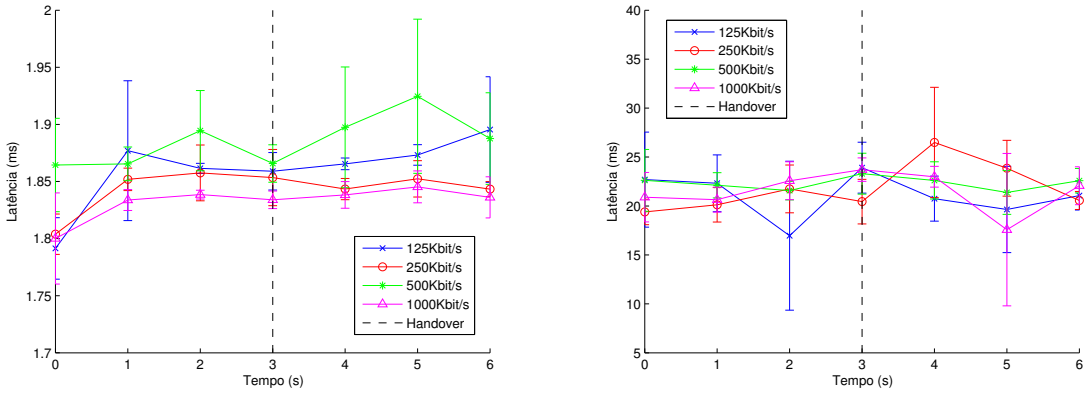
Figura 5.25: PMIPv6 - Número de pacotes perdidos durante o *handover*

A Figura 5.25 ilustra a perda de pacotes nos vários cenários de *handover* estudados. Pode-se observar que apenas existe perda de pacotes quando se efetua o movimento entre duas redes IEEE 802.11g, e tal acontece devido à perda de ligação ocorrida durante o *handover*. Verifica-se, como seria de esperar, um aumento do número de pacotes perdidos proporcional ao aumento do *bitrate* do tráfego introduzido na rede.

Ainda através da Figura 5.25 é possível verificar que existe uma ligeira perda de pacotes nos cenários de *handover* de redes IEEE 802.11 para 3G quando introduzido tráfego na rede com *bitrate* de 1000 Kbit/s, tal como aconteceu no mesmo cenário utilizando o protocolo MIPv6. Pode-se também verificar que os intervalos de confiança nestes casos são bastante elevados, do que se pode concluir que esta perda de pacotes tanto pode ser bastante significativa, como pode não acontecer.

5.4.2.3 Latência

Na Figura 5.26 encontram-se ilustrados os gráficos referentes à latência durante os cenários de *handover* entre redes IEEE 802.11p em modo contínuo e em modo alternado em (a) e (b),



(a) Modo contínuo

(b) Modo alternado

Figura 5.26: PMIPv6 - Latência durante o *handover* de IEEE 802.11p ⇒ IEEE 802.11p

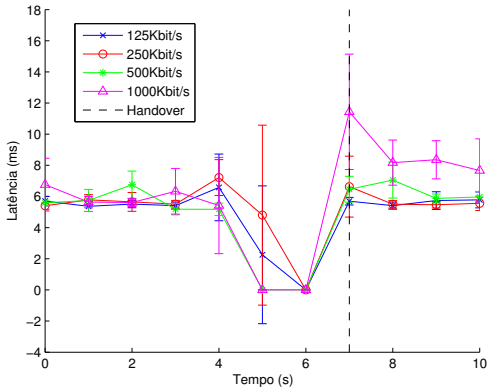
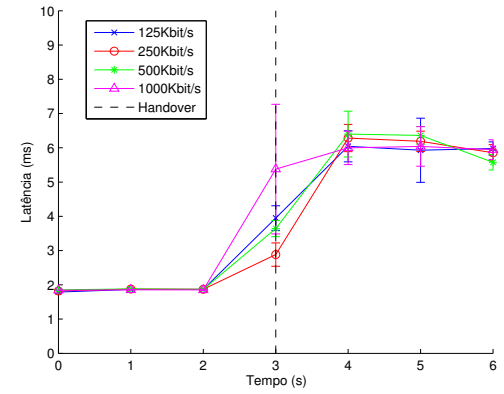


Figura 5.27: PMIPv6 - Latência durante o *handover* de IEEE 802.11g ⇒ IEEE 802.11g

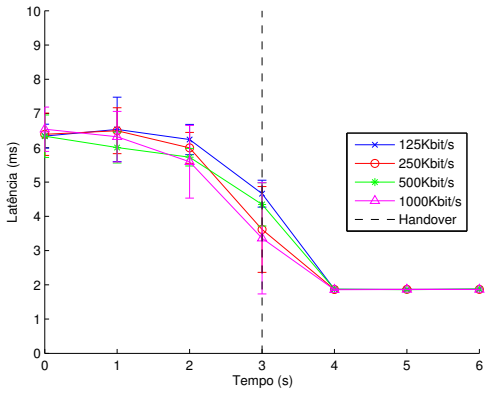
respetivamente. Analisando estas figuras percebe-se que não existem variações significativas na latência durante os vários testes realizados, não existindo nenhum pico durante o instante em que ocorre o *handover*. Isto mostra que mesmo durante o movimento entre redes a latência contínua similar. Comparando as Figuras 5.26(a) e 5.26(b), pode-se verificar um aumento significativo na latência quando é utilizado o IEEE 802.11p em modo alternado, mas mesmo neste cenário durante o momento de *handover* não se verifica um comportamento diferente, quando comparado com os outros instantes.

Analisando a Figura 5.27, referente à latência durante o *handover* entre redes homogéneas IEEE 802.11g, é possível verificar a perda de ligação, através dos valores de latência nulos, que ocorre durante este cenário. É também possível verificar que existem dois picos nas curvas referentes aos vários *bitrates*, tal como verificado na Figura 5.10. A explicação para estes picos

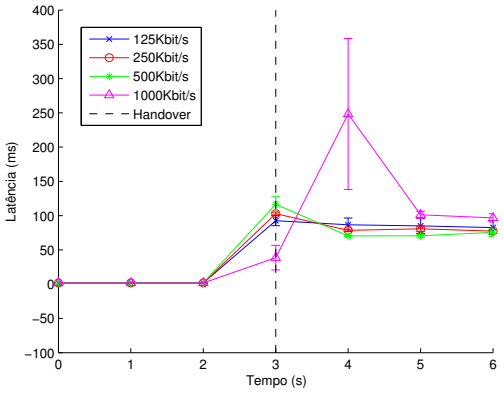
é a mesma apresentada na altura, não estando relacionado com o protocolo de mobilidade em si.



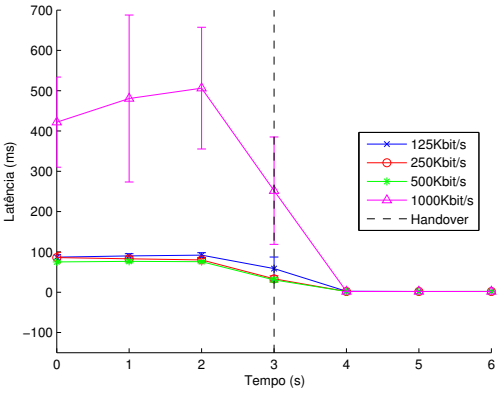
(a) IEEE 802.11p ⇒ IEEE 802.11g



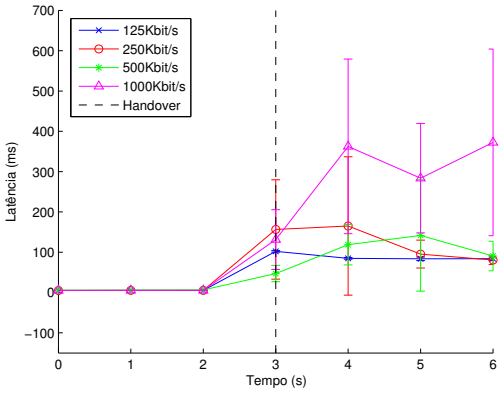
(b) IEEE 802.11g ⇒ IEEE 802.11p



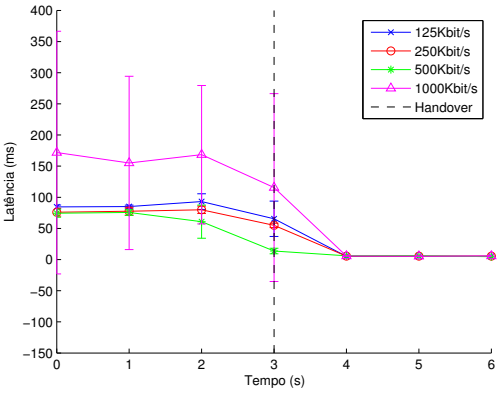
(c) IEEE 802.11p ⇒ 3G



(d) 3G ⇒ IEEE 802.11p



(e) IEEE 802.11g ⇒ 3G

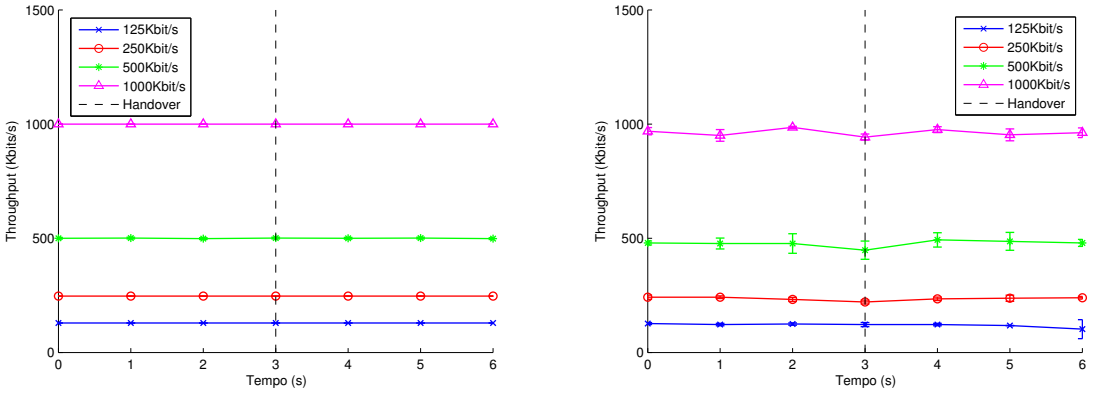


(f) 3G ⇒ IEEE 802.11g

Figura 5.28: PMIPv6 - Latência durante o *handover* entre redes Heterogéneas

Na Figura 5.28 pode-se observar a latência correspondente aos vários cenários de *handover* entre redes heterogéneas. Tal como no cenário anterior, também nestes a latência obtida utilizando o protocolo PMIPv6 é semelhante à verificada utilizando o protocolo MIPv6, como se pode observar comparando estas figuras com as Figuras 5.11 e 5.12. Deste modo, pode-se concluir que, quando o *handover* se efetua entre redes heterogéneas, ambos os protocolos não apresentam grande influência na latência apresentada.

5.4.2.4 *Throughput*



(a) Modo contínuo

(b) Modo alternado

Figura 5.29: PMIPv6 - *Throughput* durante o *handover* de IEEE 802.11p ⇒ IEEE 802.11p

Na Figura 5.29 podem-se observar os gráficos do *throughput* referentes aos cenários de *handover* IEEE 802.11p ⇒ IEEE 802.11p, tanto em modo contínuo (a), como alternado (b). Analisando as curvas representadas nestes gráficos, é possível verificar que não existem variações significativas nos valores do *throughput*, mesmo quando se dá a troca de rede. Este dado, conjugado com os valores referidos anteriormente para este cenário, comprovam que o *handover* entre redes IEEE 802.11p, mesmo se tratando de redes homogéneas e utilizando apenas uma interface, é possível efetuar o movimento sem que o utilizador note qualquer quebra no serviço ou perda de qualidade neste. Comparando as Figuras 5.29(a) e 5.29(b), verifica-se que no segundo caso existe uma maior variação no *throughput*, mas mesmo neste caso não é possível notar um comportamento diferente durante o *handover*, o que demonstra que mesmo utilizando o modo alternado, o processo *handover* não influencia a qualidade do serviço oferecido. Deste modo, é possível concluir que o protocolo PMIPv6 faz uso das caraterísticas de facilidade de ligação, presentes na norma IEEE 802.11p.

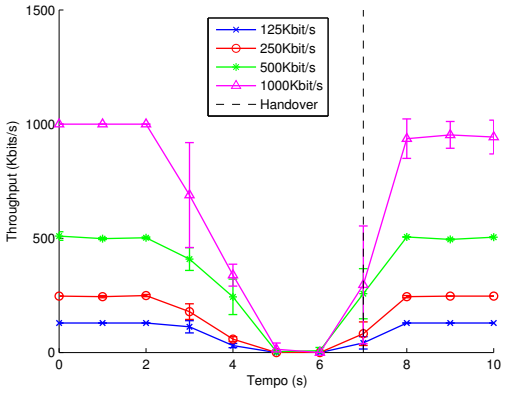
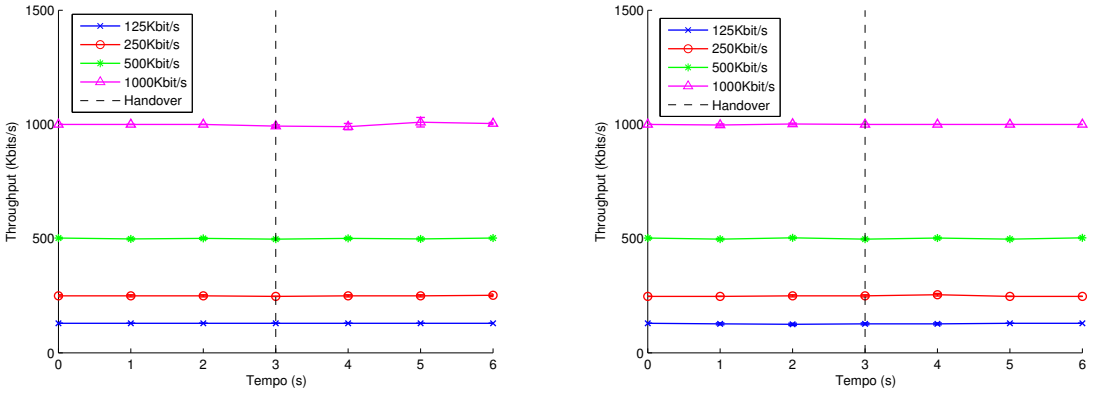


Figura 5.30: PMIPv6 - *Throughput* durante o *handover* de IEEE 802.11g ⇒ IEEE 802.11g

Analisando a Figura 5.30, que ilustra o *throughput* durante o movimento entre redes IEEE 802.11g, é possível observar a descontinuidade no serviço já referida anteriormente. É também possível verificar que o *throughput* vai decaindo de forma praticamente constante, nos instantes anteriores à perda de ligação, devido à perda de qualidade na ligação durante estes instantes. O restabelecimento do valor do *throughput* é quase imediato: no segundo seguinte ao estabelecimento da ligação com a nova rede, verifica-se que este já atingiu o valor normal. Destacando a curva referente ao *bitrate* de 1000 Kbit/s, nota-se que depois do ocorrer o *handover*, os intervalos de confiança são maiores que os apresentados pelos outros *bitrates*. Este facto pode ser explicado com auxílio da Figura 5.27: nesta verificava-se um grande pico na latência, o que levava a concluir que existia um grande congestionamento da ligação, e nos instantes seguintes este congestionamento deixava de existir. Deste modo, como se estão a transmitir pacotes que estavam em fila de espera e os pacotes que estão a ser enviados, vai existir uma maior variação no valor do *throughput*.

As Figuras 5.31(a) e 5.31(b) mostram a evolução do *throughput* durante o *handover* entre IEEE 802.11p ⇒ IEEE 802.11g e IEEE 802.11g ⇒ IEEE 802.11p, respetivamente. Observando as mesmas, pode-se notar que quase não existe variação no *throughput* e os intervalos de confiança são bastante pequenos, sendo mesmo difícil de serem observados. Este comportamento era esperado uma vez que se está na presença de *handover* entre redes equipadas com tecnologias diferentes.

Nas Figuras 5.32(a) e 5.32(c) pode-se observar o *throughput* nos cenários de *handover* de uma rede IEEE 802.11g/IEEE 802.11p para uma rede 3G. Através da análise destas é possível verificar que existe uma ligeira diferença no momento em que ocorre o *handover*, mais visível



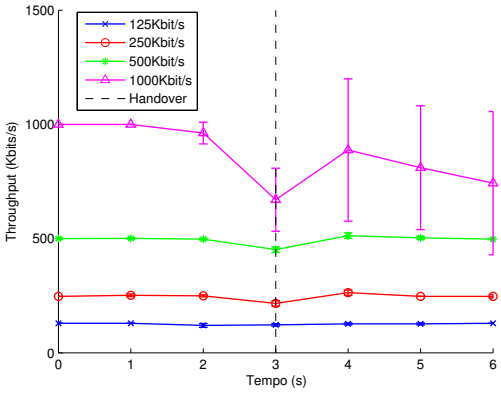
(a) IEEE 802.11p ⇒ IEEE 802.11g

(b) IEEE 802.11g ⇒ IEEE 802.11p

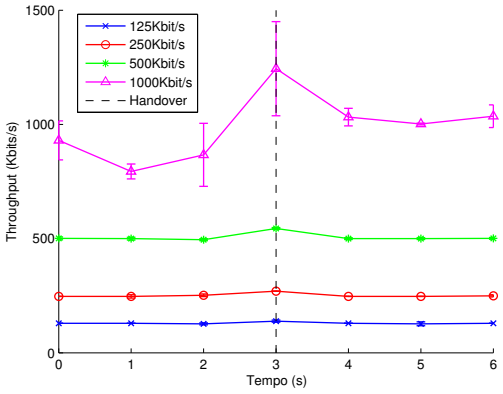
Figura 5.31: PMIPv6 - *Throughput* durante o *handover* entre IEEE 802.11p e IEEE 802.11g

quando utilizado o *bitrate* de 1000 Kbit/s. Esta ligeira quebra pode ser explicada pelo facto de a latência ser maior na ligação 3G do que nas ligações IEEE 802.11g/IEEE 802.11p, e também pelo facto já referido neste documento de não ser possível efetuar a reserva de recursos na rede 3G. No entanto, comparando estas com as Figuras 5.16(a) e 5.16(c), referentes ao mesmo cenário de *handover*, mas utilizando o protocolo MIPv6, nota-se que a quebra, utilizando o protocolo MIPv6, é muito superior. Este facto pode ser explicado porque no PMIPv6, quando o MN pretende alterar a rede a que está associado pelo protocolo, tem de enviar um aviso, através dessa rede, para o MAG que fornece essa ligação, depois disso irá ser feito todo o processo de registo. Como neste caso o MN, para começar a receber dados pela ligação 3G, tem primeiro de a utilizar com comunicações de controlo, esta já vai estar "preparada"para transmitir os dados destinados àquele MN. Quando se utiliza o protocolo MIPv6, quando um MN pretende mudar o CoA registado no seu HA, envia um pacote para o HA. No entanto, este pacote será encaminhado pela rede em que se encontra registado atualmente, que neste caso será uma rede IEEE 802.11g/IEEE 802.11p. Isto faz com que, quando o HA encaminha o tráfego através da rede 3G, esta não esteja "preparada", verificando-se assim a discrepância existente entre os dois casos.

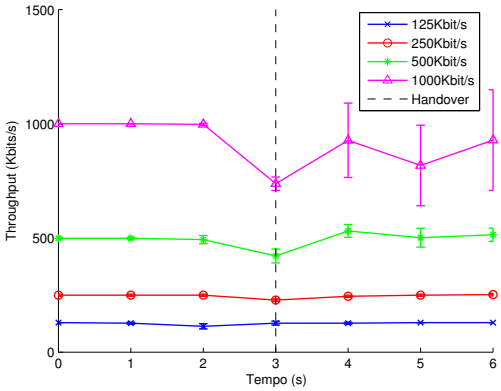
Passando agora para os cenários de *handover* de 3G para IEEE 802.11g/IEEE 802.11p, ilustrados nas Figuras 5.32(b) e 5.32(d), é possível verificar que existe um ligeiro decréscimo no valor do *throughput* no instante anterior ao *handover* e um pequeno aumento no momento em que este ocorre, este comportamento também se verificava nestes cenários (Figuras 5.32(b) e 5.32(d)) quando utilizado o protocolo MIPv6, sendo a explicação para este comportamento



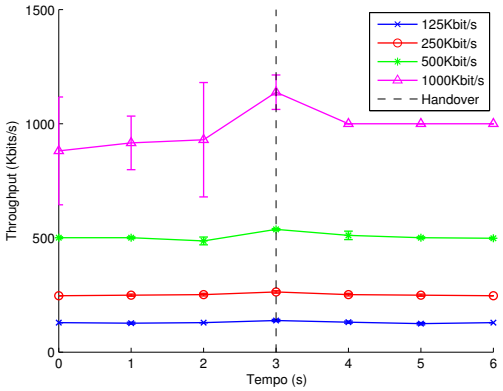
(a) IEEE 802.11p ⇒ 3G



(b) 3G ⇒ IEEE 802.11p



(c) IEEE 802.11g ⇒ 3G



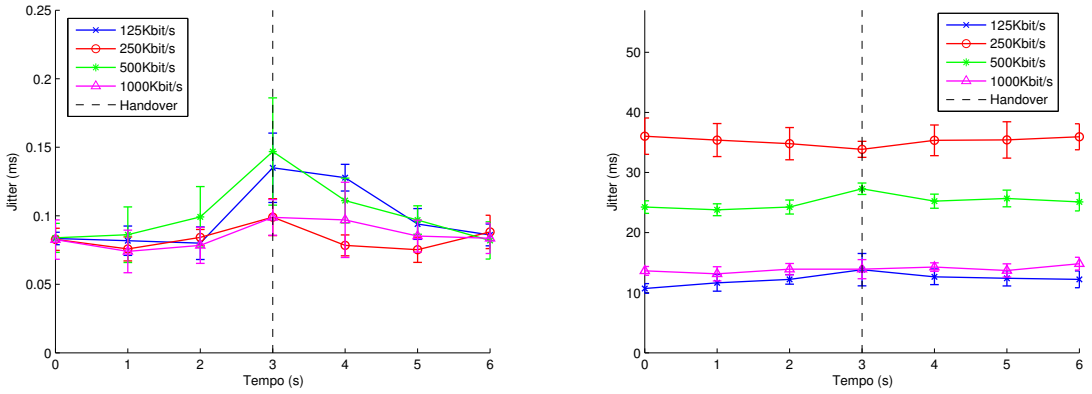
(d) 3G ⇒ IEEE 802.11g

Figura 5.32: PMIPv6 - *Throughput* durante o *handover* entre redes IEEE 802.11 e 3G

a mesma referida anteriormente.

5.4.2.5 *Jitter*

A Figura 5.33 representa o *jitter* durante o *handover* entre redes IEEE 802.11p, em (a) está representado o *jitter* quando é utilizada esta tecnologia em modo contínuo, enquanto em (b) está representado o mesmo cenário, mas com comunicações em modo alternado. Em 5.33(a) é possível verificar que existe um ligeiro aumento no *jitter* no momento em que ocorre o *handover*, no entanto é necessário ter em conta a escala presente do eixo dos *yy*. Numa primeira análise pode parecer que a variação do *jitter* é bastante elevada, mas observando com mais detalhe verifica-se que a maior diferença entre o valor máximo e o valor mínimo, não ultrapassa dos 50 μs. Mesmo quando utilizado o *bitrate* de 1000 Kbit/s, que apresenta um



(a) Modo contínuo

(b) Modo alternado

Figura 5.33: PMIPv6 - *Jitter* durante o *handover* de IEEE 802.11p ⇒ IEEE 802.11p

espaçamento entre pacotes de aproximadamente 11 ms, esta variação do *jitter* não apresentará grande impacto.

Na Figura 5.33(b) pode-se observar o mesmo comportamento verificado neste cenário com o protocolo MIPv6, ou seja, o facto de o *jitter* apresentar um valor bastante mais elevado quando introduzido tráfego na rede com *bitrate* de 250 Kbit/s do que com os restantes. A explicação é a mesma que foi dada anteriormente (ver 5.4.1.5).

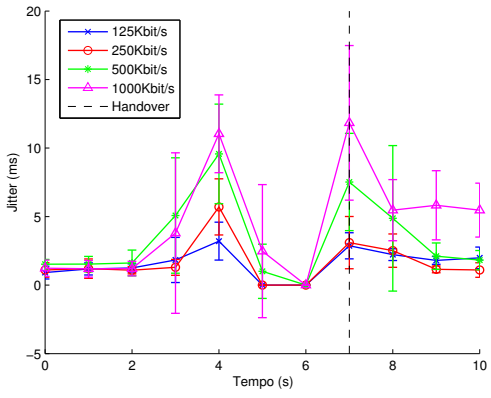
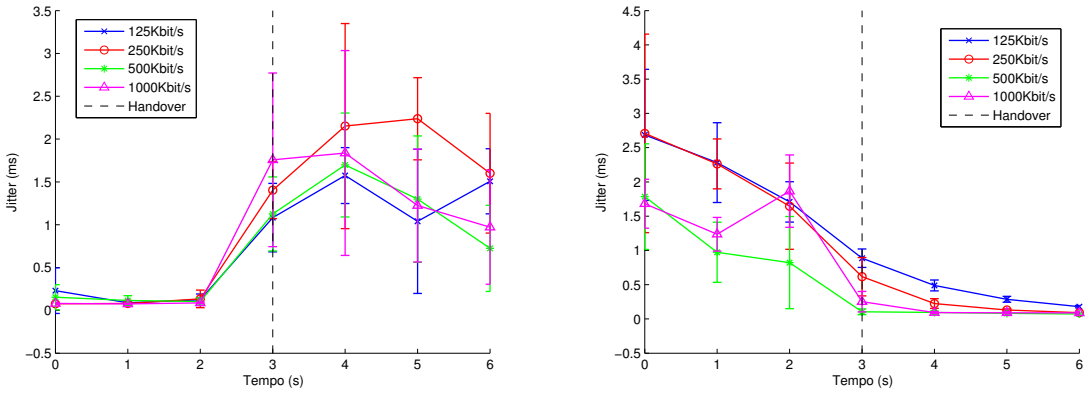


Figura 5.34: PMIPv6 - *Jitter* durante o *handover* de IEEE 802.11g ⇒ IEEE 802.11g

Na Figura 5.34 está representada a evolução do *jitter* ao longo do processo de *handover* entre duas redes que utilizem IEEE 802.11g. Observando esta, pode-se verificar que é similar à Figura 5.27, referente à latência para este mesmo cenário, ou seja, verificam-se dois picos nas várias curvas, um antes de ocorrer a perda de ligação e outro depois de esta ser reestabelecida.

No momento que antecede a perda de ligação verifica-se este pico, pois como a latência é maior e existe já uma quebra no número de pacotes entregues, como se pode verificar na Figura 5.30, juntando estes dois aspetos é normal que o *jitter* aumente. No momento posterior ao restabelecimento da ligação o aumento do *jitter* tem a mesma explicação que o aumento da latência nesta altura.



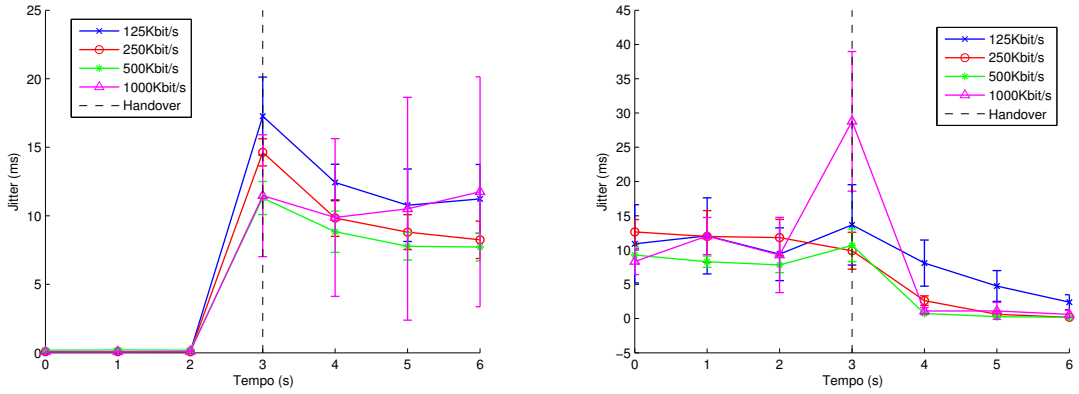
(a) IEEE 802.11p ⇒ IEEE 802.11g

(b) IEEE 802.11g ⇒ IEEE 802.11p

Figura 5.35: PMIPv6 - *Jitter* durante o *handover* entre IEEE 802.11p e IEEE 802.11g

A Figura 5.35 refere-se ao *jitter* durante o *handover* entre redes sem fios heterogéneas, utilizando o protocolo PMIPv6. Comparando esta figura com a Figura 5.20 é possível verificar que o *jitter* apresenta um comportamento semelhante ao verificado no mesmo cenário de *handover* utilizando o protocolo MIPv6. Deste modo, a explicação para o comportamento apresentado é similar à referida anteriormente.

A Figura 5.36 representa a variação do *jitter* nos vários cenários 3G estudados. Observando 5.36(a) e 5.36(c), referentes a cenários de *handover* de uma rede IEEE 802.11g/IEEE 802.11p para 3G, é possível verificar que no momento em que ocorre o *handover* existe um pico, e nos instantes seguintes o valor do *jitter* estabiliza. No entanto, apresenta um valor ainda assim bastante elevado, quando comparado com o valor verificado quando a ligação se fazia através da rede IEEE 802.11. Tal deve-se às caraterísticas, já referidas, que esta ligação apresenta. Nos cenários de *handover* de 3G para IEEE 802.11g/IEEE 802.11p, o pico não é tão pronunciado, sendo principalmente causado pelos pacotes recebidos fora de ordem: quantos mais chegarem fora de ordem, maior será o valor do *jitter*. Isto pode ser comprovado pelo maior pico verificado na curva referente ao tráfego inserido na rede com *bitrate* de 1000 Kbit/s.



(a) IEEE 802.11p ⇒ 3G

(b) 3G ⇒ IEEE 802.11p

(c) IEEE 802.11g ⇒ 3G

(d) 3G ⇒ IEEE 802.11g

Figura 5.36: PMIPv6 - *Jitter* durante o *handover* entre redes IEEE 802.11 e 3G

5.4.3 Comparação dos resultados obtidos com o MIPv6 e com o PMIPv6

Nesta secção será apresentada uma comparação dos resultados mais relevantes (latência de *handover* e número de pacotes perdidos) obtidos através dos dois protocolos em estudo, para que seja possível efetuar uma comparação entre o desempenho destes. Depois de verificadas as discrepâncias existentes nos resultados, irá ser discutido qual o protocolo que melhor se pode adaptar a um ambiente de redes veiculares. Os resultados apresentados durante esta secção correspondem aos resultados obtidos quando introduzido tráfego na rede com *bitrate* de 500 Kbit/s.

A Tabela 5.4 apresenta os resultados obtidos utilizando os dois protocolos, em (a) encontram-se os resultados referentes à latência de *handover* enquanto em (b) podem-se observar os diferentes valores de pacotes perdidos. Escolheram-se estas duas métricas para efetuar a com-

Tabela 5.4: Comparação dos resultados obtidos com o MIPv6 e com o PMIPv6

(a) Latência de *handover* (em segundos)

Cenário	**MIPv6**	**PMIPv6**
PtoP	1.6776±0.3197	0.0232±0.0005
PtoP alt	1.7499±0.1978	0.0273±0.0259
GtoG	4.2894±0.4641	3.199±0.3062
PtoG	0.0263±0.0001	0.0273±0.0016
GtoP	0.0223±0.0097	0.0193±0.0004
Pto3G	0.8249±0.0627	0.2396±0.0187
3GtoP	0.0162±0.0134	0.0083±0.0094
Gto3G	0.7557±0.2046	0.2259±0.0084
3GtoG	0.0170±0.0076	0.0134±0.0062

(b) Pacotes perdidos

Cenário	**MIPv6**	**PMIPv6**
PtoP	69.2±9.2432	0
PtoP alt	72.2±6.2104	0
GtoG	196.0±23.5771	135.2±3.8408
PtoG	0	0
GtoP	0	0
Pto3G	0	0
3GtoP	0	0
Gto3G	0	0
3GtoG	0	0

paração, pois estas efetuam uma caraterização objetiva do momento de *handover*, enquanto as restantes métricas obtidas direcionam-se à QoS durante o processo de *handover*.

Comparando a latência de *handover* obtida através dos dois protocolos, verifica-se que o PMIPv6 apresenta em quase todos os cenários testados valores inferiores aos obtidos pelo MIPv6. Esta diferença torna-se mais significativa nos cenários de *handover* IEEE 802.11p ⇒ IEEE 802.11p, tanto em modo contínuo, como em modo alternado, verificando-se neste caso diferenças da ordem dos segundos. Através da Tabela 5.4(b) pode-se verificar que esta diferença na latência de *handover* apresenta um grande impacto no número de pacotes perdidos, uma vez que enquanto com o PMIPv6 não se verificam perda de pacotes. Esta diferença de comportamento entre os dois protocolos terá grande influência num cenário veicular, pois devido à elevada mobilidade, tempos de perda de ligação da ordem de 1.7 segundos (valor apresentado pelo MIPv6) tornam-se incomportáveis para aplicações que necessitem de acesso permanente à rede, como por exemplo aplicações VoIP. Considerando que em muitos casos os veículos permanecem menos de um minuto no alcance da mesma RSU, caso o protocolo de mobilidade utilizado seja o MIPv6 iriam existir perdas de ligação frequentes, tornando alguns serviços, impossíveis de ser utilizados em redes veiculares, o que iria criar um desinteresse dos utilizadores nestas redes. No caso do PMIPv6, como não existe perda de pacotes durante o *handover*, para os utilizadores o processo de *handover* é completamente transparente.

Analisando a latência de *handover* referente ao cenário IEEE 802.11g ⇒ IEEE 802.11g, é possível observar que esta apresenta valores bastante elevados com os dois protocolos. Estes

valores confirmam a necessidade de se utilizar uma norma de comunicação específica para redes veiculares, pois estes tempos de perda de ligação são completamente incomportáveis em VANETs. Esta tecnologia poderá ser utilizada como um complemento à IEEE 802.11p, especialmente em zonas urbanas onde já existem diversos *hotspots* com esta tecnologia. No entanto, verifica-se que é muito vantajoso integrar o IEEE 802.11p nos *hotspots* atuais.

Face aos factos apresentados, pode-se concluir que o protocolo PMIPv6 se adapta melhor a VANETs. Deste modo, foi o protocolo escolhido para serem realizados testes num cenário veicular real. Assim, será possível verificar se o PMIPv6 apresenta o mesmo comportamento num cenário onde existe elevada mobilidade e uma série de fatores caraterísticos destes cenários.

5.4.4 Resultados obtidos com o Protocolo PMIPv6 em cenário veicular

Nesta secção serão apresentados e discutidos os resultados obtidos em cenário veicular, através da *testbed* apresentada em 5.2.4, utilizando o protocolo PMIPv6. Estes representam os cenários de *handover* entre redes IEEE 802.11p, utilizando os modos de funcionamento contínuo e alternado. Os valores apresentados nesta secção foram obtidos utilizando um *bitrate* de 500 Kbit/s e duas velocidades diferentes: 50 Km/h e 70 Km/h.

5.4.4.1 Latência de *Handover*

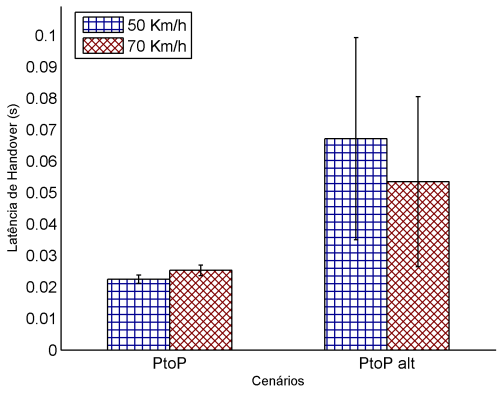


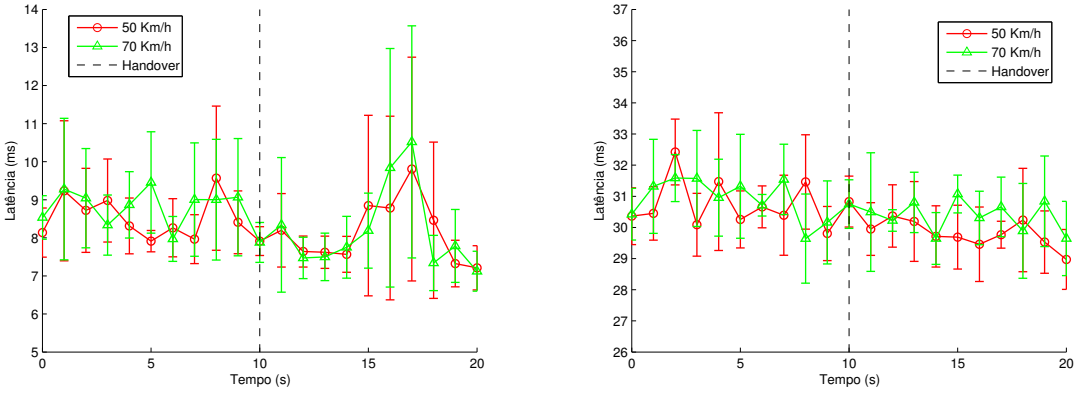
Figura 5.37: PMIPv6 - Latência de *Handover* em cenário veicular

Através da análise da Figura 5.37, representativa da latência de *handover*, pode-se verificar que tanto em modo contínuo como em modo alternado não existem diferenças visíveis em relação aos valores obtidos em ambiente laboratorial. Este facto é corroborado pela ine-

xistência de perda de pacotes, tal como verificado anteriormente. Outro especto que se pode verificar através da figura é que a variação da velocidade não apresenta grande influência sobre a latência de *handover*. Aliás, como se pode observar, o valor obtido em modo alternado para a velocidade maior é menor que o valor obtido para a velocidade inferior. Este facto, apesar de parecer estranho numa primeira análise, explica-se devido ao canal estar a funcionar em modo alternado e devido a se estar a utilizar o *bitrate* de 500 Kbit/s. Como referido anteriormente este *bitrate* causa um *jitter* elevado, logo irá também causar uma grande variação na latência de *handover*, como se pode ver pelos intervalos de confiança.

5.4.4.2 Métricas de QoS

Tal como nos gráficos representados anteriormente para as métricas de latência, *throughput* e *jitter*, também nos gráficos apresentados nesta secção, referentes a essas mesmas métricas, o instante central dos gráficos corresponde ao momento em que ocorreu o *handover*. No entanto, para que se possa ter uma ideia mais concreta da evolução das referidas métricas ao longo dos testes efetuados, foram representados intervalos de tempo maiores.



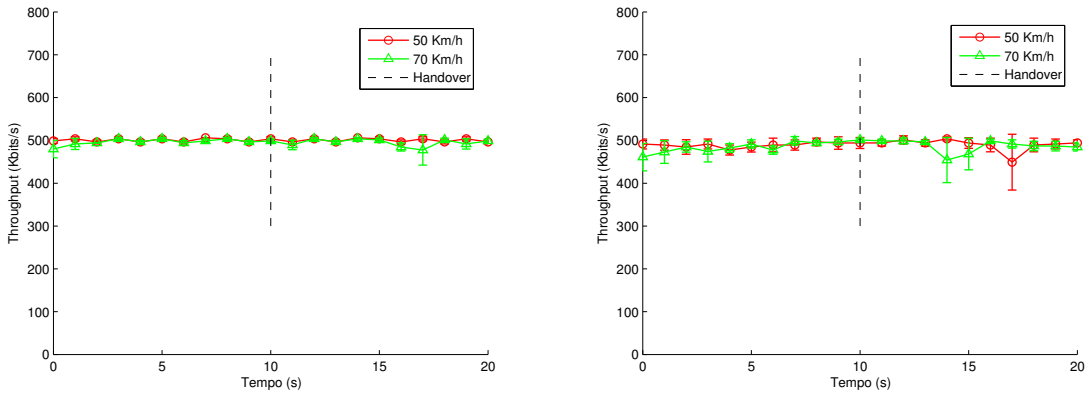
(a) Modo contínuo

(b) Modo alternado

Figura 5.38: PMIPv6 - Latência durante o *handover* de IEEE 802.11p ⇒ IEEE 802.11p

As Figuras 5.38(a) e 5.38(b) representam a latência no cenário de *handover* estudado, em modo contínuo e em modo alternado, respetivamente. Comparando as Figuras 5.38(a) e 5.38(b) com as Figuras 5.26(a) e 5.26(b), referente ao mesmo teste em laboratório, pode-se verificar que apresentam uma tendência semelhante, ou seja, não se verifica nenhuma variação no instante em que ocorre o *handover*. A diferença verificada no valor absoluto da latência está relacionado com a substituição da ligação *Ethernet* no *core* da rede por uma ligação

Wi-Fi.

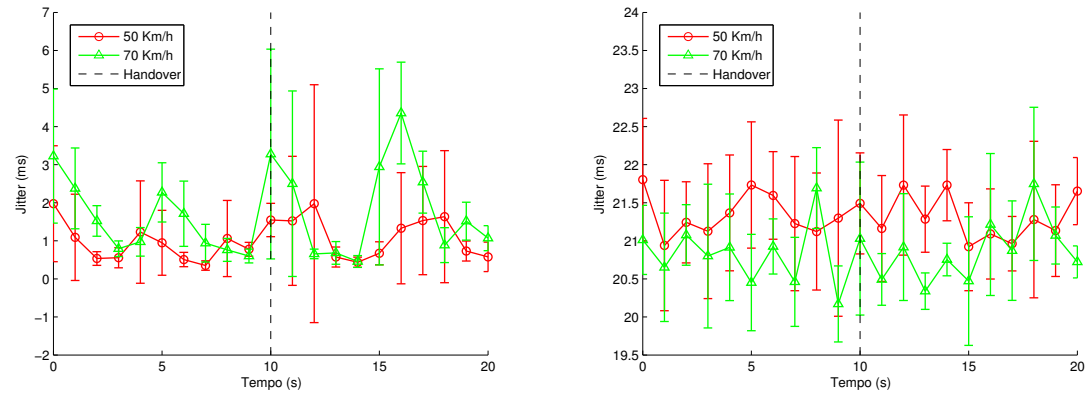


(a) Modo contínuo (b) Modo alternado

Figura 5.39: PMIPv6 - *Throughput* durante o *handover* de IEEE 802.11p ⇒ IEEE 802.11p

Também observando a Figura 5.39, referente ao *throughput*, se pode verificar o mesmo comportamento verificado anteriormente, ou seja, não se verifica qualquer discrepância entre o momento de *handover* e os restantes instantes. É também possível verificar que a variação da velocidade não apresenta influência no *throughput* obtido.

Ainda na Figura 5.39 pode-se observar uma ligeira quebra na parte final das experiências. Esta quebra pode estar relacionada com o facto de as antenas estarem colocadas sobre a bagageira do carro. Assim, quando este passa em frente à RSU a carroceria irá, por instantes, interferir na qualidade das comunicações.



(a) Modo contínuo (b) Modo alternado

Figura 5.40: PMIPv6 - *Jitter* durante o *handover* de IEEE 802.11p ⇒ IEEE 802.11p

Na Figura 5.40 encontram-se representadas as curvas referentes ao *jitter*. Nestas pode-se, mais uma vez, observar que não existe uma diferença significativa entre o instante de *handover* e os restantes, quer se esteja a utilizar comunicações em canal contínuo ou em canal alternado.

Tendo em conta os resultados apresentados esta secção, pode-se observar que estes não apresentam diferenças de comportamento em relação aos resultados obtidos sem mobilidade. Desta forma é possível perceber que os mecanismos desenvolvidos são capazes de atingir os objetivos propostos, ou seja, são capazes de detetar as redes existentes, determinar em tempo útil qual deve ser utilizada, e também efetuar a troca entre redes sem que existam perdas de dados.

5.5 Conclusões

O principal objetivo deste capítulo centrou-se na avaliação dos mecanismos de mobilidade desenvolvidos, bem como das alterações introduzidas nestes. Para atingir este objetivo, este foi dividido em três áreas essenciais em que são apresentadas: as *testbeds* utilizadas, as métricas e metodologia para as obter e por fim os resultados.

Numa primeira fase foram expostas as *testbeds* utilizadas para testar os dois protocolos de mobilidade em estudo. Como os dois protocolos utilizados têm caraterísticas diferentes, foi necessário desenvolver uma *testbed* para cada um, sendo que a principal diferença entre elas consiste na topologia e configuração da rede. Para além destas *testbeds*, de forma a ser possível testar o PMIPv6 em cenário veicular, foi necessário adaptar a *testbed* utilizada para que esta fosse possível ser efetuada em veículos. A principal diferença centra-se na alteração da tecnologia utilizada no *core* da rede, esta foi alterada de *Ethernet* para IEEE 802.11g. Neste secção foi também descrito o material apresentado para por em prática as *testbeds* utilizadas, bem como as configurações necessárias ao sistema utilizado para que este possa suportar um ambiente de mobilidade.

De seguida, na Secção 5.3, foram definidas as métricas que se pretendem obter de forma a ser possível efetuar uma boa caraterização do processo de *handover*. Estas métricas podem dividir-se, quanto ao seu objetivo, em dois grupos. A latência de *handover* e o número de pacotes perdidos fazem uma caraterização objetiva do processo de *handover*, enquanto a latência, *throughput* e *jitter* efetuam uma caraterização da QoS durante o *handover*. Desta forma é possível não só perceber qual o protocolo, mas também quais as tecnologias que apresentam melhor desempenho durante o processo de *handover*. É também possível perceber qual o impacto do *handover* na experiência de um utilizador quando utiliza este tipo de serviço.

Depois de definidas as *testbeds* necessárias e as métricas que se pretendem obter, na fase seguinte (Secção 5.4) foram apresentados os resultados obtidos utilizando os dois protocolos em cenário laboratorial e com o protocolo PMIPv6 em cenário veicular.

Os resultados obtidos através do protocolo MIPv6 mostram que este apresenta um bom desempenho em *handover* entre redes heterogéneas; no entanto, quando o *handover* se efetua entre redes homogéneas tal não se verifica. Este facto deve-se especialmente à incapacidade do protocolo conseguir realizar *handover make-before-break*, isto é, o protocolo não é capaz de fazer as devidas operações na nova rede antes de se desligar da rede atual, o que causa um aumento na latência de *handover* e consequente perda de dados.

O protocolo PMIPv6 apresenta um desempenho idêntico ao MIPv6 em cenários de *handover* entre redes heterogéneas. No entanto, quando o *handover* se processa entre redes homogéneas este apresenta um desempenho superior, especialmente quando se utiliza a tecnologia de acesso IEEE 802.11p. Tal acontece pois com este protocolo, e com esta tecnologia, é possível preparar a ligação com a nova rede enquanto ainda se está a receber dados através da rede atual. Desta forma consegue-se *seamless handover* em redes homogéneas utilizando apenas uma interface para o acesso à rede.

Através dos resultados apresentados neste capítulo é também possível verificar a necessidade de se utilizar comunicações com a norma IEEE 802.11p, pois esta, para além de possibilitar *seamless handover*, apresenta também um desempenho superior em todas as métricas de QoS apresentadas, especialmente quando comparado com o 3G.

Capítulo 6

Conclusão e Trabalho Futuro

6.1 Conclusões

O trabalho efetuado ao longo desta Dissertação consistiu no estudo de comunicações veiculares, focando-se essencialmente nas comunicações V2I e no desenvolvimento de mecanismos capazes de suportar a mobilidade, ao nível das camadas de ligação de dados e de rede, dos veículos ao longo do seu movimento entre as várias RSUs existentes. Neste trabalho também foi realizada uma abordagem a comunicações V2V através do estudo de protocolos de encaminhamento. Neste capítulo são apresentadas as principais conclusões obtidas nesta Dissertação.

A primeira abordagem a comunicações veiculares foi realizada através do estudo de protocolos de encaminhamento. Através deste estudo pretendia-se perceber quais os protocolos de encaminhamento que se poderiam utilizar em VANETs e quais as configurações que levariam a um melhor desempenho por parte destes. Foi possível concluir que o protocolo OLSR não é adequado a VANETs, uma vez que apresenta tempos de deteção de um novo nó na rede e de deteção de quebra de uma rota muito elevados, na ordem das dezenas de segundo, o que em VANETs é incomportável. Os restantes protocolos de encaminhamento estudados, B.A.T.M.A.N. e BABEL, apresentam desempenhos bastante superiores quando comparados com o OLSR, verificando-se que estes podem ser utilizados em redes veiculares. Comparando estes últimos, conclui-se que o BABEL apresenta um desempenho global ligeiramente superior ao B.A.T.M.A.N., especialmente na deteção da quebra de uma rota.

Numa segunda fase, foi estudada a capacidade destes protocolos poderem suportar a mobilidade dos veículos entre as várias RSUs existentes. Desta análise foi possível concluir que os protocolos B.A.T.M.A.N. e BABEL conseguem atingir o objetivo proposto. No entanto,

apenas o conseguem fazer em cenários em que a mobilidade seja bastante velocidade dos nós da rede seja bastante pequena. Este protocolos também não apresentam suporte para uma série de mecanismos necessários para se obter mobilidade ao nível de diferentes redes, como por exemplo: a manutenção do endereço de IP. Em relação ao protocolo OLSR, tal como nas experiências anteriores, este mostrou um mau comportamento, confirmando que não se adapta a VANETs.

Para atingir o principal objetivo proposto para esta Dissertação, estudar um mecanismo capaz de efetuar o *handover* quando os veículos se movem entre RSUs, desenvolveram-se mecanismos de mobilidade, com base nos protocolos MIPv6 e o PMIPv6, e num Gestor de Mobilidade. Em relação aos protocolos de mobilidade utilizados procedeu-se a uma análise das suas implementações, de forma a ser possível perceber possíveis limitações das mesmas. Numa segunda fase foram introduzidas alterações para fazer face a essas limitações em ambos os protocolos. Quanto à gestão da conetividade, foi implementado um Gestor de Mobilidade capaz de monitorizar as redes existentes, em cada tecnologia de acesso à rede disponível, e efetuar a ligação com as redes que ofereçam melhor qualidade de ligação. Este Gestor de Mobilidade é também responsável pelo registo da tecnologia pretendida no protocolo de mobilidade, comunicando com estes para esse efeito.

Através dos testes realizados utilizando estes dois protocolos, foi possível verificar que o PMIPv6 apresenta um desempenho superior ao MIPv6 em quase todos os cenários estudados, acentuando-se mais quando o *handover* se efetua entre rede homogéneas que utilizem a tecnologia IEEE 802.11p. Pode-se então concluir, que o protocolo PMIPv6 é mais adequado para VANETs, facto comprovado pelos testes realizados em cenário real de comunicações veiculares. Neste cenário verificou-se que, mesmo com uma velocidade relativamente elevada (efetuaram-se testes com velocidades até 70 km/h), utilizando PMIPv6 consegue-se obter *seamless handover*, utilizando apenas uma interface. Quanto ao protocolo MIPv6, os resultados obtidos mostram que este apresenta um bom desempenho quando o *handover* se efetua entre redes heterogéneas; no entanto, tal não acontece quando o *handover* se processa entre redes homogéneas. Isto faz com que este protocolo não seja tão adequado a VANETs, uma vez que nestas, como foi possível observar através dos resultados obtidos, é necessário que as RSUs estejam equipadas com a tecnologia IEEE 802.11p, pois caso contrário não será possível garantir a entrega de mensagens de segurança em tempo útil.

Por fim, pode-se concluir que o objetivo proposto para esta Dissertação foi atingido, uma vez que se conseguiram desenvolver uma série de mecanismos capazes de suportar mobilidade

entre RSUs sem que se verifiquem quebras na qualidade de serviço prestada aos utilizadores.

6.2 Trabalho Futuro

Tendo em conta o trabalho realizado e as conclusões obtidas ao longo desta Dissertação, percebe-se que ainda existem algumas lacunas que devem ser analisadas e desenvolvidas.

No que respeita ao trabalho desenvolvido em termos de protocolos de encaminhamento, foram estudados protocolos baseados na topologia da rede; no entanto, é dado como adquirido, nos vários estudos existentes nesta área, que os protocolos mais adequados para VANETs são os protocolos baseados na posição geográfica. Deste modo, torna-se necessário o desenvolvimento e consequente análise de implementações práticas destes protocolos. Outro aspeto que ainda necessita de estudo centra-se análise da sua escalabilidade, pois em redes veiculares num cenário de hora de ponta, as redes irão ter centenas ou milhares de nós.

Quanto ao trabalho desenvolvido em termos da gestão da mobilidade entre RSUs, existem ainda muitos pontos que merecem trabalho, entre os quais se destacam:

- Implementação de todas as caraterísticas definidas pelo protocolo PMIPv6, uma vez que a implementação existente deste protocolo apenas tem as funcionalidades básicas. Algumas caraterísticas foram introduzidas durante esta Dissertação, no entanto existem outras que ainda não se encontram implementadas, como o suporte para *Multihoming*.
- Introduzir as alterações necessárias para que a verificação de um novo nó na rede deixe de ser feita utilizando mensagens de RS e passe a ser feita, como definido pelo protocolo, através de mensagens da camada de ligação de dados.
- Melhorar o algoritmo de decisão de qual a rede que oferece melhor qualidade de ligação, passando este a ter em conta parâmetros de contexto;
- Estudar de mecanismos de mobilidade distribuída;
- Efetuar testes com maior número de MAGs e MNs, de forma a ser possível verificar a escalabilidade do protocolo.
- Verificar a distância máxima a que se podem colocar as RSUs e ainda assim obter *seamless handover*.

Bibliografia

[1] C.V.N.I. Forecast. Cisco visual networking index: Global mobile data traffic forecast update 2010–2015. *Cisco Public Information, February*, 2011.

[2] Distributed Routing and Infotainment through VEhicular Inter-Networking (DRIVE-IN) [Online]. Available: http://drive-in.cmuportugal.org/. Julho de 2012.

[3] H. Conceição, L. Damas, M. Ferreira, e J. Barros. The divert project: Development of inter-vehicular reliable telematics. *OSGeo Journal*, 3(1), 2008.

[4] Car 2 Car Communication Consortium [Online]. Available: http://www.car-to-car.org/. Julho 2012.

[5] Hassnaa Moustafa, Sidi Mohammed Senouci, e Moez Jerbi. *Vehicular Networks - Techiques, Strandards and Applications*, capítulo Introduction to Vehicular Networks. Auerbach Publications, 2009.

[6] F. Li e Y. Wang. Routing in vehicular ad hoc networks: A survey. *Vehicular Technology Magazine, IEEE*, 2(2):12–22, 2007.

[7] Maria Kihl. *Vehicular Networks - Techiques, Strandards and Applications*, capítulo Vehicular Network Applications and Services. Auerbach Publications, 2009.

[8] Kevin C. Lee, Uichin Lee, e Mario Gerla. *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*, capítulo Survey of Routing Protocols in Vehicular Ad Hoc Networks. Information Science Reference, 2010.

[9] R. Baldessari, B. Bödekker, M. Deegener, A. Festag, W. Franz, C.C. Kellum, T. Kosch, A. Kovacs, M. Lenardi, C. Menig, et al. Car-2-Car communication consortium-manifesto. *DLR Electronic Library [http://elib.dlr.de/perl/oai2](Germany)*, 2007.

[10] M. Mohsin e R. Prakash. IP address assignment in a mobile ad hoc network. Em *Proc. of MILCOM 2002*, volume 2, páginas 856–861. IEEE, 2002.

[11] I. Chlamtac, M. Conti, e J.J.N. Liu. Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, 1(1):13–64, 2003.

[12] Maria Fazio, Claudio E. Palazzi, Shirshanka Das, e Mario Gerla. Facilitating Real-time Applications in VANETs through Fast Address Auto-configuration. Em *Proc. of the 3rd IEEE CCNC International Workshop on Networking Issues in Multimedia Entertainment*, 2007.

[13] S. Nesargi e R. Prakash. MANETconf: Configuration of hosts in a mobile ad hoc network. Em *Proc. of INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 2, páginas 1059–1068. IEEE, 2002.

[14] Nitin H. Vaidya. Weak duplicate address detection in mobile ad hoc networks. Em *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '02, New York, NY, USA, 2002.

[15] *Commission decision of 5 August 2008 on the harmonised use of radio spectrum in the 5875-5905 MHz frequency band for safety-related applications of Intelligent Transport Systems (ITS)* , Bruxelas, Agosto 2008. Official Journal of the European Union.

[16] Y. Du, L. Zhang, Y. Feng, Z. Ren, e Z. Wang. Performance analysis and enhancement of ieee 802.11 p/1609 protocol family in vehicular environments. Em *Intelligent Transportation Systems (ITSC), 2010 13th International IEEE Conference*, páginas 1085–1090. IEEE, 2010.

[17] IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009). páginas 1 –51, 2010. doi: 10.1109/IEEESTD.2010.5514475.

[18] IEEE 1609 Working Group. 1609 WG - Dedicated Short Range Communication Working Group [Online]. Available: http://standards.ieee.org/develop/wg/1609_WG.html. Julho 2012.

[19] R. Uzcategui e G. Acosta-Marum. WAVE: a tutorial. *Communications Magazine, IEEE*, 47(5):126–133, 2009.

[20] D. Jiang e L. Delgrossi. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. Em *Vehicular Technology Conference, 2008. VTC Spring 2008*, páginas 2036–2040. IEEE, 2008.

[21] L. Cheng, B.E. Henty, R. Cooper, D.D. Stancil, e F. Bai. A measurement study of time-scaled 802.11 a waveforms over the mobile-to-mobile vehicular channel at 5.9 ghz. *Communications Magazine, IEEE*, 46(5):84–91, 2008.

[22] Y. Wang, A. Ahmed, B. Krishnamachari, e K. Psounis. IEEE 802.11 p performance evaluation and protocol enhancement. Em *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference*, páginas 317–322. IEEE, 2008.

[23] K. Fall e K. Varadhan. The network simulator–NS-2 [Online]. Available: http://www.isi.edu/nsnam/ns. Julho 2012.

[24] S. Eichler. Performance evaluation of the IEEE 802.11 p WAVE communication standard. Em *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, páginas 2199–2203. IEEE, 2007.

[25] T. Kosch, C.J. Adler, S. Eichler, C. Schroth, e M. Strassberger. The scalability problem of vehicular ad hoc networks and how to solve it. *Wireless Communications, IEEE*, 13 (5):22–28, 2006.

[26] L. Stibor, Y. Zang, e H.-J. Reumerman. Neighborhood evaluation of vehicular ad-hoc network using IEEE 802.11p. Em *Proceedings of The 8th European Wireless Conference*, Paris, France, Abril 2007.

[27] K. Bilstrup, E. Uhlemann, E.G. Strom, e U. Bilstrup. Evaluation of the IEEE 802.11 p MAC method for vehicle-to-vehicle communication. Em *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*, páginas 1–5. IEEE, 2008.

[28] W. Alasmary e W. Zhuang. Mobility impact in IEEE 802.11 p infrastructureless vehicular networks. *Ad Hoc Networks*, 2010.

[29] F. Neves, A. Cardote, R. Moreira, e S. Sargento. Real-world evaluation of IEEE 802.11 p for vehicular networks. Em *Proceedings of the Eighth ACM international workshop on Vehicular inter-networking*, páginas 89–90. ACM, 2011.

[30] S.Y. Wang, H.L. Chao, K.C. Liu, T.W. He, C.C. Lin, e C.L. Chou. Evaluating and improving the TCP/UDP performances of IEEE 802.11 (p)/1609 networks. Em *Computers and Communications, 2008. ISCC 2008. IEEE Symposium*, páginas 163–168. IEEE, 2008.

[31] S. Grafling, P. Mahonen, e J. Riihijarvi. Performance evaluation of IEEE 1609 WAVE and IEEE 802.11 p for vehicular communications. Em *Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference*, páginas 344–348. IEEE, 2010.

[32] C. Ameixieira, J. Matos, R. Moreira, A. Cardote, A. Oliveira, e S. Sargento. An IEEE 802.11 p/WAVE implementation with synchronous channel switching for seamless dual-channel access. Em *Proceedings of the Vehicular Networking Conference (VNC)*, páginas 214–221. IEEE, 2011.

[33] W. Kremer. Realistic simulation of a broadcast protocol for an inter vehicle communication system (IVCS). Em *Vehicular Technology Conference, 1991. Gateway to the Future Technology in Motion., 41st IEEE*, páginas 624–629. IEEE, 1991.

[34] M. Torrent-Moreno, D. Jiang, e H. Hartenstein. Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks. Em *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, páginas 10–18. ACM, 2004.

[35] S.Y. Ni, Y.C. Tseng, Y.S. Chen, e J.P. Sheu. The broadcast storm problem in a mobile ad hoc network. Em *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, páginas 151–162. ACM, 1999.

[36] H. ALshaer e E. Horlait. An optimized adaptive broadcast scheme for inter-vehicle communication. Em *Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st*, volume 5, páginas 2840–2844. IEEE, 2005.

[37] M. Nekovee e B.B. Bogason. Reliable and effcient information dissemination in intermittently connected vehicular adhoc networks. Em *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, páginas 2486–2490. IEEE, 2007.

[38] T. Kitani, T. Shinkawa, N. Shibata, K. Yasumoto, M. Ito, e T. Higashino. Efficient vanet-based traffic information sharing using buses on regular routes. Em *Vehicular Technology Conference, 2008. VTC Spring 2008*, páginas 3031–3036. IEEE, 2008.

[39] M. Grossglauser e D. Tse. Mobility increases the capacity of ad-hoc wireless networks. Em *Proc. of INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 3, páginas 1360–1369. IEEE, 2001.

[40] L. Wischhof, A. Ebner, e H. Rohling. Self-organizing traffic information system based on car-to-car communication: Prototype implementation. Em *International Workshop on Intelligent Transportation (WIT)*. Citeseer, 2004.

[41] C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke, e M. Mauve. Data aggregation and roadside unit placement for a vanet traffic information system. Em *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, páginas 58–65. ACM, 2008.

[42] P. Li, X. Huang, Y. Fang, e P. Lin. Optimal placement of gateways in vehicular networks. *Vehicular Technology, IEEE Transactions on*, 56(6):3421–3430, 2007.

[43] AB Reis, S. Sargento, e OK Tonguz. On the performance of sparse vehicular networks with road side units. Em *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd*, páginas 1–5. IEEE, 2011.

[44] Juan A. Sanchez Juan A. Martinez Francisco J. Ros, Victor Cabrera e Pedro M. Ruiz. *Vehicular Networks - Techiques, Strandards and Applications*, capítulo Routing in Vehicular Networks. Auerbach Publications, 2009.

[45] Bertrand Ducourthial e Yacine Khaled. *Vehicular Networks - Techiques, Strandards and Applications*, capítulo Routing in Vehicular Networks. Auerbach Publications, 2009.

[46] C.E. Perkins e E.M. Royer. Ad-hoc on-demand distance vector routing. Em *Proc. of Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop*, páginas 90–100. IEEE, 1999.

[47] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, e L. Viennot. Optimized link state routing protocol for ad hoc networks. Em *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century*, páginas 62–68. IEEE, 2001.

[48] A. Neumann, C. Aichele, M. Lindner, e S. Wunderlich. Better approach to mobile ad-hoc networking (batman). *IETF Work In Progress Internet-Draft*, 2008.

[49] S. Annese, C. Casetti, C.F. Chiasserini, N. Di Maio, A. Ghittino, e M. Reineri. Seamless connectivity and routing in vehicular networks with infrastructure. *Selected Areas in Communications, IEEE Journal on*, 29(3):501–514, 2011.

[50] J. Chroboczek. The BABEL routing protocol. 2011.

[51] S. Jaap, M. Bechler, e L. Wolf. Evaluation of routing protocols for vehicular ad hoc networks in typical road traffic scenarios. *The 11th Open European Summer School (EUNICE 2005)*, 2005.

[52] J. Haerri, F. Filali, e C. Bonnet. Performance comparison of AODV and OLSR in VANETs urban environments under realistic mobility patterns. Em *Proceedings of the 5th IFIP Mediterranean Ad-Hoc Networking Workshop*, páginas 14–17. Citeseer, 2006.

[53] I. Khan e A. Qayyum. Performance evaluation of AODV and OLSR in highly fading vehicular ad hoc network environments. Em *Multitopic Conference, 2009. INMIC 2009. IEEE 13th International*, páginas 1–5. IEEE, 2009.

[54] M. Abolhasan, B. Hagelstein, e J.C.P. Wang. Real-world performance of current proactive multi-hop mesh protocols. Em *Communications, 2009. APCC 2009. 15th Asia-Pacific Conference*, páginas 44–47. IEEE, 2009.

[55] D. Murray, M. Dixon, e T. Koziniec. An experimental comparison of routing protocols in multi hop ad hoc networks. Em *Telecommunication Networks and Applications Conference (ATNAC), 2010 Australasian*, páginas 159–164. IEEE, 2010.

[56] K. Zhu, D. Niyato, P. Wang, E. Hossain, e D.I. Kim. Mobility and handoff management in vehicular networks: a survey. *Wireless Communications and Mobile Computing*, 20 (October 2009):1–20, 2009.

[57] C.E. Perkins e D.B. Johnson. Mobility support in IPv6. Em *Proceedings of the 2nd annual international conference on Mobile computing and networking*, páginas 27–37. ACM, 1996.

[58] H. Soliman, L. Bellier, e K.E. Malki. Hierarchical mobile IPv6 mobility management (HMIPv6). *IETF RFC 4140*, Agosto de 2005.

[59] R. Koodli. Fast handovers for mobile IPv6. *IETF RFC 4068*, Julho de 2005.

[60] S. GUNDAVELLI. Proxy mobile ipv6. *IETF RFC 5213*, Agosto de 2008.

[61] D. Farinacci. Locator/ID separation protocol (LISP). *Internet-draft, draft-ietf-lisp-23*, Maio de 2012.

[62] K.W. Lee, W.K. Seo, Y.Z. Cho, J.W. Kim, J.S. Park, e B.S. Moon. Inter-domain handover scheme using an intermediate mobile access gateway for seamless service in vehicular networks. *International Journal of Communication Systems*, 23(9-10):1127–1144, 2010.

[63] Y.S. Chen, C.H. Cheng, C.S. Hsu, e G.M. Chiu. Network mobility protocol for vehicular ad hoc networks. Em *Proceedings of the Wireless Communications and Networking Conference*, páginas 1–6. IEEE, 2009.

[64] Q.B. Mussabbir, W. Yao, Z. Niu, e X. Fu. Optimized FMIPv6 using IEEE 802.21 MIH services in vehicular networks. *Vehicular Technology, IEEE Transactions on*, 56(6):3397–3407, 2007.

[65] D. Wetteroth. *OSI reference model for telecommunications*. McGraw-Hill Professional, 2001.

[66] X.P. Costa, R. Schmitz, H. Hartenstein, e M. Liebsch. A MIPv6, FMIPv6 and HMIPv6 handover latency study: analytical approach. Em *Proceedings of the IST Mobile and Wireless Telecommunications Summit*, páginas 100–105, 2002.

[67] K.S. Kong, W. Lee, Y.H. Han, M.K. Shin, e H.R. You. Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6. *Wireless Communications, IEEE*, 15(2):36–45, 2008.

[68] K.S. Kong, W. Lee, Y.H. Han, e M.K. Shin. Handover latency analysis of a network-based localized mobility management protocol. Em *Communications, 2008. ICC'08. IEEE International Conference*, páginas 5838–5843. IEEE, 2008.

[69] J. Guan, H. Zhou, Z. Yan, Y. Qin, e H. Zhang. Implementation and analysis of proxy MIPv6. *Wireless Communications and Mobile Computing*, 11(4):477–490, 2011.

[70] V. Gupta, M. Williams, A. Chan, X. Liu, D. Cypher, YY An, et al. IEEE802.21 Standard and Metropolitan Area Networks: Media Independent Handover Services. *Draft P*, 21: D00, 2009.

[71] M. Raya e J.P. Hubaux. The security of vehicular ad hoc networks. Em *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, páginas 11–21. ACM, 2005.

[72] X. Lin, X. Sun, P.H. Ho, e X. Shen. GSIS: a secure and privacy-preserving protocol for vehicular communications. *Vehicular Technology, IEEE Transactions*, 56(6):3442–3456, 2007.

[73] J.J. Haas, Y.C. Hu, e K.P. Laberteaux. Real-world VANET security protocol performance. Em *Proceedings of the Global Telecommunications Conference*, páginas 1–7. IEEE, 2009.

[74] S. Biswas, R. Tatchikou, e F. Dion. Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *Communications Magazine, IEEE*, 44(1):74–82, 2006.

[75] PORDATA - acidentes de viação com vítimas, feridos e mortos - continente em portugal [Online]. Available: http://www.pordata.pt/Portugal/Acidentes+de+viacao+com+vitimas++ferido%s+e+mortos+-+Continente-326. Julho 2012.

[76] C. Maihofer, C. Cseh, W. Franz, e R. Eberhardt. Performance evaluation of stored geocast. Em *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, volume 5, páginas 2901–2905. IEEE, 2003.

[77] B.J. Chang, B.J. Huang, e Y.H. Liang. Wireless sensor network-based adaptive vehicle navigation in multihop-relay WiMAX networks. Em *Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference*, páginas 56–63. IEEE, 2008.

[78] A. Benmimoun, J. Chen, e T. Suzuki. Design and practical evaluation of an intersection assistant in real world tests. Em *Intelligent Vehicles Symposium*, páginas 606–611. IEEE, 2007.

[79] M. Ferreira, R. Fernandes, H. Conceição, W. Viriyasitavat, e O.K. Tonguz. Self-organized traffic control. Em *Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking*, páginas 85–90. ACM, 2010.

[80] A. Tonnesen, T. Lopatic, H. Gredler, B. Petrovitsch, A. Kaplan, e SO Tcke. OLSRd: An adhoc wireless mesh routing deamon [Online]. Available: http://www.olsr.org/. Julho 2012.

[81] D.S.J.D. Couto, D. Aguayo, J. Bicket, e R. Morris. A high-throughput path metric for multi-hop wireless routing. *Wireless Networks*, 11(4):419–434, 2005.

[82] Marek Linder e Axel Neumann. B.A.T.M.A.N. deamon (Better Approach To Mobile Ad Hoc Networking deamon) [Online]. Available: http://www.open-mesh.org/wiki/batmand/. Julho 2012.

[83] J. Chroboczek. Babel a loop-free distance-vector routing protocol [Online]. Available: http://www.pps.univ-paris-diderot.fr/~jch/software/babel/. Julho 2012.

[84] G. Combs. Tshark [Online]. Available: http://www.wireshark.org/docs/man-pages/tshark.html. Julho 2012.

[85] Masafumi Aramoto et al. UMIP [Online]. Available: http://umip.org/. Julho 2012.

[86] V. Devarapalli, R. Wakikawa, A. Petrescu, e P. Thubert. Network mobility (nemo) basic support protocol. *RFC 3963*, Janeiro de 2005.

[87] N. Capela, J. Soares, P. Neves, e S. Sargento. An architecture for optimized inter-technology handovers: Experimental study. Em *Communications (ICC), 2011 IEEE International Conference*, páginas 1–6. IEEE, 2011.

[88] EURECOM. OpenAirInterface Proxy Mobile IPv6 [Online]. Available: http://www.openairinterface.org/components/page1103.en.htm. Julho 2012.

[89] FreeRADIUS Project. FreeRADIUS Client 1.1.6 [Online]. Available: http://freeradius.org/. Julho 2012.

[90] Rémi Denis-Courmont. NDisc6: IPv6 diagnostic tools for Linux and BSD [Online]. Available: http://www.remlab.net/ndisc6/. Julho 2012.

[91] P. Savola. Linux IPv6 Router Advertisement Daemon (radvd). *retrieved on January*, 28, 2011.

[92] A. Tirumala, F. Qin, J. Dugan, J. Ferguson, e K. Gibbs. Iperf: The TCP/UDP bandwidth measurement tool, 2005.

[93] K. Correll. PTP daemon (PTPd) [Online]. Available: http://ptpd.sourceforge.net/. Julho 2012.

[94] K. Correll, N. Barendt, e M. Branicky. Design considerations for software only implementations of the IEEE 1588 precision time protocol. Em *Conference on IEEE*, volume 1588, 2005.

[95] MATLAB. *version 7.10.0 (R2010a)*. The MathWorks Inc., Natick, Massachusetts, 2010.