Universidade de Aveiro
2010
Departamento de Electrónica, Telecomunicações e Informática

Nelson Filipe Capela

DEMONSTRADOR DE MOBILIDADE EM REDES DE ACESSO HETEROGÉNEAS

Universidade de Aveiro
2010
Departamento de Electrónica, Telecomunicações e Informática

Nelson Filipe Capela

DEMONSTRADOR DE MOBILIDADE EM REDES DE ACESSO HETEROGÉNEAS

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica da Prof. Dra. Susana Sargento, Professora auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e do Prof. Dr. Francisco Fontes, Professor auxiliar convidado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

Dedico esta dissertação aos meus Pais, Irmã e Namorada pelo seu incansável apoio e compreensão em todos os momentos ao longo desta caminhada.

O júri

Presidente	Prof. Dr. José Alberto Gouveia Fonseca Professor Associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.
Orientadora	Prof. Dr. Susana Sargento Professora Auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.
Vogal	Prof. Dr. Fernando José Silva Velez Professor Auxiliar do Departamento de Engenharia Electromecânica da Faculdade de Engenharia da Universidade da Beira Interior.

Agradecimentos

Gostaria de agradecer à Prof. Dra. Susana Sargento pela oportunidade que me proporcionou bem como à sua constante persistência, disponibilidade e dedicação que sempre apresentou e que permitiram a realização desta dissertação.

Ao meu colaborador Mestre Pedro Neves, pela sua disponibilidade e partilha de conhecimentos, fundamentais para o desenvolvimento desta dissertação.

Ao Mestre João Soares por todo o apoio que me prestou, pela sua imensa dedicação e interesse demonstrado ao longo de todo este trabalho.

Ao Instituto de Telecomunicações de Aveiro bem como à PT Inovação e seus colaboradores por me terem oferecido todas as condições e apoios necessários para o desenvolvimento desta dissertação.

Palavras-chave

Handover, Mobilidade IP, IEEE 802.21, IEEE 802.16, IEEE 802.11, 3GPP, Ethernet, Wi-Fi, WiMAX, LTE, Android, Handover entre redes Heterogéneas, Qualidade de Serviço, Qualidade de Experiencia, MIH.

Resumo

Devido a uma grande aceitação por parte dos consumidores, tem-se vindo a notar, ao longo dos últimos anos, um crescimento exponencial tanto da internet, como das tecnologias sem fios. Por sua vez, este tipo de crescimento implica o aparecimento de novas e diversas tecnologias de forma a suportar as necessidades crescentes de mobilidade de cada utilizador.

Com a mobilidade surge a necessidade de se estar contactável e "ligado ao mundo" em qualquer sítio e a qualquer hora, tornando-se essencial garantir qualidade de serviço durante o movimento entre várias tecnologias e de forma transparente.

Esta dissertação apresenta uma arquitectura desenvolvida para proporcionar a capacidade de movimentação dos utilizadores de forma transparente e optimizada. Para este tipo de movimentação é essencial a utilização de um protocolo de mobilidade que possa interagir com um protocolo de optimização de mobilidade. Não sendo esta interacção actualmente suportada, serão apresentadas e efectuadas modificações à implementação do protocolo de mobilidade MIPv6 para que se possa ter total controlo no processo de handover e para que este possa interagir com a implementação do protocolo IEEE 802.21, responsável pela optimização do processo de mobilidade.

Seguidamente será definido um conjunto de métricas de desempenho de handover entre redes heterogéneas, procedendo paralelamente ao desenvolvimento de um módulo capaz de obter todas as métricas pretendidas, de forma a demonstrar a real necessidade de interacção entre os protocolos apresentados. Para que seja possível obter as métricas mencionadas será desenvolvida uma testbed capaz de suportar vários cenários de handovers entre as redes Wi-Fi (com WiMAX) e 3G, bem como diversos tipos de tráfego.

Após a obtenção das métricas procede-se a uma análise descritiva dos dados obtidos, tanto a nível do desempenho do handover como a nível de QoS e QoE, para que se possa caracterizar todo o processo de handover.

Keywords

Handover, Mobile IP, IEEE 802.21, IEEE 802.16, IEEE 802.11, 3GPP, Ethernet, Wi-Fi, WiMAX, LTE, Android, Handover between Heterogeneous Networks, Quality of Service, Quality os Experience, MIH**.**

Abstract

Due to the wide acceptance by consumers, it has been noted, over the years, an exponential growing of the Internet and wireless technologies. In turn, this trend implies the appearance of new and different technologies in order to support the mobility needs of each user.

With mobility, the need to be contactable and "on the world" anywhere and anytime has gained a significant importance. It is essential to ensure the quality of service when moving into existing technologies in a transparent manner.

This dissertation presents an architecture developed to provide the ability of users mobility in a transparent and optimized form. For this type of movement it is essential to use a mobility protocol that can interact with a mobility optimization protocol. Since this interaction is not currently supported, it will be performed modifications to the implementation of the mobility protocol MIPv6 to have a full control in the process of handover, and to interact with the implementation of IEEE 802.21 protocol, responsible for the optimization of mobility process.

Next, it will be defined a set of performance metrics of handover between heterogeneous networks, which will proceed in parallel with the module development to get all the metrics in order to demonstrate the real need for interaction between the presented protocols. To be able to obtain the desired metrics, it will be developed a testbed capable to support multiple handovers scenarios between Wi-Fi (with WiMAX) and 3G as well as various types of traffic.

After obtaining the metrics, it will be performed a descriptive analysis of the results for handover performance, QoS and QoE, to characterize the whole handover.

Índice

Índice de Figuras

Índice de Tabelas

Acrónimos

1G	Primeira Geração
2G	Segunda Geração
3G	Terceira Geração
3GPP	*Third Generation Partnership Project*
4G	Quarta Geração
AIM	*Android Interface Manager*
AP	*Access Point*
AR	*Access Router*
ARP	*Address Resolution Protocol*
AuC	*Authentication Center*
BA	*Binding Acknowledgement*
BC	*Binding Cache*
BE	*Best Effort*
BS	*Base Station*
BSA	*Basic Service Area*
BSC	*Station Controllers*
BSS	*Basic Service Set*
BTS	*Base Transceiver Station*
BU	*Binding Update*
CIDs	*Connections Identifiers*
CN	*Correspondent Node*
CoA	Care-of Address
CPC	*Continuous Packet Connectivity*
CS	*Convergence Sublayer*
DAD	*Duplicate Address Detection*
DHAAD	*Dynamic Home Agent Address Discovery*
D-ITG	*DISTRIBUTED INTERNET TRAFFIC GENERATOR*
DL-MAP	*Downlink MAP*
DS	*Distribution System*

DSMIP	*Dual Stack Mobile IPv6*
DSSS	*Direct Sequence Spread Spectrum*
EDCA	*Enhanced Distributed Channel Access*
E-DCH	*Enhanced Dedicated Channel*
EIR	*Equipment Identity Registry*
ESS	*Extended Service Set*
FA	*Foreign Agent*
FBA	*Fast Binding Acknowledgment*
FHSS	Frequency *Hopping Spread Spectrum*
FMIPv6	Fast Mobile IP version 6
FN	*Foreign Network*
FNA	*Fast Neighbor Advertisement*
GGSN	*Gateway* GPRS *Support Node*
GMSC	*Gateway* MSC
GPRS	*General Packet Radio Service*
GSM	*Global System for Mobile Communications*
GW	*GateWay*
HA	*Home Agent*
HARQ	*Hybrid Automatic Repeat request*
HCF	*Hybrid coordination function*
HI	*Handover Initiate*
HLR	*Home Location Register*
HN	*Home Network*
HO	*Handover*
HoA	*Home Address*
HSDPA	*High Speed Downlink Packet Access*
HSPA	*High Speed Packet Access*
HSPA+	*High Speed Packet Access Plus*
HSUPA	*High Speed Uplink Packet Access*
IBSS	*Independent Basic Service Set*
IETF	*Internet Engineering Task Force*

IP	*Internet protocol*
ISDN	*Integrated Services Digital Network*
LLC	*Logical Link Control*
LMA	*Local Mobility Anchor*
LOS	*Line of Sight*
LTE	*Long Term Evolution*
MAC CPS	MAC *Common Part Sub-layer*
MAG	*Mobile Access Gateway*
MAHO	*Mobile Assisted Handover*
MCHO	*Mobile Controlled Handover*
ME	*Mobile Equipment*
MICS	*Media Independent Command Service*
MIES	*Media Independent Event Service*
MIH	*Media Independent Handover*
MIHF	*Media Independent Handover Function*
MIHUs	*Media Independent Handover Users*
MIIS	*Media Independent Information Service*
MIMO	*Multiple-input multiple-output*
MIP	*Mobile IP*
MIPv4	*Mobile IP* version 4
MIPv6	*Mobile IP version 6*
MM	*Mobility Manager*
MMS	*Multimedia Messaging Service*
MN	*Mobile Node*
MOS	*Mean Opinion Score*
MSC	*Mobile Switching Center*
NA	Neighbor Advertisement
NAHO	*Network Assisted Handover*
NAR	*New Access Router*
NCHO	*Network Controlled Handover*
NEMO	Network *Mobility*

NLOS	*Non Line of Sight*
NMT	*Nordic Mobile Telephone*
Non-PoS	*Non-Point of Service*
nrtPS	*Non-real-time Polling Services*
NS	Neighbor Solicitation
OFDM	*Orthogonal Frequency Division Multiplexing*
OFDMA	*Orthogonal Frequency Division Multiple Access*
PAR	*Previous Access Router*
PBA	*Proxy Binding Acknowledgement*
PDU	*Protocol Data Unit*
PMIPv6	*Proxy Mobile IP version 6*
PMP	*Point to Multi-Point*
PND	*Proxy Neighbor Discovery*
PoA	*Point of Attachment*
PoS	*Point of Service*
PrRtAdv	*Proxy Router Advertisement*
QoE	Qualidade de Experiencia
QoS	Qualidade de Serviço
RA	*Router Advertisement*
Radvd	*Router Advertisement Daemon*
RS	*Router Solicitation*
rtPS	*Real-time Polling Services*
RtSolPr	*Router Solicitation for Proxy Advertisement*
SAP	Service Access Point
SC-FDMA	*Single Carrier* FDMA
SDUs	*Service Data Units*
SGSN	*Serving* GPRS *Support Node*
SS	*Subscriber Station*
STA	*Station*
TACS	*Total Access Communications System*
UGS	*Unsolicited Grant Services*

UIT	União Internacional de Telecomunicações
UMIP	*USAGI-patched Mobile IPv6 for Linux*
UMTS	*Universal Mobile Telecommunications System*
USIM	*Subscriber Identity Module*
VLR	*Visitor Location Register*
VoIP	Voz sobre IP
WCDMA	*Wideband Code Division Multiple Access*
Wi-Fi	*Wireless Fidelity*
WiMAX	*Worldwide Interoperability for Microwave Access*
WLAN	*Wireless Local Area Network*
WMAN	*Wireless Metropolitan Area Network*

1. Introdução

1.1. Motivação

Com o passar dos anos tem-se vindo a assistir a uma crescente evolução no que diz respeito às telecomunicações, mais propriamente aos sistemas de comunicações móveis de próxima geração e às tecnologias sem fios.

Para que este tipo de mercado se mantenha em constante crescimento, torna-se então essencial satisfazer todas as necessidades impostas por parte dos seus utilizadores.

- Acesso à Internet em qualquer sítio e a qualquer hora
- Acesso em tempo real
- Maior largura de banda/*bitrate*
- Custo reduzido

Este tipo de necessidades, que foram surgindo gradualmente, levou ao aparecimento de diversos tipos de tecnologias, cada uma com as suas características. Dentro destas tecnologias temos o *Wireless Fidelity* (Wi-Fi), o qual teve uma grande aceitação nas comunicações sem fios actuais e apresenta débitos elevados para áreas locais. O *Worldwide Interoperability for Microwave Access* (WiMAX) e a Terceira Geração (3G) vêm alargar as áreas de acesso aos utilizadores, embora o 3G tenha atingido um patamar superior no que diz respeito à sua aceitação. Mais recentemente surge o *Long Term Evolution* (LTE), este representa uma evolução do HSPA e apresenta grandes melhorias a nível de taxas de transmissão. Como evolução a este tem vindo a ser desenvolvido o LTE-*Advanced* com o objectivo de cumprir todos os requisitos da União Internacional de Telecomunicações (UIT) para se designar por Quarta Geração (4G).

Cada vez mais, com o crescimento deste tipo de mercado, é fundamental que os sistemas de comunicações móveis de próxima geração suportem vários tipos de tecnologias e que possam garantir que as diferentes tecnologias de acesso sem fios sejam capazes de interagir de forma eficaz, uma vez que não é possível ter todo o tipo de tecnologias a abranger todo o espaço geográfico.

Surge então o conceito de *handover*, mais propriamente *seamless handover*, que está relacionado com o processo de transição de uma unidade móvel de uma célula para outra independentemente da tecnologia e de forma transparente, ou seja, sem que exista quebra de ligação.

Contudo, o protocolo de endereçamento IP não foi projectado para suportar a movimentação de terminais. Este facto tornou necessário o desenvolvimento de protocolos de mobilidade, ou seja, protocolos que permitem a um terminal movimentar-se entre diversas redes mantendo o mesmo endereço IP, tornando possível a movimentação do terminal móvel para que este se mantenha sempre alcançável.

Estando a mobilidade dos utilizadores suportada pelos protocolos de mobilidade, torna-se necessário optimizar todo este processo através da utilização de protocolos de optimização de mobilidade. Este tipo de protocolos foram projectados de forma a permitirem a mobilidade dos terminais, não tendo em consideração a necessidade de interacção com protocolos de optimização de mobilidade, que começaram a surgir mais recentemente, tal como o IEEE 802.21.

O protocolo IEEE 802.21 - *Media Independent Handover* tem vindo a ser definido pelo IEEE e tem como principal objectivo optimizar os processos de mobilidade independentemente da tecnologia, fornecendo um conjunto de serviços e interfaces comuns entre as várias tecnologias.

Só através da interacção entre estes protocolos será permitido aos utilizadores "viajarem" entre diferentes tecnologias, tendo sempre como garantia a continuidade e qualidade do serviço em questão.

1.2. Objectivos

Esta dissertação teve como objectivo contribuir para o desenvolvimento de um demonstrador de mobilidade entre redes de acesso heterogéneas composta pelas tecnologias Wi-Fi e 3G.

As actividades que foram desenvolvidas são:

- Utilizar uma implementação do protocolo de mobilidade bem como do IEEE 802.21 de forma a auxiliar e optimizar todo o processo de mobilidade.

- Através da implementação do protocolo de mobilidade controlar o processo de *handover*, tendo a capacidade de decidir aquando da sua execução, bem como para que rede efectuar o mesmo, sem que exista perda de conectividade durante este processo.

- Permitir a interacção entre a implementação do protocolo de mobilidade e a implementação do protocolo de optimização de mobilidade IEEE 802.21.

- Definição de métricas de desempenho do *handover* entre redes heterogéneas utilizando como suporte o protocolo IEEE802.21.

- Desenvolvimento de um módulo capaz de obter as métricas definidas para diversos tipos de *handover* e diversos tipos de tráfego. Para a obtenção das métricas pretendidas, este módulo é capaz de forçar todo o processo de *handover*, bem como ter todo o controlo sobre este a nível da rede destino.

- Desenvolver uma *testbed* real capaz de suportar a realização das experiências pretendidas e a demonstração de todo o processo.

- Efectuar um estudo referente ao processo de *handover* de forma a avaliar o desempenho de mobilidade, com e sem o auxilio do protocolo de optimização de mobilidade IEEE

802.21, tendo em conta os vários aspectos e cenários possíveis referentes a este processo.

- Observar alguns aspectos de Qualidade de Serviço e Qualidade de Experiência.

1.3. Organização da Dissertação

A corrente dissertação encontra-se organizada do seguinte modo:

- O capítulo 2 apresenta uma análise referente às tecnologias em estudo, como o Wi-Fi e o WiMAX, bem como às principais tecnologias desenvolvidas pelo 3GPP. Seguidamente são analisados alguns dos principais protocolos de mobilidade, entre os quais o MIPv4, MIPv6, FMIPv6, DSMIPv6 e PMIPv6. Para que se possa entender o modo de optimização de mobilidade é também feita uma análise ao protocolo IEEE 802.21, apresentando as suas principais características, o seu modo de funcionamento e a sua arquitectura.

- O capítulo 3 apresenta a arquitectura implementada para a realização desta dissertação seguida de uma explicação ao seu modo de funcionamento. Seguidamente é feita uma análise à implementação do protocolo de mobilidade apresentando as suas principais características e modos de funcionamento que limitaram a concretização dos objectivos pretendidos. Após esta análise são apresentadas todas as limitações existentes, bem como as modificações necessárias a efectuar. Relativamente ao protocolo 802.21 é feita uma apresentação da sua implementação, dando especial ênfase ao Mobility Manager (MM) e às capacidades por este suportadas. Neste capítulo são ainda indicadas as modificações necessárias para que o MM possa interagir com a implementação do protocolo de mobilidade. Por fim, é efectuado um estudo, seguido da respectiva definição, a nível de métricas relativas ao processo de *handover,* bem como métricas de QoS e QoE que se podem obter durante a realização deste processo com e sem o suporte do protocolo IEEE 802.21.

- O capítulo 4 apresenta todas as implementações e alterações, mencionadas no capítulo 3, para que seja possível a interacção entre a implementação do protocolo de mobilidade MIPv6 e a implementação do protocolo IEEE 802.21, mais concretamente com MM. É também apresentado um conjunto de alterações referentes à implementação do protocolo de mobilidade para que este funcione correctamente após as alterações, bem como as configurações efectuadas para a realização de um cenário de mobilidade. Segue-se a apresentação do módulo desenvolvido para a obtenção das métricas definidas.

- O capítulo 5 apresenta a *testbed* implementada seguida de uma descrição de todos os elementos que a constituem. Neste capítulo são descritos todos os processos e tipos de tráfego utilizados para a obtenção dos resultados pretendidos. São também apresentados

todos os resultados obtidos, efectuando paralelamente uma discussão dos mesmos para os diferentes cenários e processos em consideração.

- O capítulo 6 apresenta a conclusão deste trabalho bem como possíveis modificações e implementações que poderão ser efectuadas em trabalho futuro.

2. Estado de Arte

Neste capítulo é apresentado um conjunto de conceitos teóricos necessários para uma melhor compreensão e realização desta dissertação.

A secção 2.1 apresenta uma descrição relativa às principais tecnologias sem fios, descrevendo as suas características e modo de funcionamento.

Na secção 2.2 são analisados os principais protocolos de mobilidade, tais como o MIPv4, MIPv6, FMIP, PMIP e DSMIP.

Segue-se uma análise mais aprofundada relativamente ao protocolo de optimização de mobilidade IEEE 802.21 na secção 2.3.

A secção 2.4 apresenta um pequeno sumário relativo ao capítulo.

2.1. Tecnologias de Banda Larga sem Fios

2.1.1. Wi-Fi

Wireless Fidelity mais conhecido por Wi-Fi trata-se de uma marca registada pertencente à *Wi-Fi Aliance*. Esta é utilizada por produtos certificados, pertencentes ao grupo de redes locais sem fios, as Wireless LAN (WLAN).

Um dos pontos fortes desta tecnologia que permitiu o seu grande sucesso e aceitação por parte dos utilizadores é o facto de esta operar em faixas de frequência que não necessitam de licença. O Wi-Fi permite um acesso à internet de um modo simples e em zonas onde o acesso a esta seria impensável, tais como aeroportos, centros comerciais, etc., bastando para isso a utilização de um portátil ou de outro dispositivo com suporte a esta tecnologia.

Esta tecnologia é baseada no padrão IEEE 802.11.

2.1.1.1. Principais padrões IEEE 802.11

O IEEE 802.11 é um conjunto de normas referentes às redes locais sem fios, mais conhecidas por *Wireless Local Area Network* (WLAN). A primeira versão do 802.11 foi lançada em 1997 e operava num intervalo de frequências entre os 2.4 GHz e os 2.4835 GHz permitindo taxas de transmissão de 1 ou 2 Mbps. Este permitia ainda a utilização de duas técnicas de transmissão, o *Direct Sequence Spread Spectrum* (DSSS) e o Frequency *Hopping Spread Spectrum* (FHSS). Passado dois anos, em 1999, surge o padrão IEEE 802.11b como uma actualização do IEEE 802.11. Este mantêm-se fiel a algumas das características do IEEE 802.11 e tem como principais diferenças as velocidades de transmissão, que passam a ser de 5.5 ou 11 Mbps, e o modo de transmissão, que

passa a ser unicamente DSSS. No final deste mesmo ano é lançado um novo padrão, o IEEE 802.11a, este passa a operar a uma frequência de 5GHz e permite atingir taxas de transmissão até 54 Mbps. A utilização dos 5GHz, por um lado permitia reduzir a possibilidade de interferências, já que se tratava de um valor pouco usado, mas por outro trazia dificuldades acrescidas para poder comunicar com os dispositivos que operassem nos padrões anteriores. Mais tarde, já em 2003, surge o padrão IEEE 802.11g que é totalmente compatível com o IEEE 802.11b e que possui a mesma taxa de transmissão do IEEE 802.11a, mas operando a uma frequência de 2.4 GHz. Neste mesmo ano foi aprovado sob a sigla IEEE 802.11f, a recomendação de práticas para a implementação de *handovers*. Recentemente, em 2009, foi aprovado o padrão 802.11n, que tem como principais características o uso de um esquema *Multi-Input Multi-Output* (MIMO), que possibilitando a combinação de várias vias de comunicação, permite aumentar consideravelmente as suas taxas de transmissão, passando a atingir taxas de 600 Mbps e usando uma faixa de frequência de 2.4 e/ou 5 GHz. Para além de todos estes padrões mencionados foram definidos muitos mais que acabaram por não ser muito utilizados devido a acartarem diversos tipos de problemas, como a incompatibilidade com padrões anteriores ou mesmo por se adaptarem a situações muito específicas [1].

2.1.1.1.1. Arquitectura

Através do padrão IEEE 802.11 foi definida uma arquitectura para as redes sem fios, que está baseada na divisão da área coberta pela rede em várias células. A arquitectura é composta por um conjunto de componentes que interagem entre si de forma a proporcionarem uma WLAN capaz de suportar a movimentação das estações móveis de um modo transparente para as camadas superiores.

A arquitectura do padrão IEEE 802.11 contém os seguintes elementos:

- *Basic Service Set* (BSS) – é uma rede sem fios que consiste num único ponto de acesso (AP) que suporta uma ou mais STAs, onde os STAs comunicam através do AP. Trata-se do bloco principal de construção de uma LAN IEEE 802.11.

- *Basic Service Area* (BSA) – área de cobertura dentro do qual as STA podem permanecer em comunicação com a BSS.

- *Independent Basic Service Set* (IBSS) – consiste numa rede sem fios com pelo menos duas STAs que podem comunicar directamente e que não tem acesso a um DS. Por vezes um IBSS é também referido como uma rede Ad-Hoc. Trata-se do modo principal de construção de uma LAN IEEE 802.11.

- *Station* (STA) – é uma estação móvel que se pode deslocar entre diferentes BSS, pois a sua adesão às respectivas BSS é feita de modo dinâmico.

- *Distribution System* (DS) – sistema usado para interligar um conjunto de BSS, o que permite aumentar a cobertura da rede. A nível físico existem algumas limitações no que diz respeito às distâncias existentes entre cada BSS. (Figura 2.1.1.1.1-1)
- Access Point (AP) – trata-se de uma estação endereçável que permite a circulação dos dados entre a BSS e o DS.

- *Extended Service Set* (ESS) – é um conjunto de dois ou mais pontos de acesso ligados à mesma rede fisicamente que define um único segmento de rede lógica. Como estas redes são compostas por BSS e DS, as STAs podem comunicar-se e moverem-se de forma transparente para o *Logical Link Control* (LLC) (Figura 2.1.1.1.1-2) [2] [3].

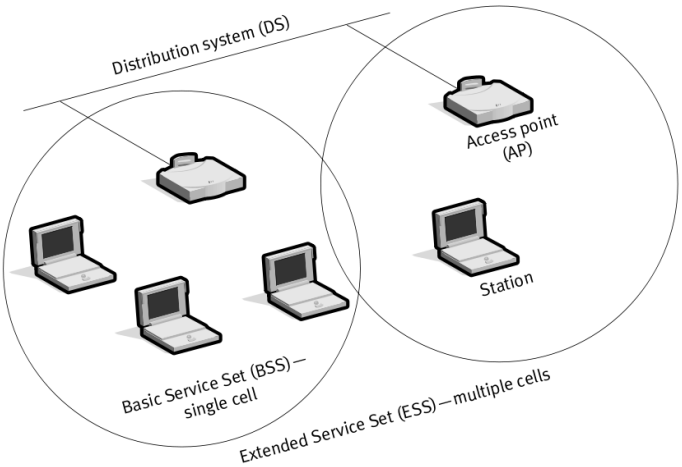

Figura 2.1.1.1.1-1 Representação de um ESS [4]

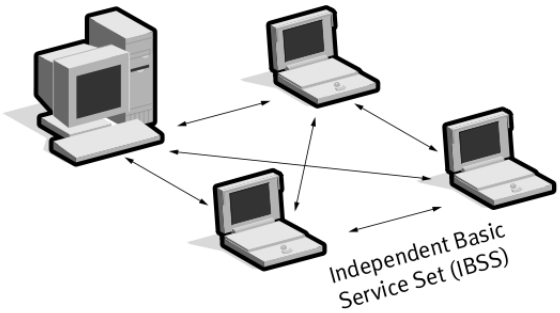

Figura 2.1.1.1.1-2: Representação de um IBSS [4]

Nas redes sem fios não existe uma área de cobertura bem definida, pois as características de propagação são extremamente dinâmicas e imprevisíveis, qualquer pequena mudança de posição pode significar uma grande mudança na qualidade de sinal. Tais características tornam extremamente difícil definir as áreas de cobertura bem como a posição onde se encontram as STAs. Como podemos observar na Figura 2.1.1.1.1-3 o STA 6 tanto pode estar na BSS 2 como na BSS 3 [5].

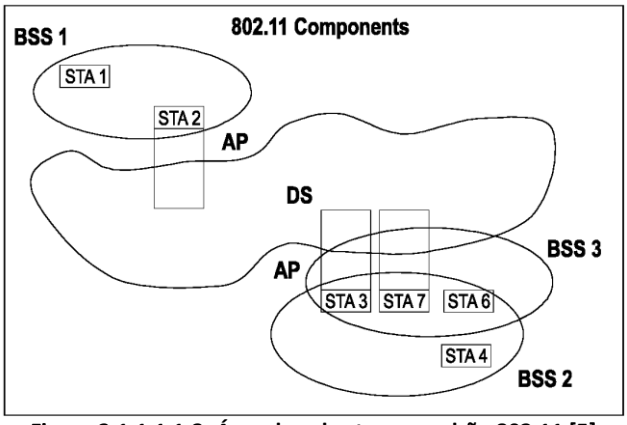

Figura 2.1.1.1.1-3: Área de cobertura – padrão 802.11 [5]

2.1.2. WiMAX

WiMAX é um acrónimo de *Worldwide Interoperability for Microwave Access* e trata-se de uma tecnologia que permite acesso à internet tanto de modo fixo como móvel, podendo abranger grandes áreas.

Tecnicamente o WiMAX é definido pela camada 1 (PHY) e pela camada 2 (MAC). Este utiliza *Orthogonal Frequency Division Multiple* (OFDM) como modo de transmissão e apresenta uma sofisticada camada MAC que permite uma utilização eficiente da frequência e da gestão de Qualidade de Serviço (QoS) de forma a obter elevadas taxas de transferencia e a suportar transmissão de vários tipos de serviços, tais como vídeo, jogos, voz, etc. Para esta transmissão podem ser utilizadas duas topologias diferentes:

- *Point to multi-point* (PMP)
- Mesh

Na topologia PMP, Figura 2.1.2-1, quando não é especificado explicitamente que determinada porção da *subframe* é atribuída a uma *Subscriber Station (SS)* específica, todas as SS poderão escutar essa porção. As *SS* verificam os identificadores de ligação (CID) no *Protocol Data Unit* (PDU) recebido e retêm apenas aqueles que lhe são endereçada, estas partilham o *uplink* para a BS consoante a necessidade. Dependendo da classe de serviço na SS, a esta podem-lhe ser garantidos direitos de transmissão pela BS após esta receber os respectivos pedidos.

No modo de operação *Mesh*, Figura 2.1.2-2, nenhum nó consegue transmitir sem que tenha de ser coordenado com outros nós. Através de escalonamento distributivo todos os nós devem coordenar as suas transmissões na respectiva vizinhança e devem fazer *broadcast* dos seus *schedules* para todos os seus vizinhos [6] [7].

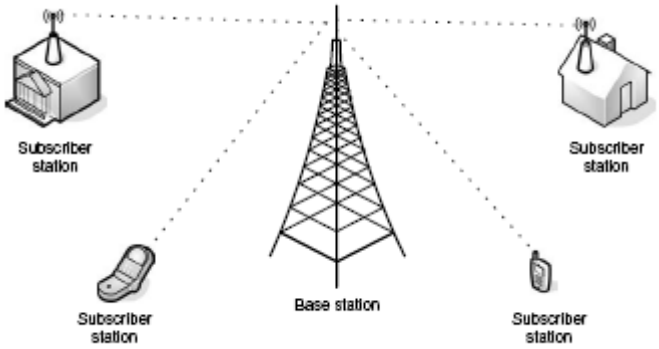

Figura 2.1.2-1: WiMAX - Topologia PMP [8]

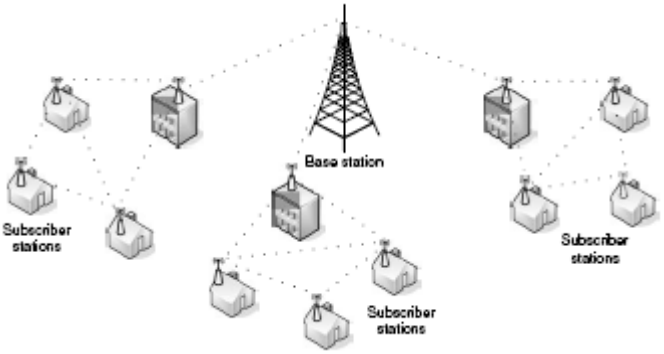

Figura 2.1.2-2: WiMAX – Topologia *Mesh* [8]

2.1.2.1. IEEE 802.16

O padrão IEEE 802.16, aprovado em Outubro de 2001 e publicado em Abril de 2002, vem especificar uma interface sem fios para redes metropolitanas, as redes *Wireless Metropolitan Area Network* (WMAN). Este padrão define as camadas PHY e MAC, tendo como objectivo integrar estas camadas criadas pelo IEEE com os protocolos de rede. Este padrão surge no mercado através do WiMAX que é criado por um grupo de indústrias designadas por WiMAX Forum.

Após a publicação do primeiro padrão seguiram-se mais três, o 802.16a, 802.16b e o 802.16c, com o intuito de resolver problemas relacionados com o espectro de frequência, Qualidade de Serviço e a inter-operabilidade.

Actualmente o IEEE 802.16 contém duas variantes:

- IEEE 802.16-2004 – define um padrão de acesso sem fios de banda larga fixa, utiliza o *Orthogonal frequency-division multiplexing* (OFDM) como técnica de acesso ao canal e suporta ambientes *Line of Sight* (LOS) na banda 10-66 GHz e *Non Line of Sight* (NLOS) na banda entre 2 e 11 GHZ [9].

- IEEE 802.16e-2005 – define um padrão de acesso sem fios de banda larga móvel, efectuando um conjunto de alterações e melhorias relativamente ao IEEE 802.16-2004 no que diz respeito ao processo de mobilidade, ao suporte de Qualidade de Serviço e à utilização do OFDMA [10].

Mais tarde, já em 2006, surge uma actualização do padrão IEEE 802.16e, designada por IEEE 802.16g, que apresenta melhorias relativamente ao processo de *handover* e ao *roaming* a alta velocidade, permitindo também a total mobilidade da SS que passa a poder deslocar-se a uma velocidade de 150 km/h.

2.1.2.1.1. MAC

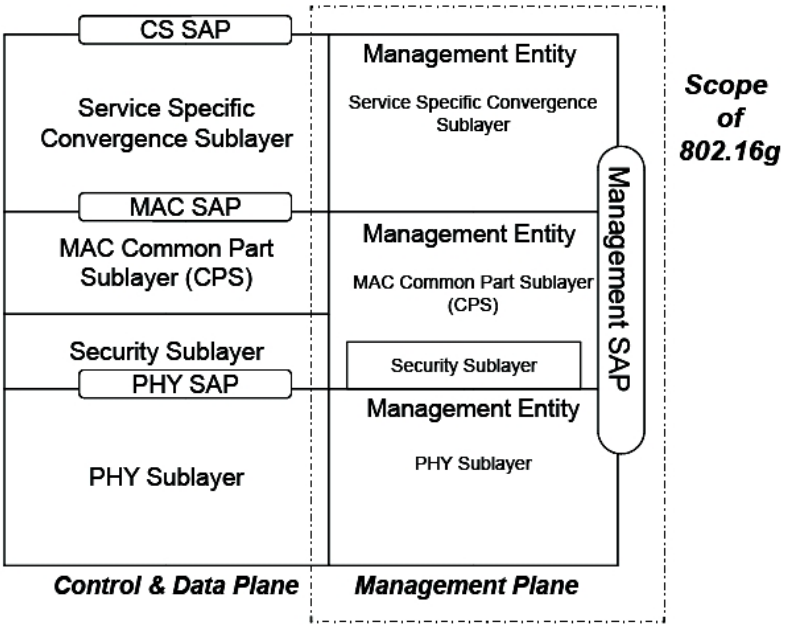

Figura 2.1.2.1.1-1: Modelo referência do 802.16 [11]

Como podemos ver pela Figura 2.1.2.1.1-1 a camada MAC pode-se dividir em três sub-camadas:

***Convergence sublayer* (CS)**

Esta subcamada opera com a convergência de serviços suportando tanto serviços ATM como serviços de pacotes tais como IPv4, IPv6, Ethernet e serviços VLAN, contendo um grande número de funções, tais como:

- Aceitar *service data units* (SDUs) vindos das camadas superiores.
- Classificação e mapeamento dos SDUs nos apropriados *Connections Identifiers* (CIDs), tratando-se esta de uma função básica de QoS (Figura 2.1.2.1.1-2).
- Processar os SDUs das camadas mais altas baseando-se na sua classificação.

- Entregar o CS Protocol Data Units (PDUs) ao Service Access Point (SAP) adequado.

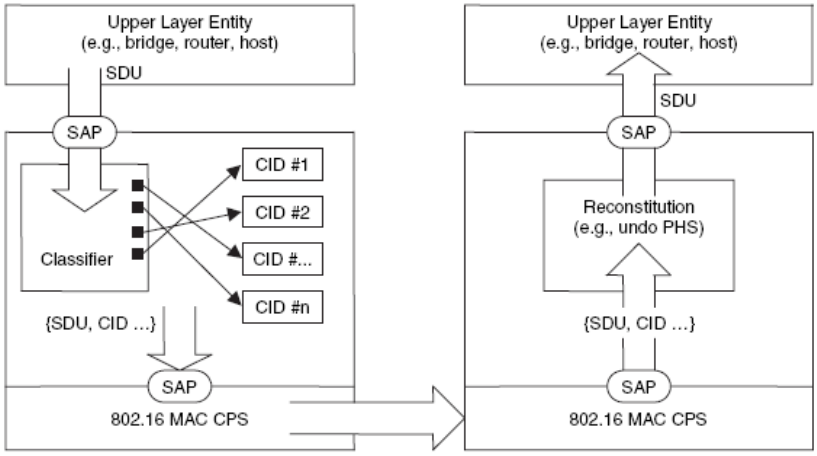

Figura 2.1.2.1.1-2: Classificação e mapeamento do CID [12]

***MAC Common Part Sub-layer* (MAC CPS)**

Sendo esta subcamada a responsável por definir o método de acesso ao meio, esta é uma das principais camadas MAC. Fornece funções relacionadas com duplexagem, acesso ao canal, entre outros. Perante isto, são dadas regras e mecanismos para acesso ao sistema, alocação de largura de banda e manutenção da ligação.

É nesta subcamada que são feitas as decisões relativas ao escalonamento (QoS). O QoS é tomado em consideração para a transmissão e o *scheduling* dos dados sobre a camada PHY.

Existem quatro classes de serviços definidas:

- *Best effort* (BE) – utilizado para serviços com menor prioridade no que diz respeito à restrição de tempo, tais como e-mail, navegação na internet, etc.
- *Non-real-time Polling Services* (nrtPS) – utilizado em serviços do tipo *non-real-time* que tem algumas restrições com o tempo, tais como o FTP.
- *Real-time Polling Services* (rtPS) – utilizado em serviços *real-time* com uma taxa de dados variável, como por exemplo o vídeo MPEG.
- *Unsolicited Grant Services* (UGS) – utilizado em serviços com um *bitrate* constante e garante pacotes de tamanho fixos emitidos em intervalos periódicos [13].

Security Sub-layer

Esta sub-camada é responsável pela autenticação, troca de chaves de modo seguro e encriptação.

Como já foi mencionado anteriormente, para que o WiMAX possa suportar mobilidade este baseia-se no padrão IEEE 802.16e que especifica uma camada MAC para processos de *handover*. Existem duas situações que levam ao desencadeamento de um processo de *handover*:

- Quando o *mobile node* (MN) se move e necessita de mudar de uma BS para outra, por motivos de perda de sinal, por exemplo;
- Quando existe outra BS que pode fornecer melhor QoS à estação móvel [1].

No padrão IEEE 802.16e o processo de *handover* pode-se dividir em duas fases:

- **Aquisição da topologia da rede**

  Para que se possa realizar um *handover* o MN necessita de adquirir informações relativas às redes que o envolvem, as quais podem ser obtidas através dos *network topology advertisements* ou através de um *scanning* às BSs vizinhas.

  Network topology advertisements é uma mensagem que é enviada em *broadcast* por todas as BSs e que contém informação relativa ao BSs vizinhos. Esta informação permite simplificar o processo de sincronização do MN com a sua nova BS.

  Adicionalmente o MN poderá efectuar um *scan* à área em que se encontra de forma a identificar as possíveis BSs alvo e estimar a qualidade dos canais existentes.

- **Processo de *handover***

  O processo de *handover* é composto por cinco fases distintas:

  - *Cell reselection* – fase em que se adquire informação sobre as BSs na rede. Esta informação é utilizada para avaliar a possibilidade da realização do *handover*.

  - Decisão e iniciação de *handover* – processo de decisão para migrar da BS actual para uma BS alvo. Esta decisão pode ser tomada tanto no MN como no BS.

  - *Sincronização com a BS alvo de downlink* – para que o MN possa estabelecer comunicação com o BS alvo o MN têm de se sincronizar com o seu canal *downlink*. Durante esta fase o MN recebe os parâmetros de transmissão de *downlink* e *uplink*.

  - *Ranging* – Após a sincronização do MN com o canal é necessário realizar o *ranging* ou *handover ranging*. O *ranging* é o processo onde o MN recebe os parâmetros correctos de transmissão, ou seja, o tempo de *offset* e o nível da potência. A BS alvo pode obter informações sobre o MN através do *backbone*, dependendo do que a BS saiba relativamente ao MN podem ser omitidas algumas partes deste processo.

  - Terminação do serviço – este é o último passo no processo de *handover,* onde a BS irá terminar todas as conexões ao MN [13].

2.1.3. 3GPP

Third Generation Partnership Project (3GPP) é uma colaboração entre vários grupos de associações de telecomunicações, que têm como objectivo padronizar a criação, envio e reprodução de arquivos multimédia em telemóveis e dispositivos *wireless*.

O 3GPP não deve ser confundido com o *3rd Generation Partnership Project 2* (3GPP2), que especifica as normas para outra rede 3G baseada em IS-95 (CDMA) também conhecida por CDMA 2000.

Actualmente existem quatro gerações, embora a última ainda esteja em desenvolvimento. A primeira geração (1G) foi desenvolvida a nível nacional, sendo os principais requisitos técnicos definidos entre a operadora de telecomunicações e a indústria, deste modo não foi possível uma publicação geral das especificações, dado que estas dependem de país para país. Devido À existência de liberdade na definição das especificações surgiu a incompatibilidade entre as várias redes. Esta primeira geração usava técnicas de transmissão analógicas e as normas que mais a marcaram foram: *Nordic Mobile Telephone* (NMT) e a *Total Access Communications System* (TACS).

Mais tarde surge então a segunda geração (2G), tendo como principais características a compatibilidade e transparência a nível internacional permitindo aos utilizadores o acesso à rede numa vasta área. Para além de suportar serviços de voz, como já acontecia na 1G, esta tem suporte de alguns serviços de dados. Outra grande diferença relativamente à 1G prende-se com o facto de esta utilizar técnicas de transmissão digitais e um mesmo canal poder suportar vários utilizadores simultaneamente. Dentro desta geração, a tecnologia mais bem sucedida foi o GSM.

Ainda antes de se efectuar a transição para a terceira geração surge a versão 2.5G que não é definida oficialmente pela União Internacional de Telecomunicações (UIT). Esta surge como uma actualização à 2G permitindo velocidades superiores, através de tecnologias de pacotes, permitindo um acesso à internet mais flexível e eficiente. A principal norma utilizada passou a ser o *General Packet Radio Service* (GPRS), dado que o GSM tinha o problema de ter uma baixa taxa de transmissão.

A rápida evolução das telecomunicações móveis faz com que apareça uma das gerações mais bem sucedidas da história, a terceira geração (3G). Esta é baseada nas normas do UIT oferecendo uma maior gama de serviços devido a ter uma melhor eficiência espectral. Entre estes serviços encontra-se as chamadas de voz e a transmissão de dados a longas distâncias, permitindo maiores taxas e número de clientes comparativamente com as gerações anteriores. O 3G utiliza o espectro de radiofrequência em bandas identificadas utilizando na Europa a norma *Universal Mobile Telecommunications System* (UMTS) [14] [15].

Actualmente tem-se vindo a definir a quarta geração (4G), em que esta é também designada por *Long Term Evolution Advanced.*

2.1.3.1. GSM

O Global System for Mobile Communications (GSM) trata-se da tecnologia mais popular em todo o mundo para telemóveis. Esta tecnologia distingue-se dos seus antecessores devido a utilizar sinais e canais de voz digitais, pertencendo deste modo à 2G.

Os motivos de sucesso do GSM são:

- Serviços abrangentes e características do sistema
    - Oferece chamadas de voz, pequenas mensagens, fax, serviço de dados e ampla gama de serviços complementares.
    - Capacidade de *roaming* a nível global (em mais de 100 países).
    - Oferece aos operadores de rede a capacidade de escolha dos métodos de codificação.
- Grande qualidade, capacidade e segurança
    - Oferece qualidade a nível de voz, dados e serviços.
    - Oferece uma grande eficiência espectral devido ao avanço da tecnologia TDMA com controlo de energia, transmissão descontínua, etc.
    - Sistema avançado de segurança.
- Equipamentos de custo reduzido

O GSM utiliza canais de rádio de 200kHz e desenvolvido para diferentes bandas de frequência, nomeadamente 900, 1800 e 1900 MHz [16].

2.1.3.2. GPRS

General Packet Radio Service (GPRS) foi desenvolvido para permitir aos utilizadores do GSM responder à crescente evolução dos serviços de dados por pacotes, causado pelo explosivo crescimento da internet. As aplicações que utilizam este tipo de serviço em redes sem fios necessitam de débitos relativamente elevados e são caracterizados pelo tráfego em rajada e por necessitarem de transferência assimétrica. Embora seja uma tecnologia destinada apenas a dados, também permite melhorar a capacidade de voz do GSM dando a capacidade de acomodar o tráfego de voz adicional sem se necessitar de uma aquisição extra de espectro.

O GPRS suporta taxas de dados com picos de *download* até 115 kbps com uma velocidade média de 40 a 50 kbps, sendo estas velocidades suficientes para aplicações como *Multimedia Messaging Service* (MMS) e navegação na internet. Para além destas características o GPRS permite ainda manter uma sessão de dados enquanto se atende uma chamada telefónica e fornece uma ligação de dados *always-on*, ou seja, os utilizadores apenas pagam pelos dados em si e não pelo tempo de ligação e download de dados.

O GPRS é associado à tecnologia 2.5G, pois é o primeiro passo para o serviço de dados sem fios e consequentemente para a 3G.

Os equipamentos suportados pelo GPRS estão divididos em três classes:

- Classe A – permite a ligação a ambos os serviços, GPRS e GSM (voz e SMS), simultaneamente.
- Classe B – permite a ligação a ambos os serviços, GPRS e GSM, mas não simultaneamente. Neste caso aquando o uso de serviços GSM, chamadas de voz ou SMS, o GPRS tem de estar desactivado.
- Classe C – Permite estar conectado só a GPRS ou só a GSM, sendo que o processo de troca tem de ser efectuado manualmente [17].

Para o transporte de voz o GPRS utiliza a arquitectura de rede já definida do GSM e acede a redes de dados que utilizem o protocolo IP. Deste modo o GPRS permite serviços não suportados pelo GSM, nomeadamente:

- Serviços ponto a ponto (PTP) – capacidade de se ligar em modo cliente - servidor a uma máquina de rede IP.

- Serviços ponto a multiponto (PTMP) – capacidade de enviar um pacote a um grupo de destinatários, ou seja, em multicast.

2.1.3.3. UMTS

Universal Mobile Telecommunications System (UMTS) é uma das tecnologias da rede 3G e surge como uma evolução ao GSM/GPRS, o que faz com que o UMTS tenha vários elementos e princípios de funcionamento do GSM, tornando o processo de transição entre as duas tecnologias mais fácil e económico.

O UMTS é orientado à difusão generalizada de serviços, permite múltiplos fluxos multimédia numa única ligação e utiliza o padrão *Wideband Code Division Multiple Access* (WCDMA) como mecanismo de codificação, sendo este uma variante do *Frequency Division Duplex* (FDD) e do *Time Division Duplex* (TDD) [18].

No formato original o UMTS possibilita transportar dados a velocidades de 2Mbps, tendo a capacidade de transportar mais de 100 chamadas de voz simultaneamente usando uma largura de banda de 5MHz.

UMTS

Telecomunicações:

- Mobilidade
- Serviço de comutação de circuitos
- Serviço de comutação de dados

Internet:

- Acesso à internet
- E-mail
- Transferência de imagens em tempo real
- Transferência de documentos multimédia

Conteúdos:

- Vídeo
- Serviços interactivos de vídeo
- Televisão e rádio
- Serviços de entretimento

Figura 2.1.3.3-1: UMTS – Convergência de mídea, dados e telecomunicações

2.1.3.3.1. Arquitectura

De forma a representar a arquitectura geral do UMTS temos a Figura 2.1.3.3.1-1:

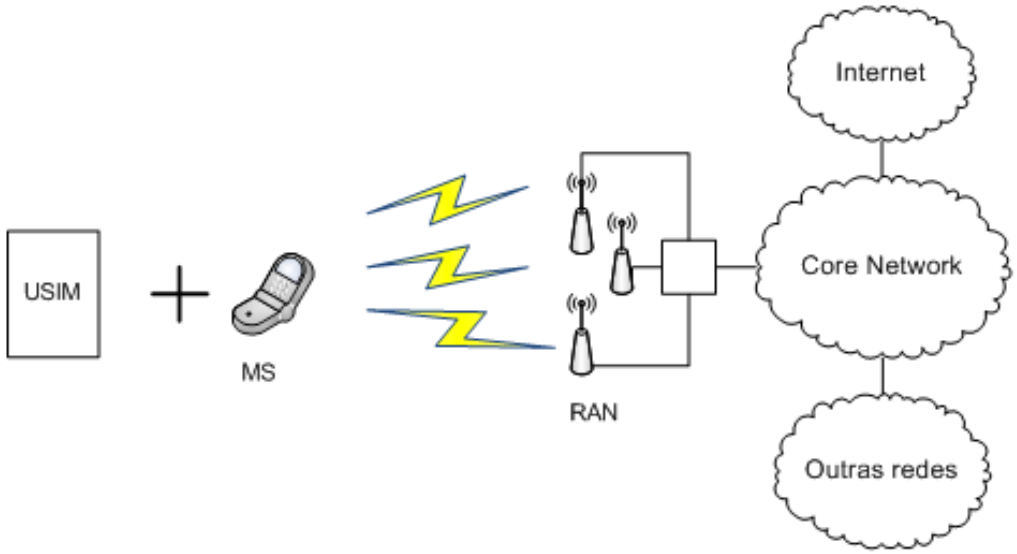

Figura 2.1.3.3.1-1: UMTS – Arquitectura básica

O UMTS *Subscriber Identity Module* (USIM), tal como já acontecia para o GSM, é um chip que contém informações relativas ao utilizador e contém uma palavra-chave para autenticar o acesso de um utilizador a uma rede. A partir do momento em que o USIM pertence a uma determinada

rede operadora, passa a existir uma relação contratual entre o utilizador e a operadora correspondente.

Para o caso do UMTS é atribuído o nome de *Mobile Equipment* (ME) ao terminal. Neste estão incorporados os protocolos da interface rádio bem como os elementos de funcionamento da interface do utilizador. É neste elemento que é inserido o USIM.

A infra-estrutura de rede fixa que contém as instalações de transmissão rádio é designada por *Radio Access Network* (RAN), esta é composta por uma estação base, designada por *Node* B e um *Radio Network Controller* (RNC) que conecta o RAN à *Core Network*. O RAN incorpora todas as tarefas que estão relacionadas com a transmissão de informação via rádio, sendo que deste modo, para se suportar outras interfaces rádio basta modificar o RAN.

A *Core Network* é a rede responsável por transportar a informação de todos os utilizadores ao destino respectivo. Esta contém um elevado número de sistemas de comutação bem como *gateways* para outras redes, tal como o *Integrated Services Digital Network* (ISDN) ou a Internet. A *Core Network* contém ainda uma base de dados que utiliza para a gestão de mobilidade, gestão de utilizadores e para a facturação [19].

2.1.3.3.1.1. UTRAN

UMTS *Terrestrial Radio Access Network* (UTRAN) trata-se da arquitectura rádio usada pela tecnologia UMTS, ou seja, o RAN apresentado na Figura 2.1.3.3.1-1. Tal como já foi mencionado esta é composta pelo *Node* B e pelo RNC.

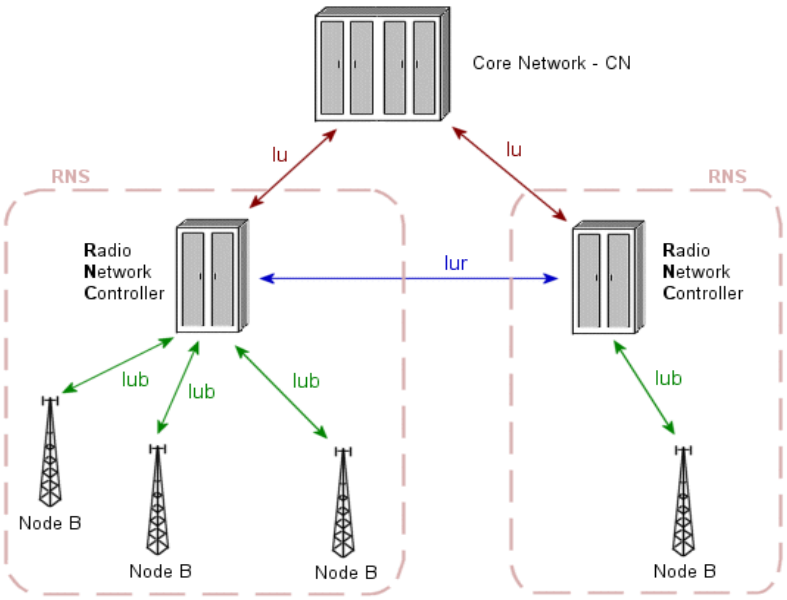

Figura 2.1.3.3.1.1-1: Arquitectura do UTRAN [1]

Relativamente ao *Node B*, este é responsável pelas seguintes funções:

- Interface de transmissão/recepção.

- Modulação.
- Codificação do canal.
- Micro diversidade.
- Controlo de potência.

Para o caso do RNC temos:

- Controlo dos recursos de rádio.
- Controlo de admissão.
- Atribuição de canal.
- Macro diversidade.
- Sinalização *broadcast.*
- Segmentação.
- Controlo de definições de potência.
- Controlo de *Handover.*
- Cifragem

2.1.3.3.2. Mecanismos de QoS

Relativamente ao QoS, o UMTS apresenta a capacidade de transmitir informação entre pontos de acesso, possibilitando a definição das características relativas à ligação utilizada. Este permite ainda a diferenciação de fluxos através de mecanismos de sinalização e escalonamento e diferencia quatro tipos de serviços, dependendo do tipo de tráfego a transporta, nomeadamente:

- Conversação - vós, vídeo-chamadas, jogos de vídeo;
- *Streaming* – multimédia, webcast;
- Interactivo - *web browsing,* jogos em rede, acessos a base de dados;
- *Background* – sms, correio electrónico, *downloads*;

2.1.3.4. HSPA

High Speed Packet Access (HSPA) é a terminologia utilizada quando estamos perante a utilização das tecnologias *High Speed Downlink Packet Access* (HSDPA) e *High Speed Uplink Packet Access* (HSUPA). Esta tecnologia é baseada na 3G (UMTS/WCDMA) e é vista como uma das principais tecnologias de dados móveis para um futuro próximo.

O HSDPA e o HSUPA são utilizados para optimizar tanto o *downlink* como o *uplink*, respectivamente, estes incluem melhorias a nível de *throughput*, redução de latência e aumento da eficiência espectral.

No início de 2009, a maioria das redes HSPA conseguiam oferecer a nível de *downlink* uma taxa de pico de 3.6 Mbps. No entanto estes valores foram progredindo, chegando a atingir uma taxa de pico de *downlink* de 14.4 Mbps, teoricamente.

2.1.3.4.1. HSDPA

O HSDPA (*release 5*) surge como uma actualização ao UMTS, permitindo um aumento das velocidades de download para cerca de 14.4Mbitps. Este tipo de velocidades é ideal para aplicações que utilizem de forma intensiva a largura de banda, tais como o *streaming* de multimédia ou mesmo para uma navegação rápida na internet. O HSDPA permite ainda obter baixas latências, cerca de 70 a 100 milissegundo, o que o torna ideal para aplicações em tempo real. Para que seja possível este melhoramento a nível de *downlink* o HSDPA utiliza várias técnicas tanto do lado do servidor como do lado do cliente (terminal). Do lado do servidor temos a modulação e codificação adaptativa, *hybrid* ARQ e um rápido *scheduling*. Já para o lado do terminal este é baseado na utilização do CDMA.

No que diz respeito às operadoras, esta tecnologia apresenta vantagens, ao proporcionar uma utilização mais eficiente do espectro, as operadoras passam a poder agrupar um maior número de utilizadores e serviços no mesmo espectro, não necessitando de obterem espectro adicional.

O processo de transição para esta tecnologia a partir do UMTS torna-se extremamente simples e pouco dispendiosa, dado que não necessita da substituição de elementos importantes da infra-estrutura do UMTS. Para este processo basta uma simples troca de software e de cartões [20].

2.1.3.4.2. HSUPA

O HSUPA (*release 5*) surge como uma actualização do UMTS-HSDPA e utiliza o *Enhanced Dedicated Channel* (E-DCH) de forma a proporcionar uma optimização no que diz respeito ao *uplink*. Este permite aumentar a velocidade de *uplink* do HSDPA de 384 kbps para uma taxa de pico de 5.76 Mbps, teoricamente [21].

Para que o HSUPA consiga este melhoramento a nível de *uplink*, este contém as seguintes características:

- Um canal físico dedicado.
- Reduzido tempo de transmissão, o que permite respostas mais rápidas às mudanças das condições de transmissão.
- Permite a alocação de recursos rádio através da estação base de modo eficiente.

- Melhoramento no processamento de erros através do *Hybrid Automatic Repeat request* (HARQ).

O melhoramento a nível de *uplink* permitiu também um melhoramento a nível da cobertura, possibilitando células maiores.

2.1.3.4.3. HSPA+

High Speed Packet Access Plus (HSPA+) surge com o intuito de prolongar a "vida" das redes HSPA aplicando algumas das técnicas utilizadas no *Long Term Evolution* (LTE). Esta tecnologia apresenta um melhor desempenho e suporte para aplicações em tempo real, serviços de conversação interactivos e partilha de vídeo e voz sobre IP (VoIP), recorrendo à introdução de recursos como o *Multiple-input multiple-output* (MIMO), *Continuous Packet Connectivity* (CPC) e maiores ordens de modulação.

As principais características desta tecnologia são:

- Fácil de proceder à sua actualização através das redes HSPA.
- Oferece um plano estratégico de desempenho para os operadores GSM-HSPA.
- Permite aumentar a capacidade do HSPA bem como reduzir a sua latência abaixo dos 50 ms.
- A primeira fase do HSPA+ com o processo de modulação 64 QAM consegue oferecer taxas de pico de *downlink* de 21 Mbps, teoricamente.
- Utiliza técnicas que permitem a inter-funcionalidade com o LTE.
- Suporta serviços de voz e dados na mesma transportadora e em todos os espectros de radiofrequência disponível e permite oferecer este tipo de serviços simultaneamente aos utilizadores [22].

2.1.3.5. LTE

Long Term Evolution (LTE) é actualmente o nome de um projecto do 3GPP que teve início em Novembro de 2004 e irá permitir aos utilizadores atingirem picos de débitos maiores do que os já atingidos pelo HSPA+ com um maior espectro de largura de banda.

Um dos objectivos principais do LTE é proporcionar um desempenho elevado a nível da tecnologia de acesso que permite oferecer mobilidade a velocidades elevadas e ter a capacidade de interagir com redes HSPA ou mesmo com as redes anteriores a esta. Esta tecnologia é baseada no *Internet protocol* (IP), sendo indicada para suportar voz a nível de pacotes. Utiliza como

processo de modulação o *Orthogonal Frequency Division Multiple Access* (OFDMA), que é adequado para atingir elevadas taxas de dados num grande espectro de largura de banda. No entanto para o *uplink* a utilização do OFDMA provocaria um elevado *Peak to Average Ratio* (PAR) no sinal, o que iria comprometer a eficiência energética bem como a durabilidade da bateria. De forma a ultrapassar este problema o LTE utiliza para *uplink* o *Single Carrier* FDMA (SC-FDMA) [23].

O LTE apresenta então as seguintes características:

- Taxas de pico de *downlink* até 326 Mbps com uma largura de banda de 20MHz.
- Taxas de pico de *uplink* até 86.4 Mbps com uma largura de banda de 20MHz.
- Opera em ambos os modos, TDD e FDD.
- Largura de banda escalável até 20 Mhz.
- Aumento da eficiência espectral.
- Redução da latência, até 10 ms de tempo de ida e volta entre o equipamento do utilizador e a estação base.

O facto da largura de banda ser escalável torna o processo de migração entre as redes HSPA e LTE mais fácil de realizar.

LTE-*Advanced*:

Como evolução ao LTE já se encontra em desenvolvimento o LTE-*Advanced*, este surge com o intuito de ultrapassar os requisitos definidos pelo UIT para poder ser considerada como a quarta geração (4G).

2.1.3.5.1. E-UTRAN

Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) surge como uma evolução ao UTRAN e trata-se da rede de acesso rádio utilizada pelo LTE.

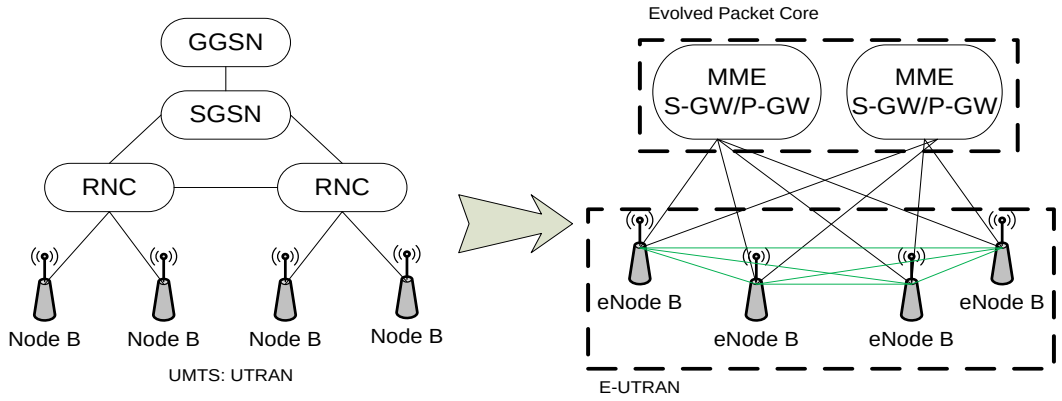

Figura 2.1.3.5.1-1: Evolução do E-UTRAN - Arquitectura

Como se pode observar pela Figura 2.1.3.5.1-1, o E-UTRAN é composto pelos *eNodes B*, que incluem todas as funções relacionadas com a interface rádio e os *Mobility Management Entity's* (MMEs), responsáveis pela gestão de mobilidade, identificação dos equipamentos dos utilizadores

e parâmetros de segurança. Esta entidade é exclusivamente dedicada á sinalização não tendo qualquer relação com o tráfego de dados.

Relativamente ao *Serving Gateway* (S-GW), este contém funções de tratamento de tráfego de dados e de tráfego de sinalização. O S-GW permite o encaminhamento de tráfego de e para o eNode B, funcionando como a "base" do processo de mobilidade.

O *Packet Data Network Gateway* (P-GW) possui funcionalidades ao nível IP executando a atribuição de endereços, classificação e encaminhamento de pacotes e aplicação de políticas de QoS.

2.1.4. Mobilidade

A nível de mobilidade, tal como se pode observar pela Figura 2.1.4-1, cada tecnologia existente apresenta características distintas que se adequam a cenários distintos.

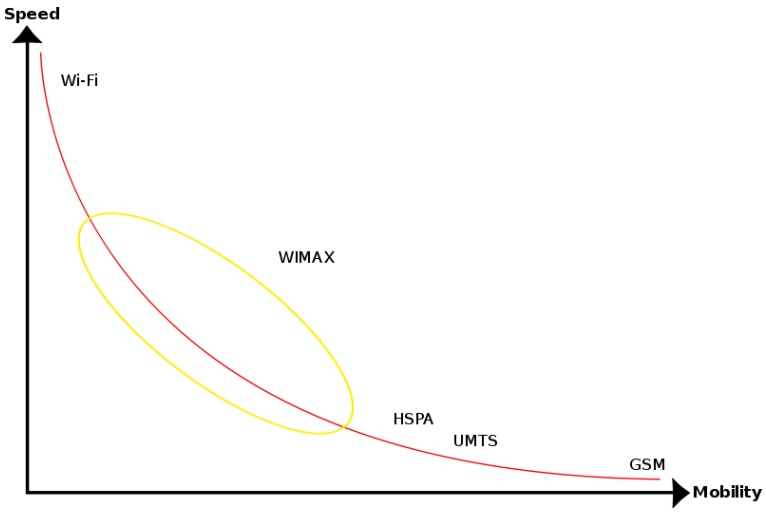

Figura 2.1.4-1: Redes sem fios – *Speed* vs *Mobility* [1]

Relativamente ao Wi-Fi, este não é propriamente a tecnologia sem fios mais apropriada em termos de mobilidade para grandes áreas, comporta-se bem na deslocação dentro de um centro comercial ou de um hospital, ou seja, em espaços reduzidos, mas para o caso de grandes deslocações, por exemplo, efectuar um deslocamento de carro entre dois pontos distantes esta já não será a mais indicada.

Tecnologias tais como o HSPA, UMTS e GSM são tecnologias extremamente versáteis a nível de mobilidade, conseguindo abranger uma vasta área geográfica, embora limitadas na velocidade que conseguem atingir, sendo esta inferior comparativamente com o Wi-Fi ou mesmo o WiMAX.

A melhor relação existente entre velocidade e mobilidade ocorre para o caso do WiMAX, sendo que esta tecnologia apresenta boas características tanto a nível da sua mobilidade como a nível das velocidades que consegue atingir.

2.2. Protocolos de Mobilidade

2.2.1. Mobilidade IP

Com a extrema necessidade de mobilidade entre redes IP começam a surgir alguns mecanismos de forma a suportar a mobilidade exigida. O primeiro mecanismo que surge neste campo é designado por *Mobile IP* (MIP), este é uma extensão do protocolo IP para dar suporte à mobilidade e destina-se a permitir que terminais móveis possam deslocar-se entre diferentes redes mantendo o mesmo IP e encaminhando os pacotes, do terminal móvel ou para o terminal móvel, de forma transparente para as camadas superiores. Trata-se de um mecanismo adequado tanto para redes homogéneas como heterogéneas, ou seja, possibilita a mobilidade, a nível da camada de rede, entre redes da mesma tecnologia bem como entre redes de tecnologias diferentes.

De forma a resolver a questão da mobilidade nas redes IP torna-se necessário considerar dois tipos de mobilidade, a macro-mobilidade e a micro-mobilidade, tal como se pode observar na Figura 2.2.1-1.

A micro-mobilidade está relacionada com a mobilidade dentro do mesmo domínio, não afectando deste modo a camada de rede IP. Este tipo de mobilidade pode ser resolvida utilizando protocolos de comunicação entre *Access Points* e tem como objectivo a obtenção de melhor qualidade de sinal.

Por outro lado, a macro-mobilidade está relacionada com a mobilidade entre domínios, o que implica a afectação da camada de rede IP. A resolução dos problemas deste tipo de mobilidade é efectuada através da utilização de alguns protocolos de mobilidade, tais como o MIPv4 e o MIPv6.

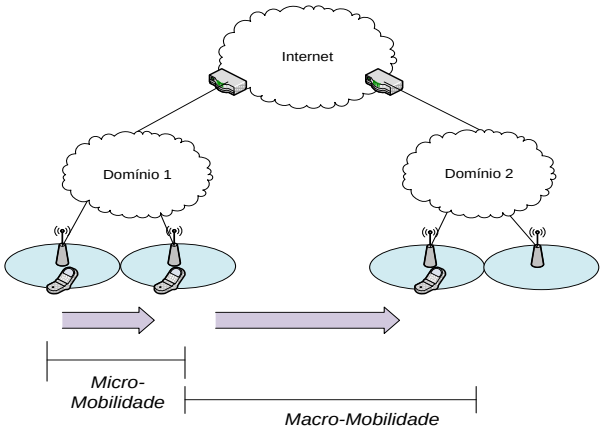

Figura 2.2.1-1: Mobilidade IP – micro-mobilidade e macro-mobilidade

2.2.1.1. Classificação de *Handovers*

Ao processo de transferência de acesso é atribuído a designação de *Handover* (HO), este trata-se de um processo crucial no que diz respeito à mobilidade de um terminal, pois uma boa

optimização deste processo permite uma boa continuidade de serviços sem quebras significativas de ligação.

O *handover* pode ser classificado a vários níveis, em âmbito, tecnologia, controlo, conectividade e desempenho. No que diz respeito ao âmbito este pode ser, já como foi mencionado anteriormente, a nível 2, intra-célula, caso seja efectuado entre interfaces numa mesma célula; ou inter-célula, caso sejam células diferentes e inter-rede quando existe mudança de rede de acesso. Relativamente à tecnologia este pode ser intra-tecnologia, ou seja, ocorre entre equipamentos da mesma tecnologia, ou inter-tecnologia, quando ocorre entre tecnologias diferentes. Os termos horizontal e vertical são idênticos à intra-tecnologia e inter-tecnologia, respectivamente, mas a nível da interface tecnológica. Para o controlo é necessário decidir quem inicia e controla este processo, quem auxilia e por onde estes são realizados. No processo de controlo pode-se ter então um controlo de *handover* centralizado, *Network Controled Handover* (NCHO), ou descentralizado, Mobile *Controled Handover* (MCHO). Para além destes, existe ainda a capacidade de cooperação entre o terminal móvel e a rede, para este processo estão definidos dois modos, o *Network Assisted Handover* (NAHO) e o *Mobile Assisted Handover* (MAHO). A nível de conectividade são definidos dois tipos possíveis, o *make-before-break handover*, que permite a coexistência de conectividade aos dois pontos de acesso, fazendo com que a nova ligação seja estabelecida antes da ligação "antiga" ser terminada e o *break-before-make handover.* Neste ultimo caso não é possível a existência simultânea dos dois pontos de acesso, o que implica que a ligação antiga seja terminada antes de a nova ser estabelecida. Finalmente, a nível de desempenho, o *handover* pode ser um *handover* suave (*smooth handover*), o que permite minimizar a perda de pacotes, um *handover* rápido, minimizando o tempo de atraso de comunicação, um *handover* transparente, ou seja, um *handover* rápido sem existência de perda de pacotes, e um *handover* baseado no contexto, que permite garantir a continuidade de uma determinada informação específica.

2.2.2. MIPv4

O *Mobile IP* version 4 (MIPv4) [24] trata-se de um protocolo que se destina a permitir a mobilidade IP utilizando como protocolo de endereçamento o IPv4. Este é um dos protocolos utilizados para resolver os problemas relativos à macro-mobilidade.

Dado que se trata de uma extensão ao IPv4 para que este seja capaz de suportar mobilidade, foi necessário definir-se três novas entidades:

- *Mobile Node* (MN) – trata-se de um *host* ou router que se pode movimentar de uma rede para outra. Este tem a capacidade de se movimentar mantendo o seu endereço IP constante, permitindo deste modo a continuidade de comunicação com outros nós.
- *Home Agent* (HA) – router presente na *Home Network* do MN responsável por registar a localização do MN permitindo que este esteja sempre alcançável. Esta entidade utiliza um túnel para enviar datagramas IP para o Care-of Address actual do MN.
- *Foreign Agent* (FA) – router presente na *Foreign Network*, ou seja, presente nas redes "estrangeiras" para onde se irá movimentar o MN. Este permite fornecer serviços de

encaminhamento enquanto o MN se encontrar na sua rede, de forma a o manter sempre acessível. Este agente recebe os datagramas enviados pelo HA via túnel entregando-os ao MN.

2.2.2.1. Terminologia

***Care-of Address* (CoA):**

Ponto de terminação do túnel com o HA, sendo do ponto de vista IP a verdadeira localização do MN. Este endereço permite ao MN estar sempre "alcançável" enquanto se encontra fora da sua HN.

Existem dois tipos de CoA, o *foreign agent CoA* que é o endereço do FA onde o MN se registou e o *co-located* CoA que é um endereço local obtido externamente que o MN associa como uma das suas interfaces de rede, neste caso a utilização do FA deixa de ser necessária.

Correspondent Node* (CN)*:

O CN trata-se do elemento com o qual o MN vai comunicar, este pode encontra-se tanto na HN como nas FNs.

***Foreign Network* (FN):**

Rede para a qual o MN se irá deslocar, ou seja, pode-se referir a todas as redes que não sejam a HN do MN em questão.

***Home Address* (HoA):**

Endereço atribuído ao MN que se mantém inalterado ao longo da sua movimentação. Este endereço encontra-se relacionado com a sua HN e permite um acesso permanente ao MN independentemente de este estar ou não na sua HN.

***Home Network* (HN)**

Rede definida como a mais provável para encontrar o MN, teoricamente. Esta deverá ter um prefixo de rede igual ao do MN e permitir que quando o MN se encontrar na HN este consiga receber todos os pacotes pelo processo normal de encaminhamento, sem que seja necessário aplicar qualquer processo de mobilidade.

Tunel:

"Caminho" pela qual os pacotes serão enviados sempre que o MN se encontra longe da sua HN. Este túnel é definido desde o HA até ao CoA actual do MN [24].

2.2.2.2. Arquitectura

Pela Figura 2.2.2.2-1 podemos observar a arquitectura básica do MIPv4 para que seja possível a realização de movimentação do MN sem que este deixe de ser acessível.

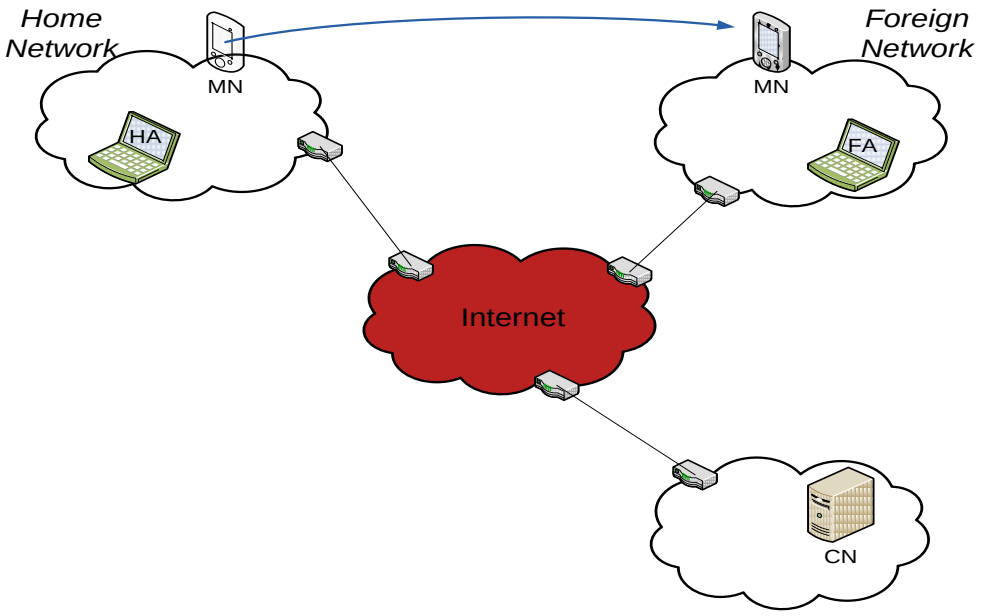

Figura 2.2.2.2-1: MIPv4 – Arquitectura

Existem três mecanismos básicos efectuados pelo MIPv4 para que a mobilidade seja possível:

- Descoberta do CoA – para a descoberta do CoA são utilizadas as mensagens ICMP *Router Advertisement* (RA). Estas mensagens são enviadas periodicamente ou de modo solicitado e contém informação relativa aos *default* routers de cada rede. São denominadas por *Agent Advertisements* e normalmente utilizadas pelos HAs para se darem a "conhecer". Estas mensagens tornam também possível a detecção de movimentação.

- Registo do CoA – Após a obtenção do CoA por parte do MN este necessita de transmitir essa informação ao seu HA para que os envios dos datagramas sejam redireccionados. Este processo pode ser feito directamente entre o MN e o seu HA ou através do FA, com o envio de mensagens de *Registration Request* e *Registration Reply*. O HA ao receber a informação relativa ao novo CoA utilizado pelo MN, adiciona-a à sua tabela de encaminhamento de forma a efectuar o redireccionamento dos datagramas.

- *Tunneling* para o CoA – para efectuar o processo de redireccionamento sempre que o MN não se encontra na sua HN é utilizado o processo de *tunneling* IP-em-IP.

Sempre que um MN se desloca para uma FN temos as seguintes trocas de mensagens, Figura 2.2.2.2-2:

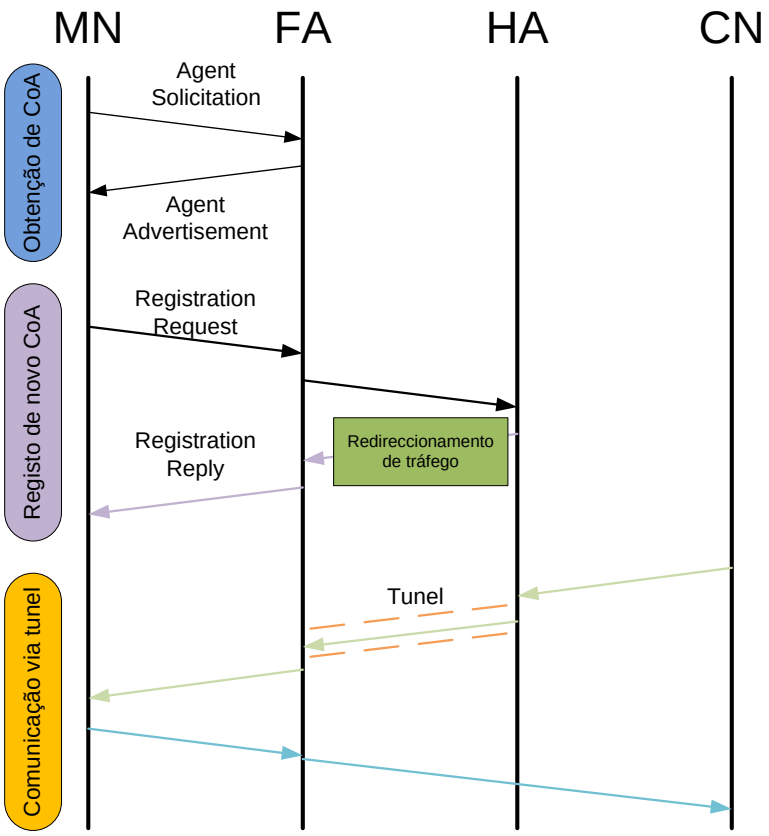

Figura 2.2.2.2-2: MIPv4 – Troca de mensagens durante processo de movimentação

Caso não existisse o FA, a troca de mensagens seria feita directamente com o HA, exceptuando a obtenção do CoA, que seria do tipo *co-located* CoA e o túnel que seria entre o HA e o MN.

2.2.3. MIPv6

O *mobile IP version 6* (MIPv6) é baseado no MIPv4 embora utilize para endereçamento o IPv6. Este surge com o intuito de resolver alguns dos problemas existentes no MIPv4 e optimizar o processo de mobilidade.

Podem-se então mencionar um conjunto de diferenças existentes entre o MIPv4 e o MIPv6:

- A obtenção dos CoAs passa a ser feita pelo MN de forma automática através do DHCPv6 ou da auto-configuração, suportada pelo IPv6, deixando de haver necessidade da utilização do FA.

- No MIPv4 os mecanismos de encaminhamento baseiam-se em *triangle routing*, sem optimização, enquanto no caso do MIPv6 esta optimização já é possível, eliminando o problema de *triangle routing*, ou seja, o MN e o CN podem "comunicar" directamente sem a interacção do HA.

- MIPv6 possibilita a capacidade do MN ter vários CoAs.

- No MIPv4 ao se enviarem datagramas do MN para o CN o endereço origem destes será o HoA, enquanto no caso do MIPv6 o endereço origem é o CoA primário, podendo opcionalmente indicar o seu HoA.

- O MIPv6 utiliza o *IPv6 Neighbor Unreachability* para detectar se o MN se encontra acessível.

- No MIPv6 a maioria dos pacotes enviados para o MN, enquanto este se encontrar longe da sua HN, são enviados usando o IPv6 *routing header* em vez do encapsulamento IP, o que permite a redução de sobrecarga comparativamente ao MIPv4.

- O MIPv6 é dissociado de qualquer camada de ligação, devido a utilizar o IPv6 *Neighbor Discovery* em vez do *Address Resolution Protocol* (ARP), o que dá uma maior robustez a este protocolo.

- O mecanismo *dynamic home agent address discovery* utilizado no MIPv6 retorna apenas uma resposta, enquanto no MIPv4 o processo similar retorna uma resposta de cada HA [25].

2.2.3.1. Arquitectura

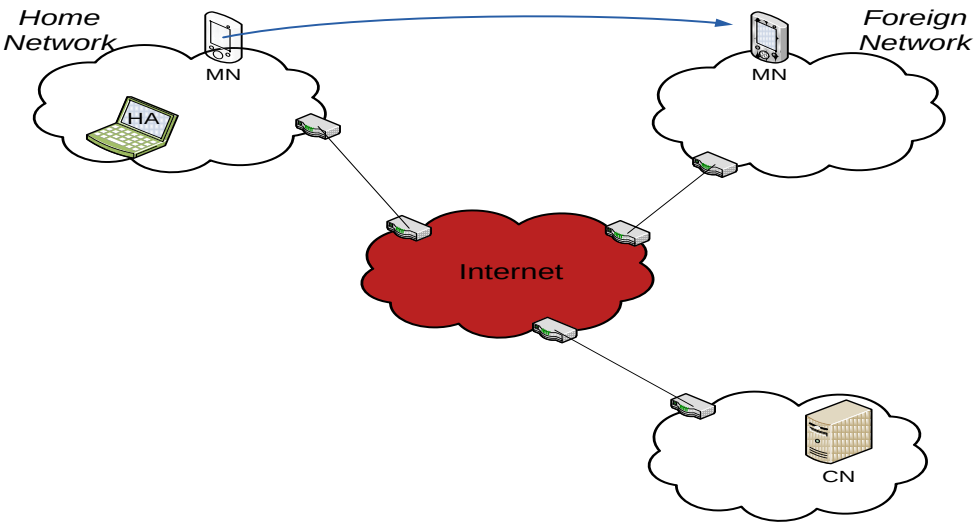

Figura 2.2.3.1-1: MIPv6 – Arquitectura

Como se pode ver pela Figura 2.2.3.1-1, a arquitectura é idêntica à já apresentada para o caso do MIPv4, com excepção de não termos a presença do FN.

Quando o MN se move para a FN, este inicia o processo para obter um novo CoA, sendo que o CoA pode ser obtido por *stateless address auto-configuration* ou *statefull address auto-configuration*, ou seja, através da recepção de *routers advertisements* enviados pelo *default* router da rede ou via servidor DHCP, respectivamente.

Após a obtenção do CoA por parte do MN torna-se necessário que este o registe no seu respectivo HA. Este registo é efectuado através do envio da mensagem *Binding Update* (BU), contendo informação relativa ao novo CoA, para o HA. Paralelamente, a informação relativa ao envio do BU é adicionada a uma *Binding Update List* presente no MN com o respectivo tempo de validação da mensagem enviada. O HA ao receber esta mensagem irá colocar essa informação numa *Binding Cache* (BC) para que quando receber um pacote para o HoA do MN este vá verificar à sua lista se o MN em questão lhe "pertence" e reencaminhe o pacote para o destino pretendido. Seguidamente é enviada a mensagem *Binding Acknowledgement* (BA) ao MN indicando se a actualização do CoA foi aceite ou não. O processo de troca das mensagens BU e BA é feito periodicamente para actualizar o registo, permitindo que o CoA continue válido.

Terminado o processo de registo, é estabelecido o túnel entre o HA e o MN.

Para que o CN possa comunicar com o MN existem dois processos distintos. Caso o CN suporte o protocolo MIPv6, após o MN receber o BA por parte do seu HA, este iniciará o processo de registo do seu novo CoA no CN. Este processo consiste no *Return routability procedure* seguido do respectivo registo. O processo de *Return routability* é efectuado através do envio de duas mensagens, a *Home Test Init* que é enviada para o CN via HA e a *Care-of Test Init* que é enviada directamente para o CN. Estas mensagens têm como finalidade a obtenção de uma *home keygen token* e uma *care-of keygen token* que são enviadas via *Home-Test* e *Care-Test*, respectivamente. Seguidamente, após a obtenção por parte do MN da *home keygen token* e da *care-of keygen token* este pode enviar um BU, com as respectivas garantias de validade, para o CN para que este actualize a sua BC. Por fim, o CN envia um BA ao MN indicando que a actualização foi aceite. A partir deste momento toda a comunicação entre o MN e o CN será efectuada directamente, pois sempre que o CN pretender enviar um pacote este irá verificar a sua BC de forma a identificar um CoA correspondente ao MN. Este processo tem a designação de optimização de rota.

Caso o CN não suporte o protocolo MIPv6 e pretenda enviar pacotes para o MN, não se encontrando este na sua HN, os pacotes serão interceptados pelo HA recorrendo ao *Proxy Neighbor Discovery* (PND), uma vez que este age como proxy da rede para o MN na ausência deste. Ao interceptar os pacotes, o HA deduz que o CN não tem o CoA do MN na sua BC e reencaminha-os via túnel para o MN. A resposta por parte do MN será efectuada através do túnel, efectuando o percurso inverso. Este processo é designado por *Reverse Tunneled*.

Para demonstrar a troca de mensagens existentes entre as principais entidades no processo de *handover* com optimização de rota temos a Figura 2.2.3.1-2:

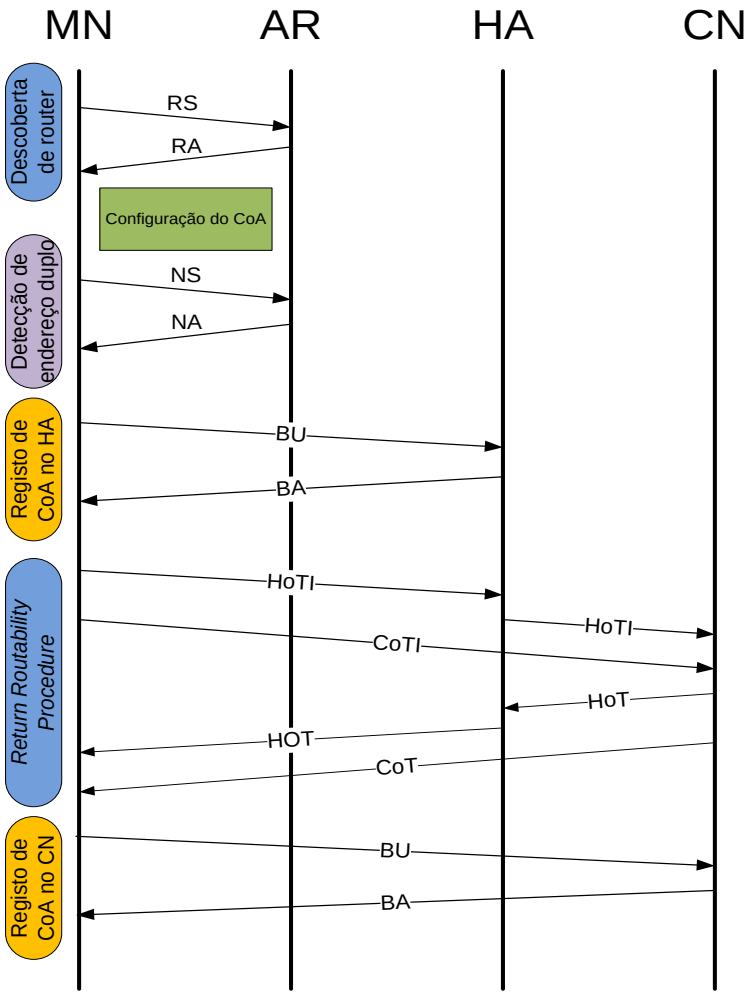

Figura 2.2.3.1-2: MIPv6 – Troca de mensagens durante processo de movimentação com optimização

O *Access Router* (AR) presente na Figura 2.2.3.1-2 representa o router da FN através do qual o MN irá obter o seu CoA.

Embora toda a explicação dada tenha sido para o caso do MN se mover da sua HN para uma FN, esta é análoga à situação de movimentação de uma FN para outra FN. Caso o MN se encontre numa FN e se desloque para a sua HN, este através do protocolo *Neighbor Discovery* detecta que se encontra na sua HN e envia um BU ao seu HA com o CoA igual ao seu HoA. O HA ao detectar que o MN se encontra na HN elimina as associações relativas ao endereço do MN da sua BC, deixando de ser proxy do endereço. A partir deste momento, todo o tráfego é efectuada normalmente utilizando o IPv6, sem que exista necessidade de se utilizar o protocolo de mobilidade.

2.2.4. FastMIPv6

Os protocolos de mobilidade mencionados até ao momento durante o processo de *handover* contêm latência e interrupção da conectividade, devido aos tempos da fase de detecção de

movimento, geração do CoA e envio do BU. Este tipo de problemas vem afectar principalmente o tráfego em tempo real.

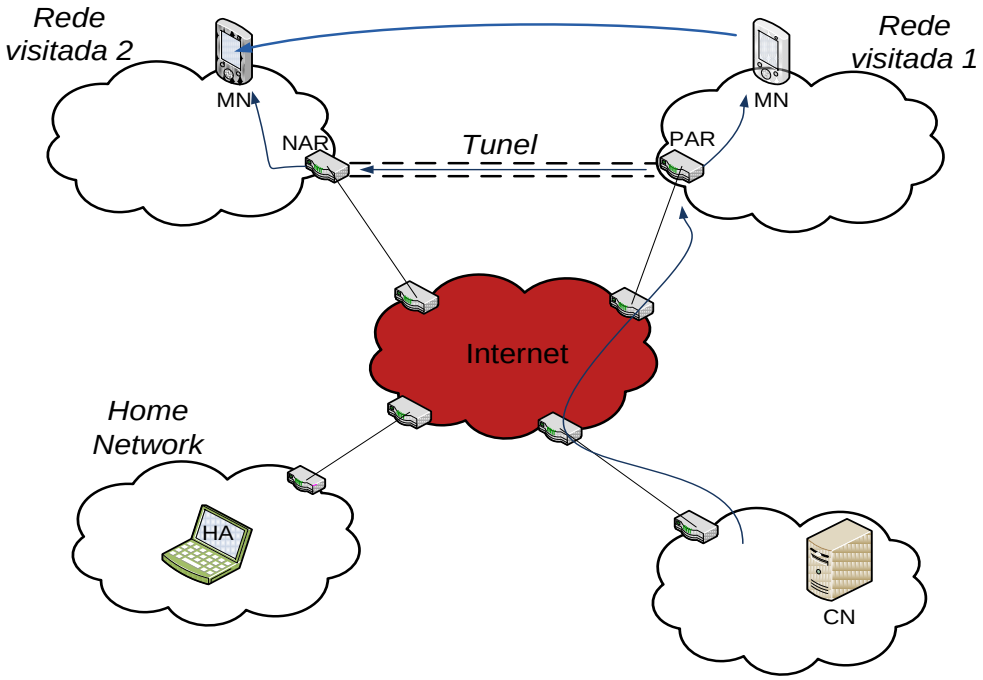

Figura 2.2.4-1: FastMIPv6 - Arquitectura

O protocolo *Fast Mobile IP version 6* (FMIPv6) é uma extensão do MIPv6 e surge com o intuito de reduzir a latência existente no processo de *handover*. Este protocolo permite que um MN detecte rapidamente quando se move para uma nova rede, onde se encontra o *New Access Router* (NAR), através do fornecimento de um novo ponto de acesso e informação relativa a este enquanto o MN ainda se encontra na rede actual, onde temos o *Previous Access Router* (PAR), ou seja, é dada a capacidade de o MN poder obter informações relativas a pontos de acesso mesmo antes de este se movimentar.

As mensagens *Router Solicitation for Proxy Advertisement* (RtSolPr) e *Proxy Router Advertisement* (PrRtAdv) são utilizadas para a detecção de movimento. Através destas mensagens o MN consegue ter informação do novo CoA enquanto se encontra no PAR, deste modo é eliminada a latência existente na descoberta do novo CoA. Para além disto, este novo endereço pode ser utilizado imediatamente após ser estabelecida a ligação com a nova rede, ou seja, após a recepção da mensagem *Fast Binding Acknowledgment* (FBA) ainda antes do MN se mover para o NAR. Caso o MN se mova sem ter recebido a mensagem FBA, este pode continuar a utilizar o novo CoA após anunciar a sua utilização através da mensagem *Fast Neighbor Advertisement* (FNA).

Para reduzir o tempo de latência do BU, este protocolo especifica um túnel entre o CoA antigo e o novo CoA; deste modo o PAR consegue enviar os pacotes para ambos os endereços e garantir que nenhum pacote é descartado, quer tenham como destino o antigo CoA ou o novo CoA. Este túnel permanecerá activo até que o processo de movimentação esteja totalmente finalizado.

Resumidamente, utilizando este protocolo é permitido:

- O MN estar ligado simultaneamente a mais de um *link*.
- Enviar pacotes simultaneamente para o antigo e novo CoA do MN.
- Obter informação relativa aos novos pontos de acesso possíveis antes de se efectuar o *handover*.

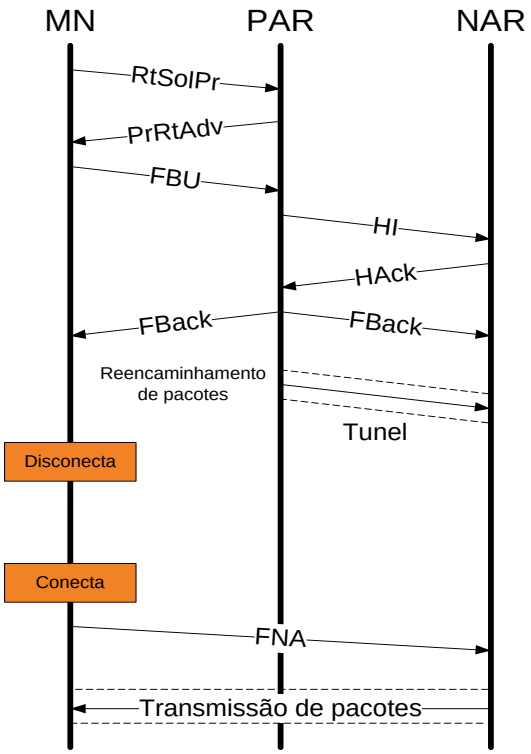

Figura 2.2.4-2: FMIPv6 – Troca de mensagens no modo preditivo

Pela Figura 2.2.4-2 podemos visualizar todo o processo para a realização do *handover*. Inicialmente, é feito um pedido por parte do MN para que este obtenha informações relativas a novos pontos de acesso utilizando a mensagem RtSolPr. Segue-se o envio da mensagem FBU com o objectivo de definir um túnel temporário entre o PAR e o NAR e seguidamente o envio da mensagem *Handover Initiate* (HI) de forma a indicar ao NAR o inicio de *handover*. Finalmente o MN assinala que já pode receber os pacotes pelo seu novo CoA através da mensagem FNA [26].

Ao modo de funcionamento que tem vindo a ser descrito e que está representado na Figura 2.2.4-1 designa-se por preditivo, este permite a realização de *handovers make-before-break*. No entanto este protocolo tem outro modo de funcionamento designado por reactivo, neste caso o *handover* realizado é do tipo *break-before-make* e o processo de construção do túnel entre o PAR e o NAR não é efectuado.

2.2.5. PMIPv6

Os protocolos referidos até ao momento requerem sempre o funcionamento do mesmo no terminal móvel e necessitam da existência de interacção entre este e os restantes elementos. O protocolo PMIPv6 surge com um novo conceito, a mobilidade baseada na rede. Este conceito torna possível o suporte de mobilidade sem que seja necessária a interacção do MN, para isso é utilizado um *proxy mobility agent* na rede onde se encontra o MN de forma a executar toda a sinalização necessária com o HA.

As principais entidades funcionais nesta estrutura são o *Local Mobility Anchor* (LMA) e o *Mobile Access Gateway* (MAG). O LMA é responsável por manter o MN acessível e é topologicamente o ponto de âncora para o prefixo da HN do MN. Já o MAG é a entidade responsável pela gestão de mobilidade de um MN e encontra-se na ligação de acesso onde o MN se encontra "ancorado". Esta entidade permite detectar os movimentos efectuados pelo MN de e para o *link* de acesso e iniciar o registo do MN no LMA.

Do pondo de vista do MN o domínio PMIPv6 é visto como uma ligação única, a rede garante que o MN não detecta qualquer mudança no que diz respeito à camada 3, mesmo que este mude o seu ponto de ligação à rede.

Caso o MN se conecte ao domínio PMIPv6 através de múltiplas interfaces e em redes de múltiplo acesso, será atribuído um único conjunto de prefixos da HN a cada interface ligada. O MN será capaz de configurar o endereço de cada uma das suas interfaces a partir do respectivo prefixo da HN. Contudo, se o MN executar um *handover* através da movimentação da configuração do endereço de uma interface para outra e caso o LMA receba uma mensagem a indicar esse *handover*, vinda do MAG, o LMA irá atribuir o mesmo prefixo de HN que já tinha sido previamente configurado. O MN também poderá efectuar um *handover* através da mudança de pontos de acesso, de um MAG para outro MAG, usando a mesma interface e mantendo a mesma configuração [27].

Através da Figura 2.2.5-1 pode-se visualizar o processo de sinalização após um MN entrar num domínio PMIPv6. A mensagem *Router Solicitation* (RS) enviada pelo MN pode ser enviada a qualquer momento após o MN se ligar, não tendo qualquer tipo de ligação com as outras mensagens. Após o MAG detectar que existe uma nova ligação a um MN este irá actualizar o LMA relativamente à posição actual do MN enviando a mensagem *Proxy Binding Update*. O LMA ao aceitar esta mensagem responde com um *Proxy Binding Acknowledgement* (PBA) incluindo o prefixo da HN do MN. Neste ponto é também criada uma entrada na *Binding Cache* e estabelecido o ponto de extremidade do túnel com o MAG. O MAG ao receber a mensagem PBA estabelece o outro ponto de extremidade do túnel para o LMA e "activa" o envio de tráfego para o MN. Após todos estes passos o MAG contém todas as informações necessárias para que possa emular o *home link* do MN e envia a mensagem *Router Advertisement* (RA) ao MN pelo *link* de acesso anunciando o prefixo da HN do MN. O MN ao receber esta mensagem pelo seu *link* de acesso tenta configurar a sua interface usando o método *stateful* ou *stateless*.

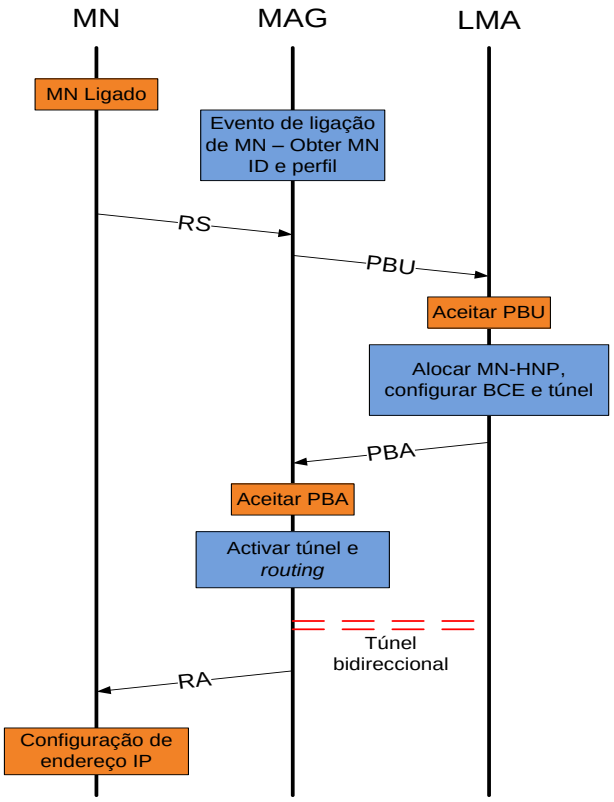

Figura 2.2.5-1: PMIPv6 – Ligação do MN

Sempre que um CN pretender enviar pacotes ao MN, quer esteja no domínio PMIPv6 ou não, estes são enviados para o LMA, por sua vez o LMA reencaminha-os para o MAG através do túnel e o MAG ao receber estes pacotes remove o seu cabeçalho exterior e envia-os ao MN. Para o caso do MN pretender comunicar com algum CN o processo é efectuado de modo inverso.

Para o caso do MN efectuar um *handover* de um MAG para outro MAG, é dada informação a partir do MAG antigo ao LMA relativamente a este evento, efectuando de seguida todo o processo apresentado na Figura 2.2.5-1 para o caso no novo MAG.

2.2.6. DSMIPv6

O protocolo *Dual Stack Mobile IPv6* (DSMIP) trata-se de uma extensão do MIPv6. Embora o MIPv6 permita a mobilidade de terminais entre diversas redes, permitindo que estes estejam sempre acessíveis, tem-se de ter em consideração que nem todos os terminais móveis utilizam este tipo de endereçamento, sendo que nos dias de hoje o IPv4 ainda continua a ser o mais utilizado. Deste modo o DSMIP surge com o intuito de suportar ambos os tipos de endereçamento, IPv4 (privado ou publico) e IPv6, estendendo as capacidades do MIPv6 para que este permita tanto MNs como HAs *dual stack*, através da utilização de túneis e CoA que tanto podem ser baseados em IPv4 como IPv6.

Embora o DSMIP suporte ambos os protocolos de endereçamento, este apenas utiliza a sinalização do MIPv6 para que não seja necessário a utilização de dois protocolos de mobilidade em simultâneo. Neste caso, a optimização de rota apenas é suportada no caso do endereçamento IPv6.

Este protocolo toma em conta cinco tipos de cenários:

FN utiliza apenas IPv4

Neste caso o MN conecta-se a uma rede que apenas contém endereçamento IPv4, podendo deste modo apenas configurar o seu CoA em IPv4.

O registo do CoA é feito através do envio da mensagem BU (MIPv6) através da utilização de um túnel para o endereço IPv4 do HA. O HA ao receber o BU acrescenta duas entradas na sua BC, uma para o HoA IPv6 e outra para o HoA IPv4 de forma a fazer corresponder o novo CoA.

Todos os pacotes enviados para o HoA do MN serão encapsulados num túnel IPv4.

MN encontra-se atrás de um NAT

Neste cenário o MN encontra-se numa FN com endereçamento IPv4 privado atrás de um dispositivo NAT. Caso o HA se encontre do outro lado do dispositivo NAT o MN necessitará de um mecanismo de NAT transversal para que possa comunicar com o seu HA.

HA encontra-se atrás de um NAT

Nesta situação o processo de comunicação entre o MN e o seu HA torna-se ainda mais complicada. Neste tipo de cenário é assumido que o HA adquire um endereço IPv4 global e único. Este endereço não pode ser configurado fisicamente na interface do HA, sendo então associado ao dispositivo NAT.

Utilização de aplicações que usem apenas IPv4

Neste caso o MN pode-se encontrar numa rede IPv4, IPv6 ou que utilize ambos os protocolos, contudo o MN necessita de comunicar apenas com IPv4, para isso o MN precisa de obter um endereço IPv4.

MN encontra-se numa rede que permite ambos os protocolos de endereçamento

Neste cenário o MN terá preferência por utilizar um CoA IPv6, quer o seu HoA seja IPv4 ou IPv6, necessitando da utilização de túneis [28].

2.3. IEEE 802.21

Com o número elevado de tecnologias que permitem o acesso à internet, especialmente as tecnologias sem fios como o Wi-Fi, WiMAX e 3G, e sendo possível a mobilidade dos utilizadores nestas mesmas redes através do uso de protocolos de mobilidade, surge a necessidade do aparecimento de meios e mecanismos de apoio à abstracção do tipo de tecnologia para as camadas superiores. Esta abstracção é efectuada desde a camada de rede até à camada de aplicação, onde normalmente são tomadas decisões relativamente ao processo de mobilidade,

controlo de admissão e balanceamento de carga. Este é objectivo da arquitectura IEEE 802.21 [29]. Para além deste objectivo, o IEEE 802.21 pretende ainda:

- Proporcionar continuidade de serviço.
- Permitir que as aplicações intervenham no processo de *handover.*
- Permitir *handovers* baseados em critérios de Qualidade de Serviço (QoS).
- Providenciar ao utilizador informação relativa às células candidatas para o *handover.*
- Fornecer assistência no processo de decisão de *handover.*
- Providenciar alguns mecanismos para gestão de energia.

O IEEE 802.21 surge com o intuito de responder a todas as necessidades apresentadas para que seja possível optimizar o processo de mobilidade, fornecendo informações, à entidade responsável pela gestão da mobilidade, relativas à camada de ligação e às camadas superiores. Deste modo é permitida a realização de s*eamless handovers* quer seja entre tecnologias iguais ou diferentes.

Este protocolo enquadra-se na fase de iniciação e preparação de *handover*, tal como mostra a Figura 2.3-1.

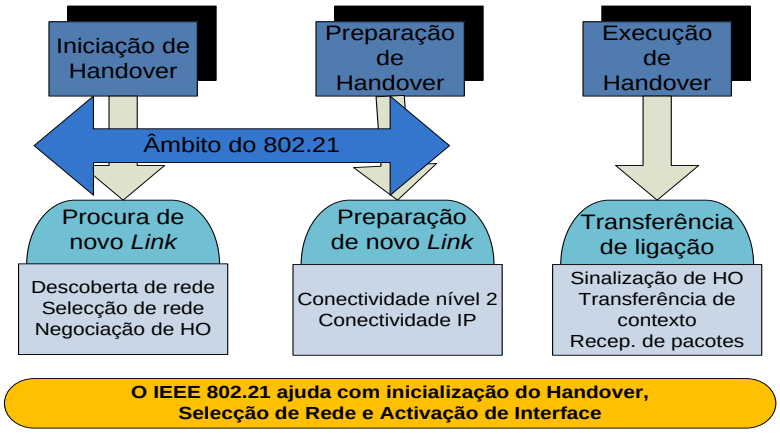

Figura 2.3-1: IEEE 802.21 – Âmbito

A iniciação do processo de *handover* pode ocorrer por diversos motivos. Caso o utilizador seja móvel, este pode ser causado por mudanças das condições da rede sem fios, como a perda do sinal, a existência de redes aglomeradas ou mesmo a detecção de uma rede com melhores características. Se por outro lado se tratar de um utilizador estacionário, o inicio do *handover* pode ser causado por mudanças da rede onde se encontra o utilizador ou por mudanças das necessidades deste, o que pode acontecer, por exemplo, para o caso de um utilizador necessitar de uma maior taxa de dados.

Para que seja possível a realização de um seamless *handover*, ou seja, efectuar uma mudança de rede sem existir quebra de ligação, torna-se fundamental que se consiga estabelecer uma

ligação com o novo ponto de acesso do terminal móvel antes de este perder a sua antiga ligação. Esta necessidade é tratada pelo IEEE 802.21, aquando a realização da fase de preparação.

Podendo existir várias tecnologias no ambiente onde se encontra o terminal móvel, para que seja possível a realização do *handover* de forma optimizada, o protocolo IEEE 802.21 toma em conta a interacção existente entre o terminal móvel e a rede. Deste modo a rede destino para a qual será efectuado o *handover* é seleccionada tendo em conta os seguintes aspectos:

- Redes existentes ao alcance do terminal móvel.
- Qualidade do sinal de cada rede.
- Diferença de sincronização de tempos.
- Máxima taxa de transferência.
- Capacidades das camadas superiores.

2.3.1. Arquitectura

O núcleo do IEEE 802.21 encontra-se no *Media Independent Handover Function* (MIHF). Este consiste nas funcionalidades intermédias que se encontram entre a camada de ligação e a camada de rede.

As redes MIH são compostas pelas seguintes entidades:

- *Point of Attachment* (PoA) – ponto que permite ao MN conectar-se à rede de acesso.
- *Point of Service* (PoS) – ponto de comunicação existente no MIH entre o MN e o operador da rede.
- *Non-Point of Service* (Non-PoS) – ponto de comunicação do MIH com o PoS. Esta entidade não permite a troca de mensagens com o MN.

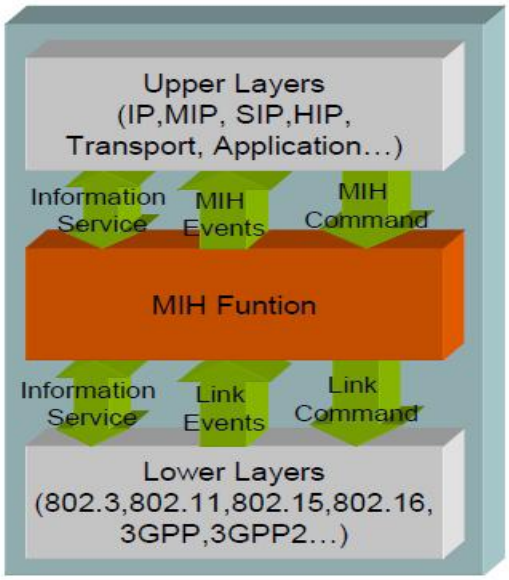

Figura 2.3.1-1: MIHF *Framework* [30]

Do ponto de vista do MIHF, Figura 2.3.1-1, este apenas recebe *Link Events* provenientes das camadas inferiores, que serão seguidamente reencaminhados para as camadas superiores como MIH Events. Para o caso de se tratar de MIH *Commands* estes terão sempre como origem as camadas superiores e o MIHF reencaminha-os para as camadas inferiores como *Link Commands*. Relativamente ao *Information Service*, este já poderá ter como origem tanto as camadas superiores como inferiores.

O MIHF fornece três tipos de serviços, nomeadamente o *Media Independent Event Service* (MIES), o *Media Independent Command Service* (MICS) e o *Media Independent Information Service* (MIIS).

- MIES – fornece eventos capazes de reportar mudanças dinâmicas nas condições de ligação, estado da ligação, qualidade de ligação, etc. Estes eventos são baseados na subscrição e notificação de processos para a camada superior, sendo que podem ser obtidos localmente ou remotamente. No caso de serem remotos estes são obtidos através de uma outra entidade MIHF. Os eventos mais comuns que são efectuados por esta entidade são:

    - *Link up.*
    - *Link down.*
    - *Link parameters change.*
    - *Link going down.*
    - *Layer 2 handoff imminet.*

    É através desta entidade que se torna possível a detecção de necessidades de *handover* [31].

- MICS – este serviço permite fornecer ao *Media Independent Handover Users* (MIHUs), localizados na camada superior, a capacidade de gerirem e controlarem os parâmetros relacionados tanto com a ligação como com o *handover*. Estes comandos, tal como já acontece para o MIES, podem ser locais ou remotos, Figura 2.3.1-2 [32].

- MIIS – este serviço tem a capacidade de fornecer informações aos MIHUs relativamente às características e serviços suportados pelas redes de serviço. Para além disto possibilita fornecer informação sobre outras redes disponíveis que se encontram ao alcance do terminal móvel. Este tipo de informação poderá ser utilizada para auxiliar a tomada de decisão sobre a escolha da rede alvo para a qual se efectuará o *handover*. Através deste serviço é também possível fornecer à camada de ligação informações relativas ao estado de execução de comandos efectuados pelas camadas superiores. A informação gerada por este serviço pode ser estática ou dinâmica [33].

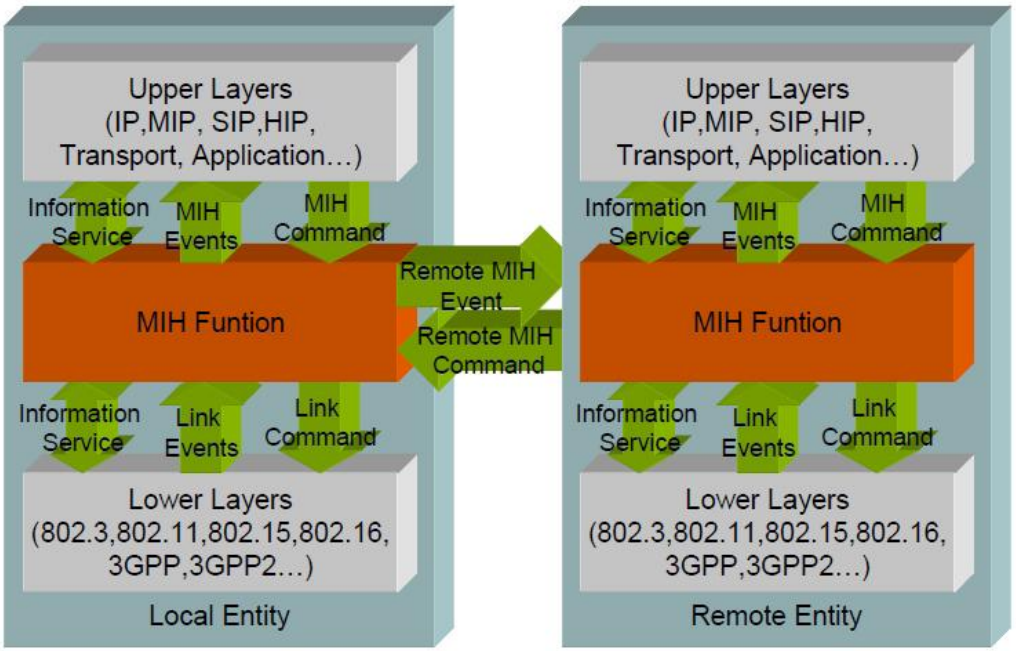

Figura 2.3.1-2: Interacção com outra entidade MIHF [30]

2.3.2. Processos de *Handover*

Para se poder iniciar o processo de *handover* existem dois métodos, um deles permite iniciar este processo do lado da rede, e o outro do lado do terminal móvel. No que diz respeito ao IEEE 802.21, este divide o processo de *handover* em 4 fases:

- Iniciação de *Handover*.
- Preparação de *Handover.*
- Execução de *Handover.*
- Conclusão de *Handover.*

2.3.2.1. Iniciação de *Handover*

Esta primeira fase de *handover* pode ser dividida em duas sub-fases, ou seja, a fase de aquisição da topologia da rede e a fase de avaliação dos recursos de cada rede.

Através da Figura 2.3.2.1-1, Figura 2.3.2.1-2 e Figura 2.3.2.1-3 são apresentadas as trocas de mensagens existentes neste processo caso este seja iniciado pelo terminal móvel ou pela rede.

Handover Iniciado pelo Terminal:

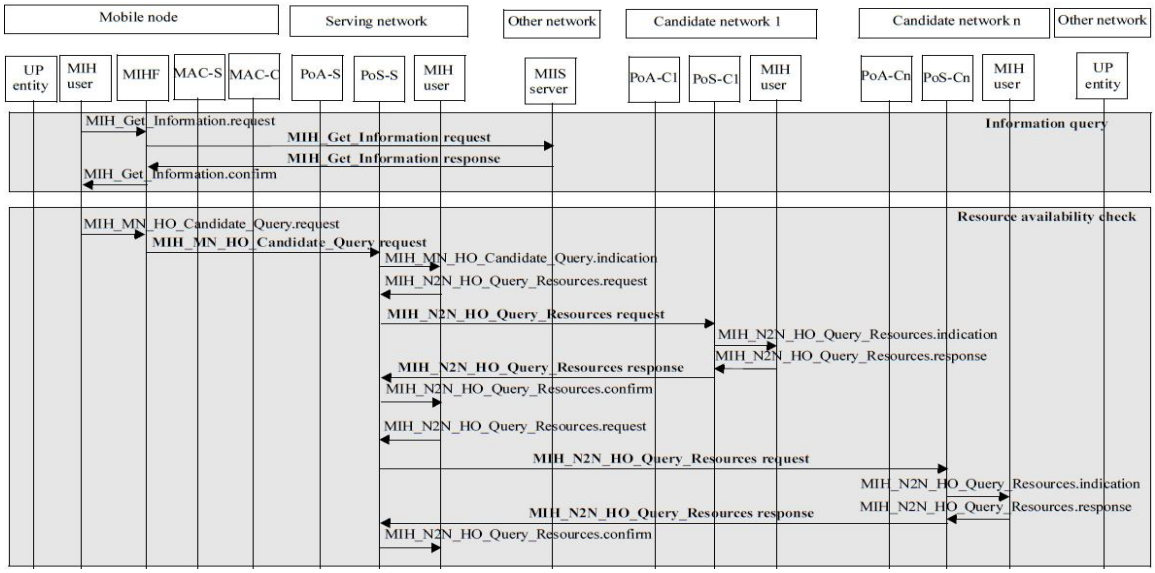

Figura 2.3.2.1-1: *Handover* iniciado pelo terminal móvel – Fase de iniciação [34]

Handover Iniciado pela Rede:

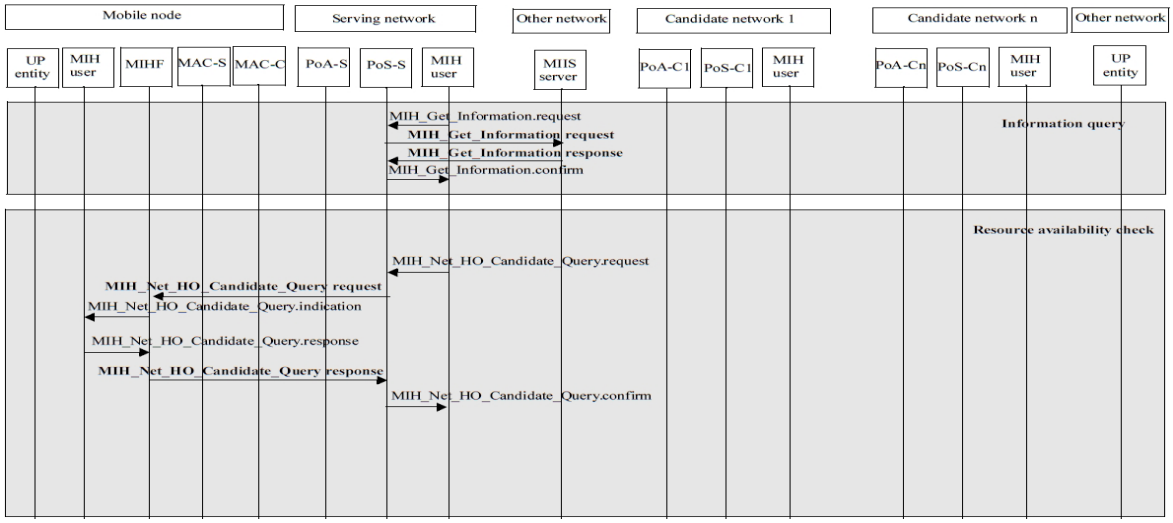

Figura 2.3.2.1-2: *Handover* iniciado pela rede – Fase de iniciação [34]

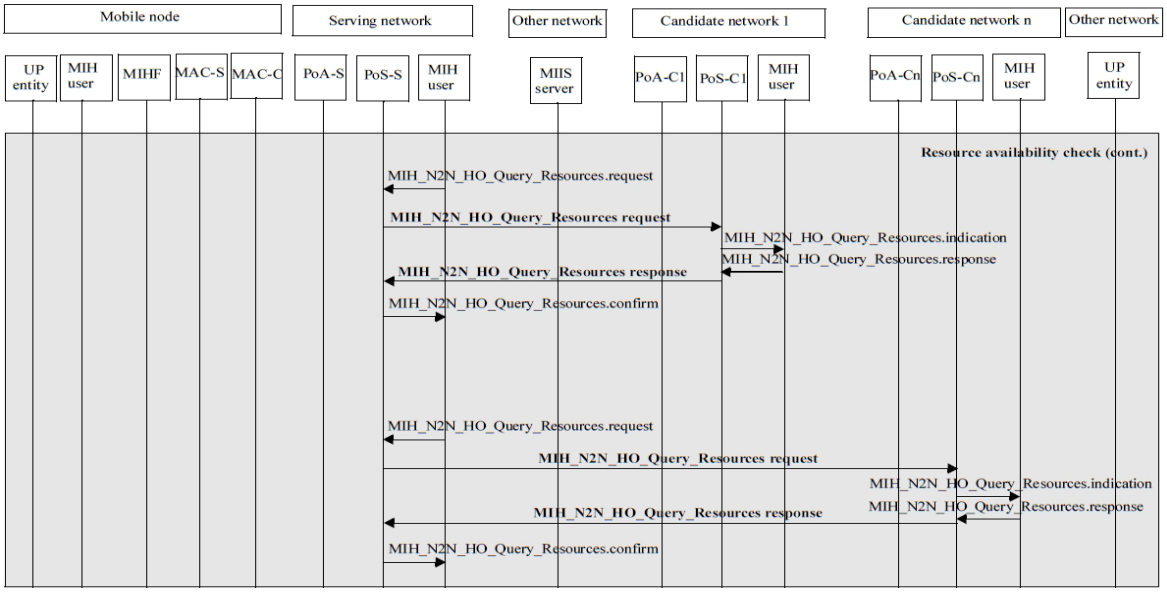

Figura 2.3.2.1-3: *Handover* iniciado pela rede – Fase de iniciação (continuação) [34]

2.3.2.2. Preparação de *Handover*

Tal como se pode observar pela Figura 2.3.2.2-1, Figura 2.3.2.2-2 e Figura 2.3.2.2-3, a fase de preparação é responsável pela reserva de recursos na rede destino do MN, ou seja, é responsável por preparar os recursos de QoS.

***Handover* Iniciado pelo Terminal:**

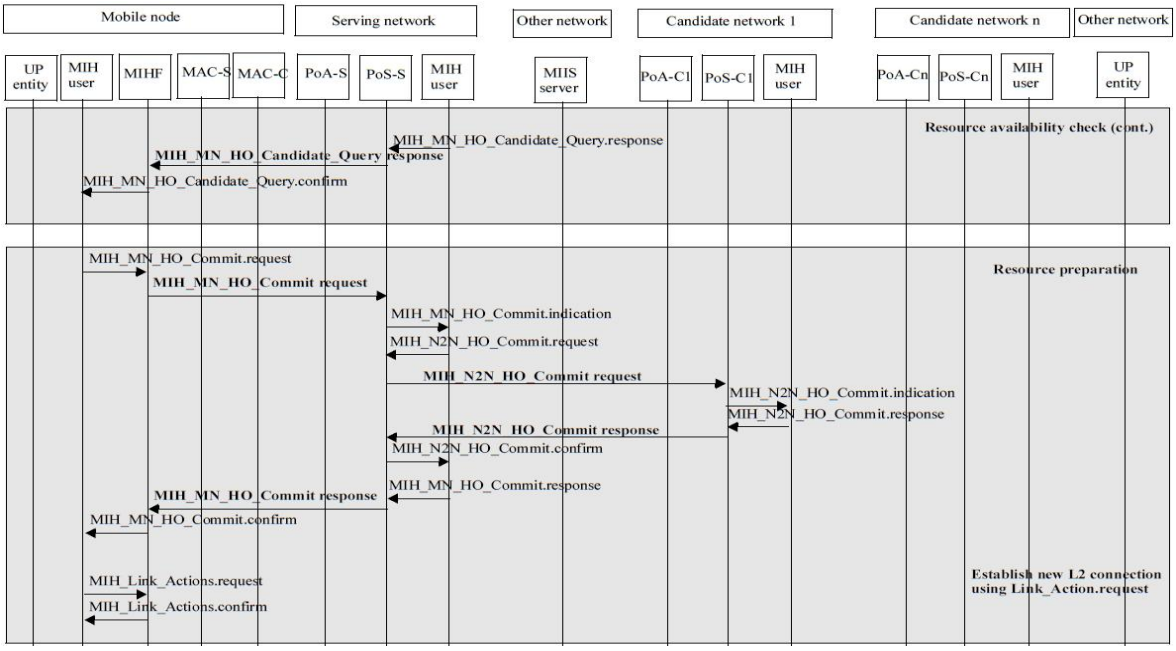

Figura 2.3.2.2-1: *Handover* iniciado pelo terminal – Fase de preparação [34]

***Handover* Iniciado pela Rede:**

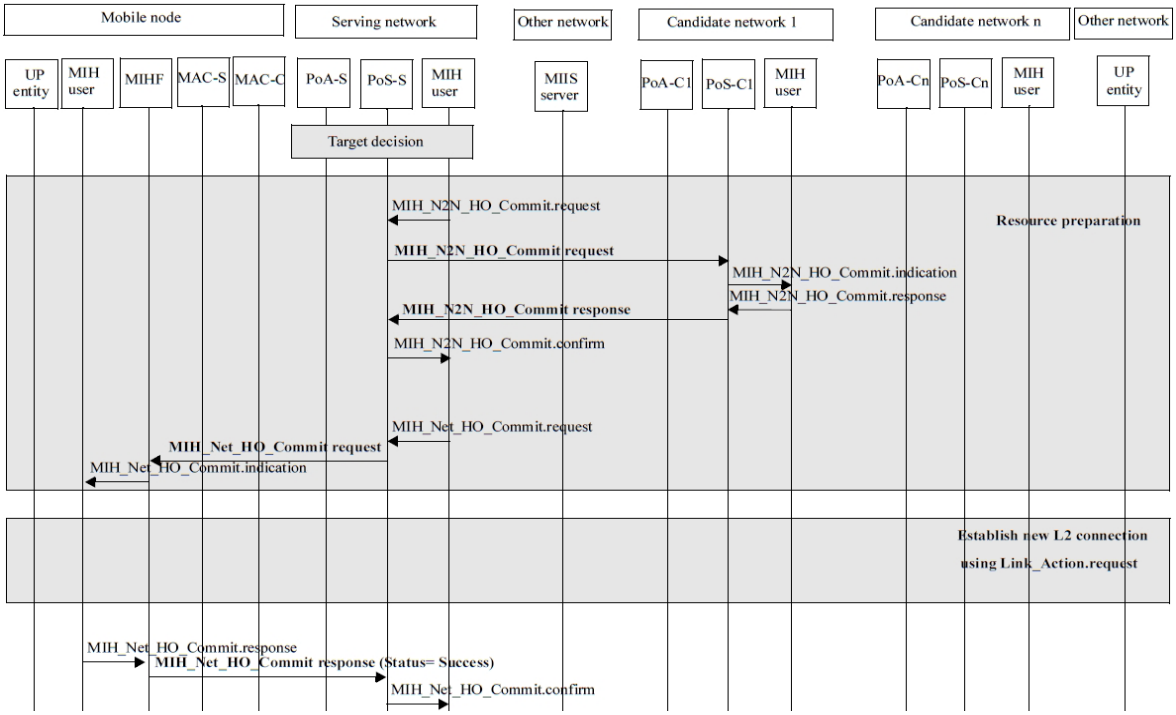

Figura 2.3.2.2-2: *Handover* iniciado pela rede – Fase de preparação [34]

2.3.2.3. Execução de *Handover*

Caso se trate de um *handover* iniciado pelo MN, esta fase é executada após a fase de preparação. Se por outro lado se tratar de um *handover* iniciado pela rede, esta fase é efectuada no final da fase de preparação.

No final desta fase o MN já se encontra ligado ao PoS da rede alvo.

2.3.2.4. Conclusão de *Handover*

Como processo final temos a fase de conclusão de *handover*, que é responsável pela libertação de todos os recursos alocados pelo MN na rede antiga.

Este processo é idêntico para ambos os casos, caso seja *handover* iniciado pelo terminal ou pela rede, tal como se pode observar pela Figura 2.3.2.4-1, Figura 2.3.2.4-2 e Figura 2.3.2.4-3.

Handover Iniciado pelo Terminal:

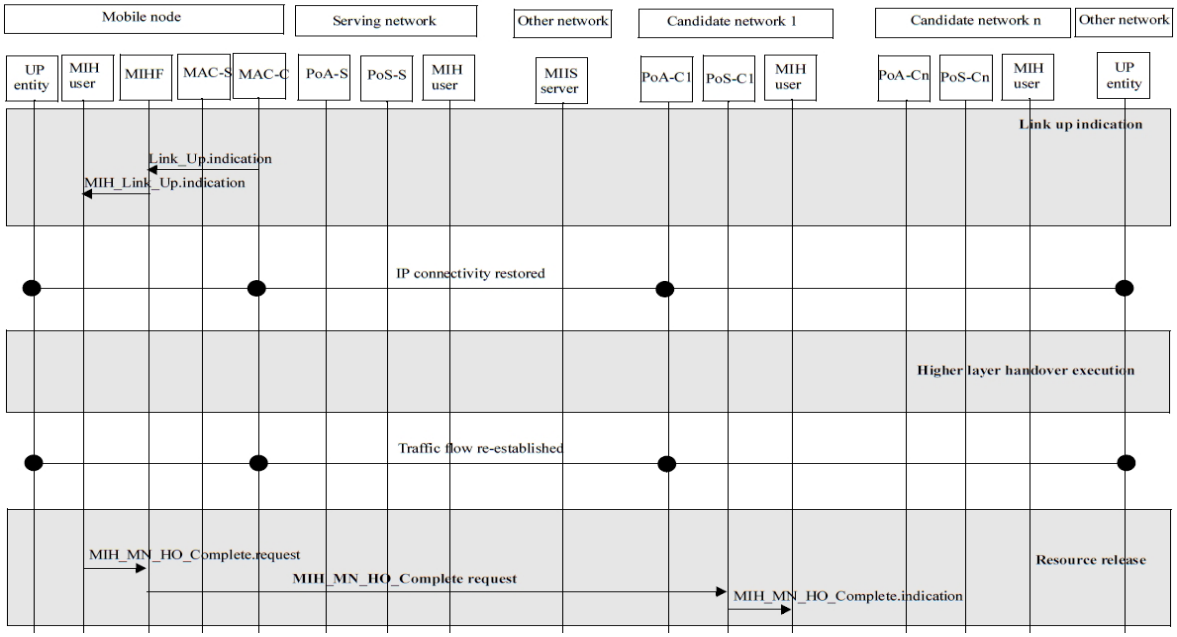

Figura 2.3.2.4-1: *Handover* iniciado pelo terminal – Fase de conclusão [34]

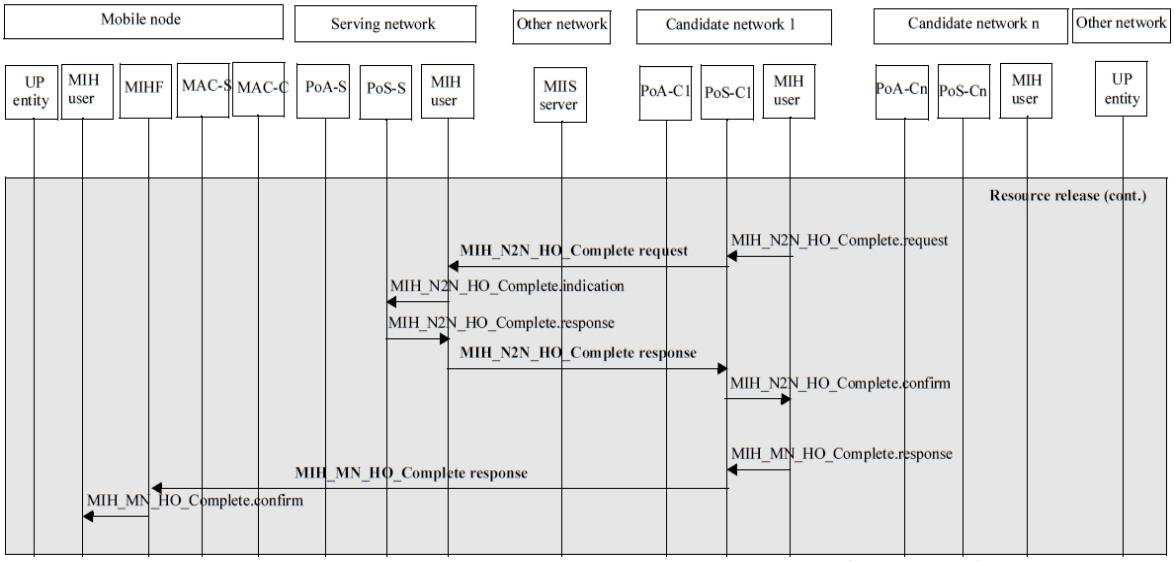

Figura 2.3.2.4-2: *Handover* iniciado pelo terminal – Fase de conclusão (continuação) [34]

***Handover* Iniciado pela Rede:**

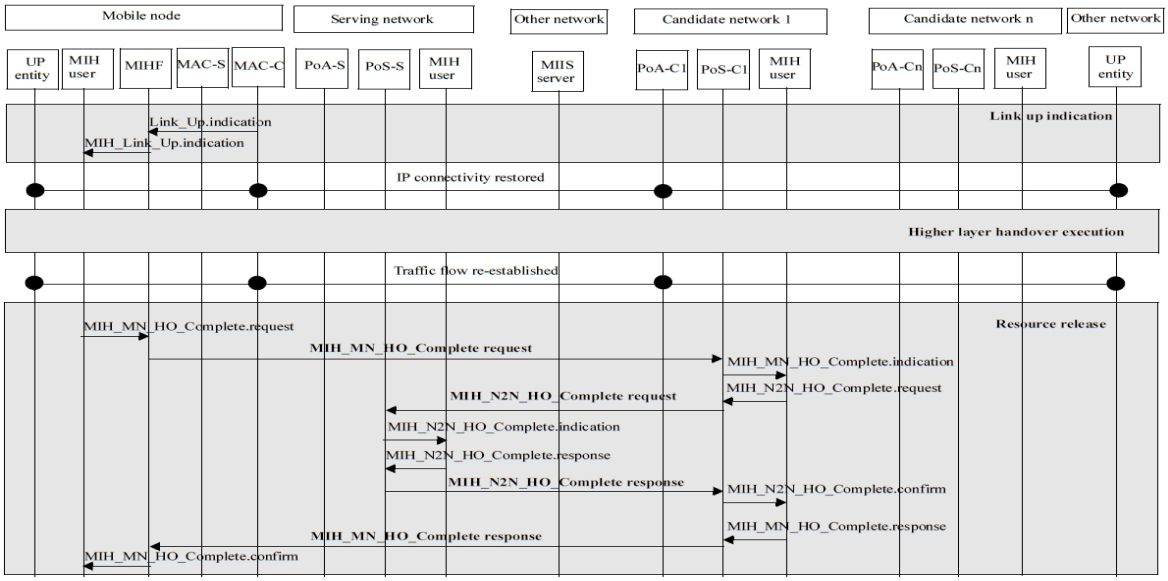

Figura 2.3.2.4-3: *Handover* iniciado pela rede – Fase de conclusão [34]

2.4. Resumo

Neste capítulo foi efectuado um estudo referente às tecnologias sem fios da actualidade, relativo ao Wi-Fi, WiMAX e principais tecnologias desenvolvidas pelo 3GPP, bem como a sua evolução ao longo dos anos.

Seguidamente foi efectuado um estudo aos principais protocolos e arquitecturas de mobilidade, de forma a apresentar os seus princípios de funcionamento e as situações a que cada um se adequa melhor. Deste modo torna-se possível apresentar e tomar conhecimento das alterações necessárias para que seja possível o suporte de mobilidade nos terminais.

Tendo sempre em vista o processo de *handover* e de mobilidade foi também apresentado o protocolo (e arquitectura) IEEE 802.21 de forma a optimizar todo este processo, referindo as suas principais entidades bem como o seu modo de funcionamento, podendo distinguir cada fase que este utiliza para poder optimizar o processo de *handover*.

3. *Handover* Optimizado entre Redes Heterogéneas

Com a evolução crescente das telecomunicações, mais especificamente das redes móveis, começaram a surgir vários tipos de tecnologias que permitem ao utilizador estar ligado à Internet em qualquer lugar.

Existindo um elevado número de tecnologias e sabendo que é impossível fisicamente uma determinada tecnologia abranger toda a área pretendida, torna-se necessário que os utilizadores se possam mover entre as diferentes tecnologias sem ocorrer quebra de ligação e de modo transparente. Para que este processo se torne possível é necessária a interacção entre dois protocolos, o protocolo de mobilidade e o protocolo de optimização de mobilidade.

Toda esta evolução a nível das tecnologias e das redes móveis é acompanhada pelo igual crescimento do número de utilizadores. Deste modo, e sabendo todas as limitações existentes a nível de endereçamento IPv4, devido à escassez do espaço de endereçamento, foi optado por efectuar todo este estudo, dentro do possível, utilizando endereçamento IPv6. Este contém um espaço de endereçamento muito maior e a sua "adopção", de um modo global, por parte das várias empresas prende-se numa questão de tempo.

Através deste capítulo é demonstrado todo o modo de funcionamento tanto da implementação do protocolo de mobilidade como da implementação do protocolo de optimização de mobilidade, sendo estes apresentados sem qualquer tipo de modificações para que se possa identificar as principais características necessárias a modificar bem como o tipo de interacções existentes.

Na secção 3.1 é apresentada e analisada a arquitectura geral implementada, explicando as funcionalidades de cada entidade. Seguidamente, na secção 3.2 e secção 3.3, é efectuada uma análise às principais entidades existentes, apresentando algumas das suas características a nível de funcionamento interno de forma a identificar e realçar as modificações necessárias. Através da secção 3.4 é apresentado um conjunto de métricas para que se possa quantificar todo o processo de *handover*. Por fim, na secção 3.5 é apresentado um resumo relativo ao capítulo.

3.1. Arquitectura Geral

Através da Figura 3.1-1 é apresentada uma visão geral da arquitectura implementada para que se possa realizar todo o processo de mobilidade de forma optimizada após a integração das modificações indicadas no capítulo 4.

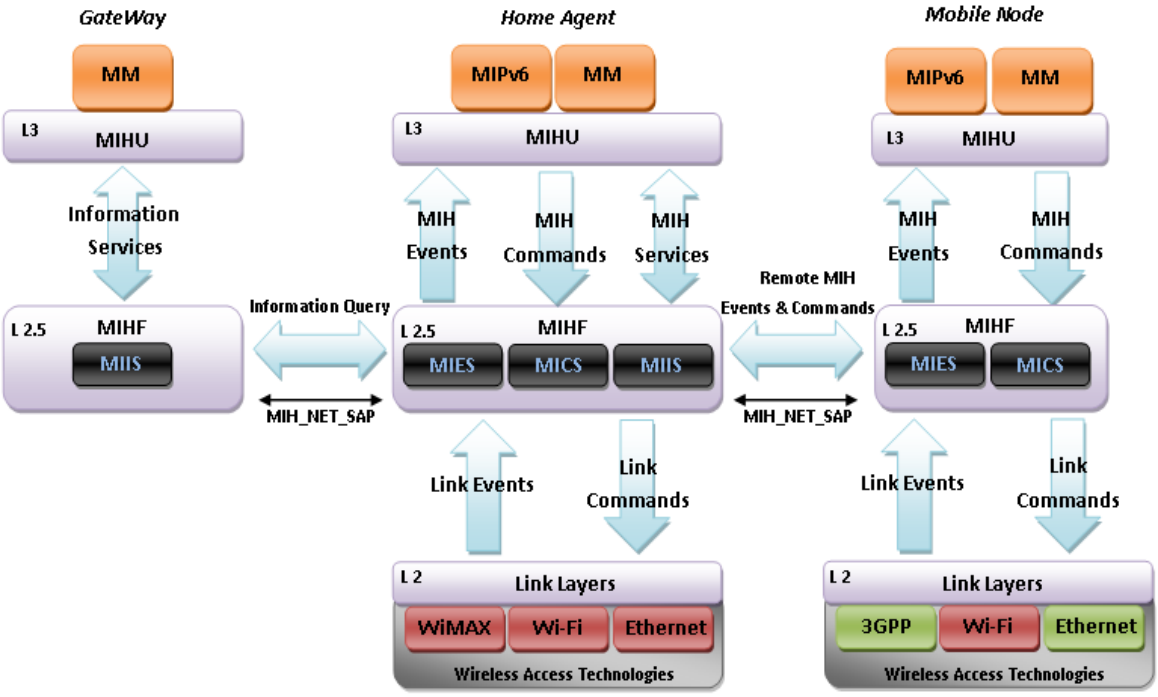

Figura 3.1-1: Arquitectura geral

Como se pode observar através da Figura 3.1-1, o IEEE 802.21 *Media Independent Handover* (MIH) é aplicado em três entidades distintas, no MN, no HA e no *GateWay* (GW). Esta arquitectura tem como finalidade controlar o *handover* do lado da rede, estando deste modo o MN liberto da decisão de execução do *handover*.

Como entidade principal temos o *Mobility Manager* presente no HA que representa um MIHU. Neste é efectuado todo o processo de decisão e controlo. É através desta entidade que são tomadas todas as decisões a nível de execução de *handover*, reservas de recursos, obtenção de informação relativa às interfaces, controlo de interfaces, entre outros.

Relativamente ao GW, este funciona como um *Information Server* contendo informações relativas às redes que se encontram na área geográfica do MN. Sempre que for necessário efectuar um *handover*, este tipo de informação é requisitada pelo MM presente no HA, para que este possa optar pela rede mais adequada.

Através do MN são obtidas todas as informações relativas ao estado actual das interfaces bem como informações sobre a realização efectiva do *handover,* tanto a nível da camada de ligação como da camada de rede. Esta entidade contém algumas limitações no que diz respeito às tecnologias de acesso. Uma vez que o MN foi implementado em dois tipos de dispositivos, num portátil e num telemóvel, no caso do portátil temos suporte da rede Ethernet e não da rede 3G, e no caso do telemóvel temos a situação inversa.

A necessidade de se proceder à realização de um *handover* pode ocorrer em duas situações distintas. Caso se esteja perante uma tecnologia sem fios, o MN irá analisar periodicamente a força do sinal da rede em que se encontra através da recepção de *beacons;* caso este se encontre

abaixo de um limite pré-definido é fornecida essa informação ao MM presente no HA. Se por outro lado estivermos perante uma tecnologia com fios, o processo de *handover* será iniciado caso o MN indique que necessita de melhor qualidade de serviço, e caso a rede onde se encontre não consiga satisfazer esse pedido.

3.2. Implementação do protocolo de mobilidade: UMIP

O USAGI-patched Mobile IPv6 for Linux (UMIP) [35] trata-se de uma implementação *open-source* do protocolo de mobilidade em IPv6, ou seja, trata-se de uma implementação do protocolo MIPv6 para sistemas operativos GNU/Linux. O UMIP é baseado no MIPL2 [35], sendo este uma implementação mais antiga, e surge como uma actualização a este, correndo nos *kernels* mais recentes.

A versão utilizada para implementar o protocolo de mobilidade foi a 0.4 (*mipv6-deamon-umip-0.4*).

3.2.1. Funcionamento Interno: Mobilidade e Gestão de interfaces

Com o intuito de se conseguir controlar todo o processo de *handover*, no que diz respeito ao início da sua execução, bem como a interface para o qual é executado, torna-se necessário efectuar um estudo relativamente ao processo de controlo, da gestão das interfaces e ao modo como *o handover* é iniciado.

Esta análise será efectuada apenas para o UMIP implementado no MN, pois é através deste que se pretende ter todo o controlo neste processo, embora o *handover* possa ser iniciado através de entidades externas.

Existem dois pontos cruciais que se devem ter em conta: um deles está relacionado com a detecção de movimento por parte do MN e o outro com o modo como o MN avalia cada uma das redes que tem disponível.

As redes disponíveis dependem muito do suporte a nível de *hardware* do MN, pois este apenas consegue efectuar *handover* entre diferentes interfaces. Sendo assim, caso tenhamos as tecnologias Wi-Fi, WiMAX e 3G, sendo todas tecnologias sem fios, seria necessário que o MN possuísse três placas de rede, uma para cada tecnologia, tornando deste modo possível o *handover* entre as diferentes tecnologias, mais propriamente, entre as três interfaces existentes no MN.

3.2.1.1. Detecção de Movimento

Um dos pontos mais críticos na mobilidade prende-se com a capacidade de detecção de movimento. Para este processo é utilizado pelo MN o protocolo *IPv6 Neighbor Discovery* [36], mais propriamente a mensagem *Neighbor Unreachability Detection*, que permite ao MN detectar quando um determinado router se encontra ao seu "alcance". A informação relativa aos routers presentes na rede é dada através das mensagens *Router Advertisement* (RA). Estas mensagens são enviadas periodicamente e contêm um conjunto vasto de informação, tendo como principais as que se seguem:

- Permite indicar ao MN se o RA foi enviado pelo seu HA, dando a possibilidade de MN detectar quando se encontra na sua HN ou ao alcance desta.

- Possibilita indicar o endereço global do router que envia o RA, em vez de anunciar o seu endereço *Link-Local*. Esta informação é necessária aquando a criação da *Home Agent List*.

- Indica o intervalo de tempo desde o último RA enviado de forma não solicitada.

- Permite o envio de informação relativo ao seu HA.

Quando um MN recebe um RA e sabendo que este auxilia o processo de detecção de movimento, sempre que este tem como origem um novo router que contém um conjunto diferente de prefixos na ligação não significa que estamos perante uma situação de *handover (layer 3)*. Caso o MN detecte que continua com ligação ao seu *default router* este deve continuar ligado.

Deste modo, para se usar a informação presente nos RAs de forma a se detectar uma possível movimentação de um modo não ambíguo é necessário ter em consideração alguns aspectos:

- É possível existirem vários routers na mesma ligação, o que implica que detectar um novo router não constitui necessariamente um *handover (layer 3).*

- Quando existem vários routers na mesma rede, estes podem anunciar diferentes prefixos, o que não implica que se trate de um *handover (layer 3)*.

- É necessário que os routers utilizem *o Router Address (R) bit* de forma a anunciarem o seu endereço global. Caso seja usado o endereço *link-local* e sabendo que este não é único, pode acontecer o MN após a execução de um *handover (layer 3)* continuar a receber RA com o mesmo endereço *link-local* [37].

De forma a representar os processos básicos efectuados pelo UMIP após a recepção de um RA temos a Figura 3.2.1.1-1/3.2.1.1-2. Através desta podemos observar os pontos cruciais neste processo bem como dar maior ênfase à necessidade de modificações.

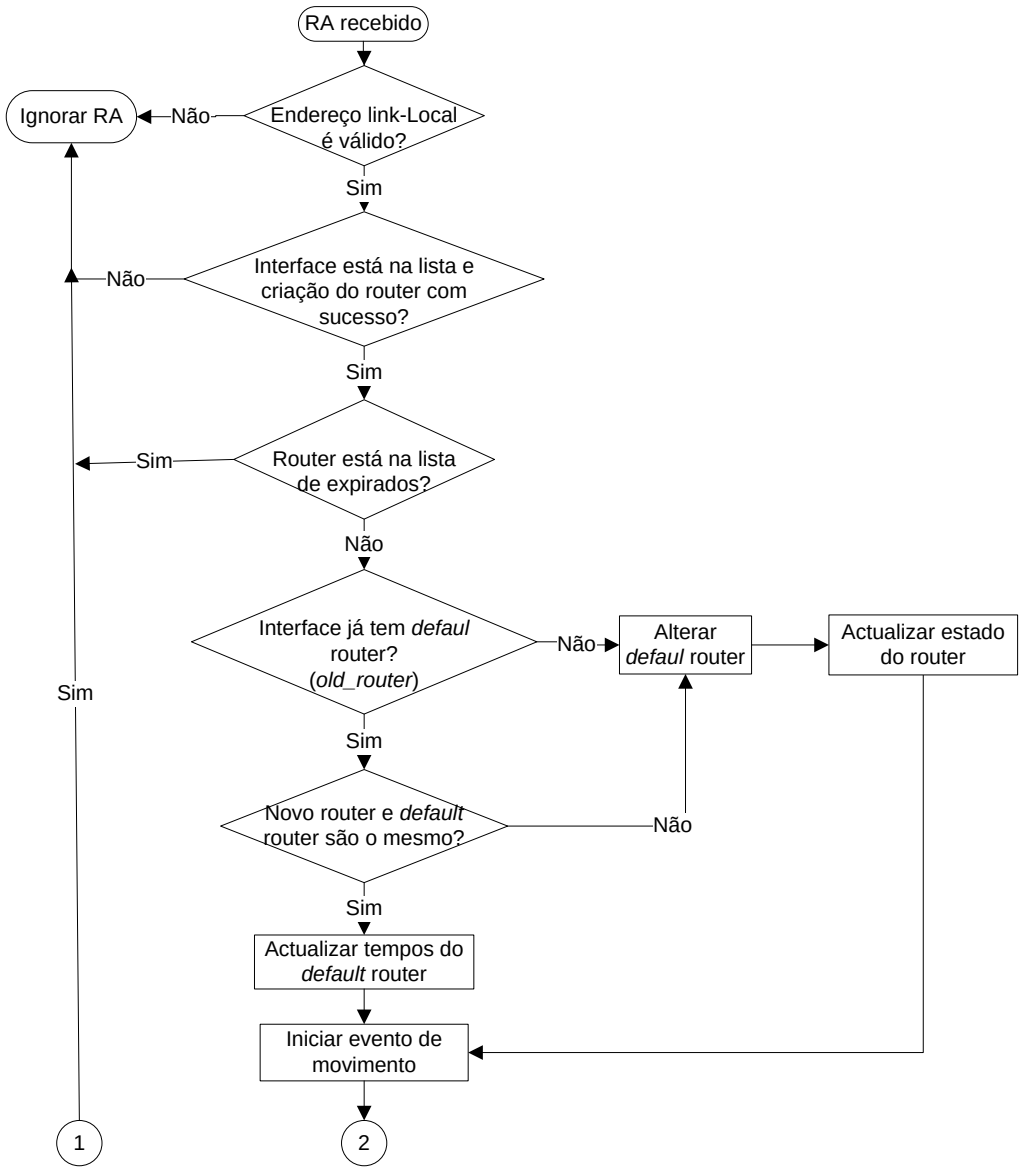

Figura 3.2.1.1-1: Representação dos processos básicos do UMIP após recepção de um RA

Inicialmente é verificado o endereço *link-local* da interface que envia o RA, caso este seja válido é obtida toda a informação disponível referente à interface que recebeu o RA, bem como o router que o enviou. Este mesmo router não pode estar contido na lista de router expirados do MN, pois poderá conter informação desactualizada. Se alguma destas verificações falhar o RA será descartado.

Segue-se uma análise ao router responsável pelo envio do RA, neste caso podem ocorrer duas situações, caso já exista um *defautl router* na interface em análise é verificado se o *defautl router* e o router em análise se tratam do mesmo. Se se tratar do mesmo router, é actualizado o estado do *defautl router*. Se pelo contrário ainda não existir um *defautl router* na interface, ou caso este seja diferente do router que enviou o RA, o "novo" router é definido como *default router*.

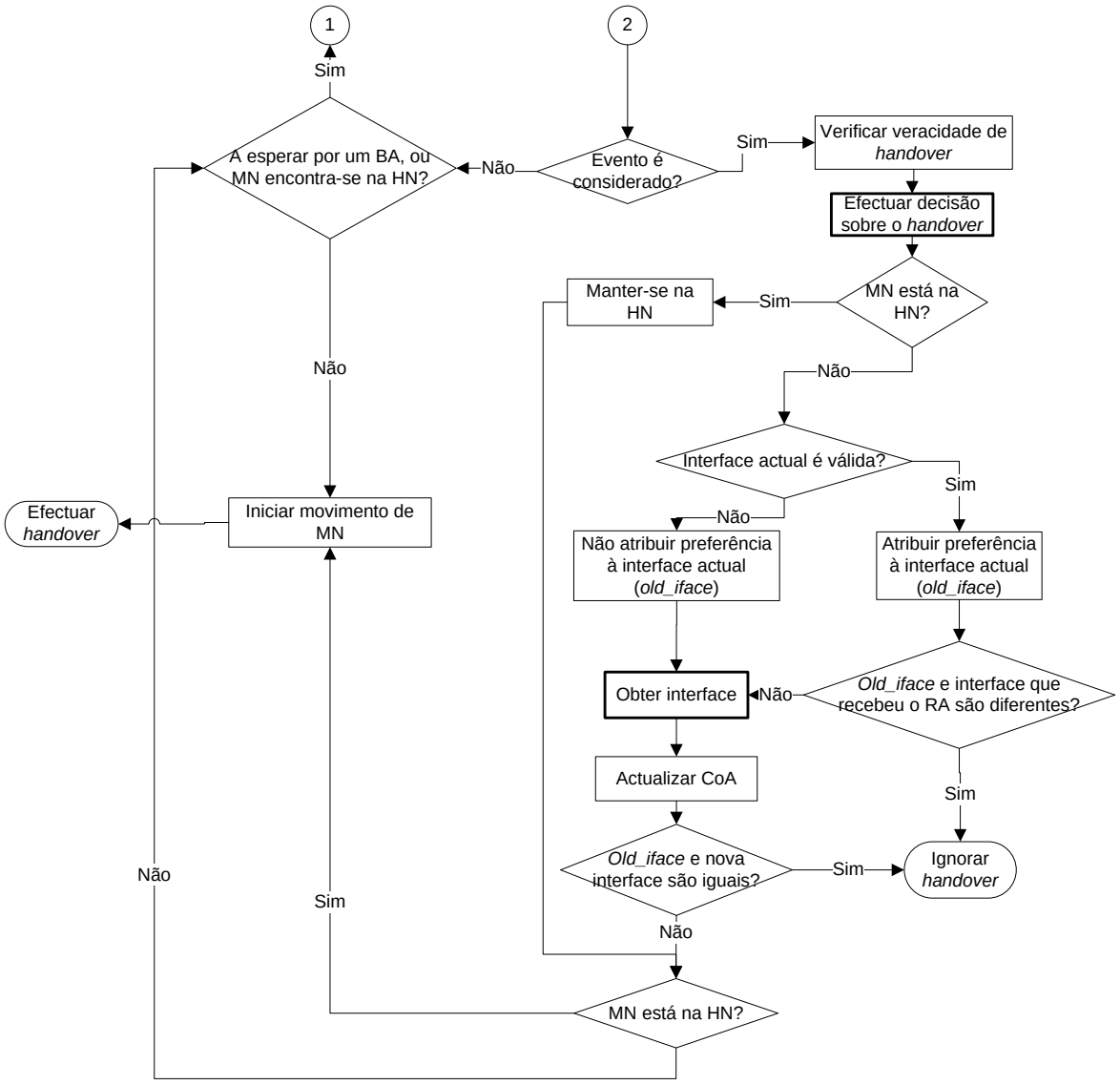

Figura 3.2.1.1-2: Representação dos processos básicos do UMIP após recepção de um RA (continuação)

A iniciação de movimento pode ser causada por diversos tipos de eventos. Caso o evento indique que o CoA expirou ou que é necessário efectuar um Dynamic Home Agent Address Discovery (DHAAD) é feita uma verificação relativamente à decisão de *handover*, se por outro lado o evento não for deste tipo, e caso o MN não esteja à espera de nenhum BA, não esteja na sua HN e tenha sido tomada uma das seguintes decisões é iniciado o processo de movimentação do MN e por consequente o seu *handover*. As decisões a considerar são:

- MN deve proceder com o *handover.*
- MN retornou à sua HN.
- Restabelecer *handover* (esta decisão é tomada sempre que se actualiza o estado do router em que se encontra o MN).

- Verificar o “tempo de vida” do CoA.

Ao efectuar a decisão sobre o *handover*, função *mn_make_ho_verdict(),* é verificado à priori a existência de ligação entre o MN e a sua HN. Caso esta exista, é retornada uma mensagem a indicar que o MN se encontra na sua HN e por consequente é nesta rede que ele se irá manter, independentemente das redes que tenha ao seu alcance e sem verificar a preferência das suas interfaces. Se por outro lado o MN não se encontrar na sua HN, é atribuída uma preferência à interface actual em que se encontra, caso esta exista. Se esta for diferente da nova interface, ou seja, a interface que recebe o RA, o *handover* será ignorado e o MN mantém-se na rede em que se encontra. Caso o MN não se encontre em nenhuma interface ou caso a nova interface seja igual à actual, é obtida uma nova interface através da função *mn_get_iface()*, verificando as interfaces existentes e tendo em conta as preferências definidas em cada interface. Após a escolha da interface é feita uma actualização do CoA e torna-se a verificar se a nova interface obtida é igual à interface actual. No caso de serem iguais, o processo de *handover* é ignorado; por outro lado, se forem diferentes é devolvida uma mensagem a indicar que o *handover* deve proceder, executando seguidamente o mesmo.

Chegando a este ponto torna-se necessário distinguir os dois tipos de preferências existentes, a preferência por uma determinada interface e a preferência de uma determinada interface, sendo esta última tomada em consideração apenas na função *mn_get_iface()*. Para o MN é possível que este tenha preferência ou pela interface em que se encontre ou pela interface que permite a ligação à sua HN, ou seja, preferência por uma determinada interface. No entanto, caso esta preferência não exista, o MN irá verificar a preferência que é definida em cada interface no campo *preference*, ou seja, preferência de uma determinada interface. Por norma esta preferência é igual para todas as interfaces existentes, não sendo o UMIP responsável pela sua alteração.

3.2.1.2. Processo de Análise das Interfaces

Como se pode verificar na secção 3.2.1.1, existem duas funções cruciais onde são tomadas decisões que influenciam a escolha da interface. Essas funções são a *mn_make_ho_verdict()* e a *mn_get_iface()*.

Através da Figura 3.2.1.2-1 pode-se observar de um modo mais pormenorizado o funcionamento da função *mn_make_ho_verdict().* Ao se invocar a função *mn_make_ho_verdict()*, esta assume de imediato uma preferência pela interface actual onde o MN se encontra. Seguidamente é verificada a existência da interface que recebeu o RA podendo ocorrer diversas situações. Caso esta exista e o MN tenha ligação com a sua HN, este irá manter-se ou deslocar-se para a HN. Se por outro lado o MN não se encontrar na HN e não tiver ligação com esta ou a interface que enviou o RA for inválida, o que acontece aquando a existência de quebra de ligação, será verificada a existência de preferência por alguma interface em concreto. Caso esta preferência exista, são obtidos os dados referentes à interface e verificado se esta é diferente da interface que recebeu o RA. Se for, o *handover* será ignorado. Se não existir preferência por

nenhuma interface, o que significa que a interface onde o MN se encontra não é válida ou já não existe, é obtida uma nova interface, através da função *mn_get_iface()*, e um novo CoA, podendo ocorrer duas situações: o CoA ser válido e a nova interface ser diferente da interface actual, o que implica a continuação do processo de *handover*, ou as condições não se verificarem e o *handover* ser ignorado.

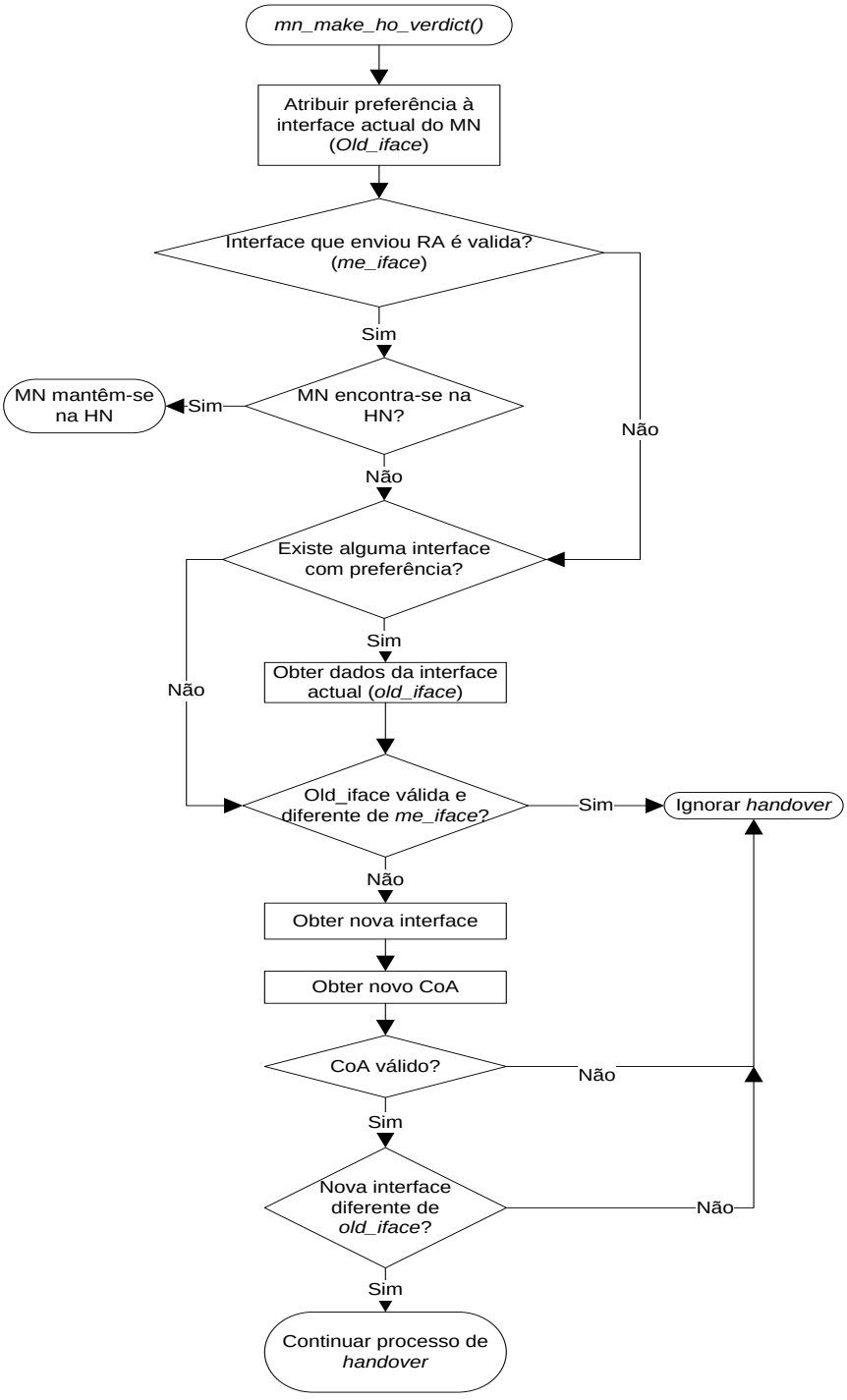

Figura 3.2.1.2-1: Diagrama da função *mn_make_ho_verdict()*

Segue-se a representação de todo o funcionamento da função *mn_get_iface()* através Figura 3.2.1.2-2.

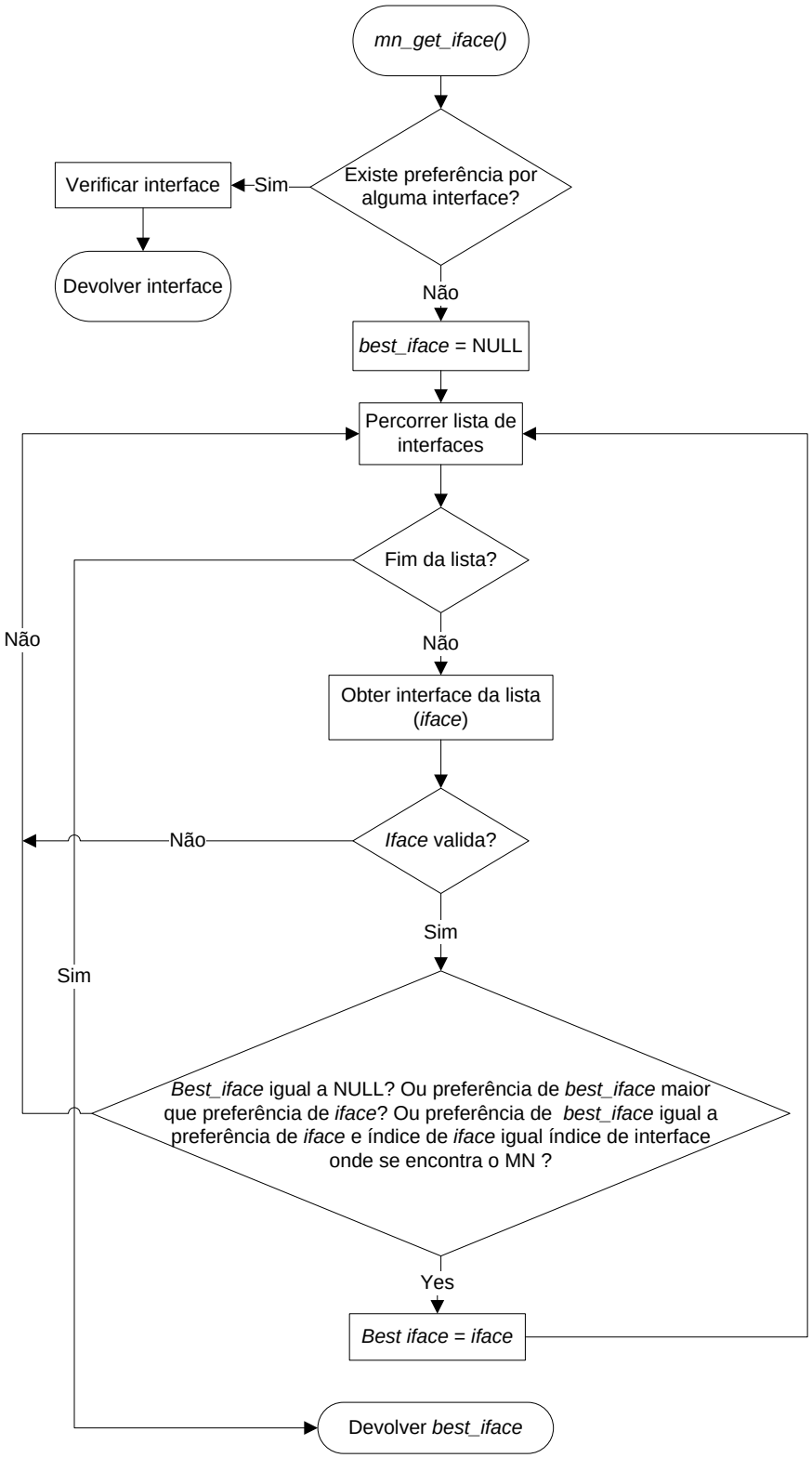

Figura 3.2.1.2-2: Diagrama da função *mn_get_iface()*

Após a invocação desta função é verificada à "cabeça" a existência de preferência por alguma interface, preferência esta que está sempre associada à interface actual onde se encontra o MN. Caso esta exista é retornada como interface escolhida. Se por outro lado não existir, é percorrida uma lista onde estão guardadas as informações relativas às interfaces do MN verificando a preferência de cada uma bem como o seu índice.

No primeiro ciclo que percorre a lista de interfaces é atribuída à variável *best_iface* (variável que será devolvida) a primeira interface da lista, dado que esta tem o valor NULL. Seguidamente, se existir alguma interface com maior preferência será essa a interface devolvida; mas se por outro lado todas as interfaces tiverem a mesma preferência é tido em conta o índice das interfaces da lista, que é comparado com o índice da interface pela qual o MN tem preferência. sendo assim, no caso em que o MN chega a este ponto, esse índice será zero, dado que não se encontra em nenhuma interface, o que significa que a interface devolvida é a primeira da lista.

3.2.2. Limitações da Implementação do Protocolo de Mobilidade

Através da secção 3.2.1 pode-se observar características fulcrais existentes no UMIP que limitam e tornam impossível o controlo do processo de *handover*.

Essas características são:

- Não permite intervir activamente na escolha da interface para efectuar o *handover*. Sendo um dos objectivos principais a interacção entre o protocolo de mobilidade e o protocolo de optimização de mobilidade, para que este último possa indicar a interface para a qual se deverá efectuar o *handover,* torna-se necessário que o UMIP consiga comunicar com o "exterior".

- Não permite a realização de *handover make-before-break* nem de *seamless handover*. Dado que a detecção de movimento é feita através da mensagem *Neighbor Unreachability Detection* e aquando a não recepção de *Routers Advertisements* da rede em que se encontra o MN, torna-se necessário existir quebra de ligação para que se inicie todos os processos necessários à realização do *handover*, com a excepção da rede HN.

- Caso o MN tenha ao seu alcance várias redes, se uma delas for a sua HN, o MN prefere estar sempre ligado a esta. Neste caso, se conseguíssemos obrigar o MN a efectuar o *handover* para outra rede, este voltaria imediatamente para a sua HN mal detectasse a sua presença.

- O MN prefere sempre a ligação em que se encontra. Mesmo que este tenha ao seu alcance várias redes, não sendo nenhuma delas a HN, este não mudará de rede enquanto tiver ligação com a rede em que se encontra.

Deste modo torna-se necessário desenvolver e efectuar as seguintes modificações:

- Desenvolver um método para que seja possível intervir activamente na escolha da interface para a qual se pretende efectuar o *handover*.

- Desenvolver um método que permita iniciar o *handover* sem que seja necessário quebrar a ligação, podendo deste modo efectuar um *handover make-before*-break ou mesmo um *seamless handover*.

- Modificar a função *mn_make_ho_verdict()* para que esta permita que apenas no iniciar do UMIP, o MN tenha preferência pela sua HN ou mesmo por outra interface. Após esta fase inicial, o MN terá de verificar, sempre que pretender iniciar o *handover* de modo forçado, a preferência definida em cada interface.

- Modificar as funções *mn_make_ho_verdict()* e *mn_ge_iface()* de forma a que sempre que se pretenda efectuar o *handover* de modo forçado, o MN não prefira a ligação em que se encontre e que vá verificar a preferência de cada interface; só no caso de todas as interfaces terem a mesma preferência, este se deve manter na ligação em que se encontra.

Devido ao facto de se tornar possível que o MN efectue o *handover* sem necessidade de quebra de ligação, ou seja, tendo deste modo ambas as interfaces activas e acessíveis, surge um problema no processo de *uplink* do MN que se prende com as tabelas de encaminhamento. Sempre que alguma entidade pretende efectuar o envio de tráfego para o MN, este segue pela interface que foi indicada ao HA como interface a ser utilizada, ou seja, a interface correcta. No entanto, caso o MN pretenda comunicar com essa mesma entidade, dado que tem as duas interfaces activas, esta comunicação será realizada por uma das suas interfaces, dependendo da tabela de encaminhamento actual do MN. No entanto, este problema não se torna num ponto crítico. Caso o MN efectue um *handover* para uma nova interface e continue a responder às entidades externas pela interface antiga, se por qualquer motivo a ligação à interface antiga se perder, o MN automaticamente passará a utilizar a nova interface.

3.3. *Media Independent Handover Function: Mobility Manager*

No âmbito desta tese foi disponibilizada uma implementação do protocolo IEEE 802.21 existente, bem como uma implementação de um MIHU ao qual nos referimos como *Mobility Manager* (MM), efectuada no âmbito de outra Dissertação complementar.

O MM representa uma entidade MIHU que permite tomar decisões sobre o processo de *handover* e tem as seguintes características:

- Suporta vários utilizadores.

- Gestão da configuração do terminal móvel.
- Gestão de recursos.
- Toma decisões relativamente ao processo de *handover* tendo em conta algumas condições, tais como a preferência de utilizadores, recursos existentes e redes existentes.

Através desta secção são apresentados todos os processos e mensagens suportadas pelo MM implementado no HA, o qual foi utilizado na implementação do protocolo IEEE 802.21 nesta mesma entidade.

3.3.1. Fases Suportadas

Uma vez que existem vários passos desde o processo de configuração das interfaces do MN até à fase de conclusão de *handover*, são seguidamente apresentadas todas essas fases bem como a descrição das mesmas.

Registo do *Mobile Node*

Inicialmente, após a activação do MIHF, é iniciado o processo de configuração por parte do MN através do envio de um pedido para o MM de forma a indicar a intenção de se registar. O MM, ao receber esta indicação, efectua um pedido ao MN com o intuito de obter informações relativas ao tipo de interfaces que o MN está a tentar registar bem como os eventos e comandos suportados por estas, para que sempre que seja gerado um evento no MN este seja reencaminhado para o MM.

De forma a finalizar este processo, o MM indica ao MN que sempre que a força do sinal da rede onde ele se encontra ultrapassar um determinado limite pré-definido este deverá avisar.

Após estas configurações torna-se possível a recepção de tráfego por parte do MN.

Iniciação e Preparação de *Handover*

Para que seja possível despoletar a fase de iniciação torna-se necessária a ocorrência de uma das duas situações mencionadas na secção 3.1. Após a detecção da necessidade de *handover* por parte do MN, esta é reportada ao MM, sendo esta a única acção na fase de iniciação.

Dada por concluída a fase de iniciação, é iniciada a fase de preparação. O MM, ao receber a indicação da necessidade de *handover*, obtêm informações relativas às redes que se encontram ao alcance do MN através do MIIS *Server*, efectuando de seguida um *scan* ao MN para que possa confirmar a veracidade das redes indicadas pelo MIIS Server.

Após a confirmação das redes existentes, o MM questiona o MN relativamente à existência de preferência por alguma rede dentro das redes existentes, ao qual o MN responde com o envio da lista de interfaces, mas ordenada por preferência. Tendo a lista das redes ordenada por

preferência, o MM irá efectuar um pedido à rede destino para que possa ter informação relativa aos recursos existentes nesta, efectuando de seguida uma reserva dos mesmos (QoS).

No que diz respeito aos pedidos de informação relativos aos recursos de cada rede, embora este processo esteja implementado, não é tomado em consideração dado que o pedido de informação relativamente aos recursos de cada rede não é suportado pelas tecnologias utilizadas.

Execução de *Handover*

Estando a fase de preparação concluída, segue-se a fase de execução. Nesta fase, o MM presente no HA, uma vez que já optou pela interface para a qual se vai efectuar o *handover*, envia essa informação ao MM presente no MN para que o *handover* seja executado. Chegando a esta fase, tanto a implementação do protocolo IEEE 802.21, como a do MM (independentemente de qual seja) não efectuará qualquer tipo de processo, uma vez que é precisamente nesta fase que se encontra a necessidade de comunicação entre o MM presente no MN e a implementação do MIPv6 (UMIP). Deste modo, não existindo esta interacção, o *handover* não será executado.

Conclusão de *Handover*

Na fase de conclusão procede-se à libertação dos recursos alocados na rede onde se encontrava o MN [38].

3.3.2. Modificações Necessárias

No que diz respeito ao *Mobility Manager* presente no MN, para que este consiga forçar o processo de *handover* torna-se necessário a implementação de uma função que permita a este comunicar com o UMIP. Esta função terá de se poder chamar em qualquer instante e ter a capacidade de indicar qual a interface para a qual se pretende efectuar o *handover.*

3.4. Métricas de QoS, de QoE e de Mobilidade entre Redes Heterogéneas

Com o aumento da exigência por parte dos utilizadores no que diz respeito às garantias de qualidade de serviço, torna-se crucial a obtenção de medidas que possam quantificar e dar garantia do que se pode esperar de um determinado serviço.

Relativamente à mobilidade entre redes heterogéneas podem-se definir um conjunto de métricas que possibilitam a obtenção da informação pretendida. Estas métricas podem ser obtidas tanto a nível do protocolo de mobilidade (MIPv6) como a nível do protocolo de optimização de mobilidade IEEE 802.21.

Para o caso do MIPv6 temos:

- *Handover Delay*
  Tempo obtido desde o último pacote recebido no MN pela interface antiga, até ao primeiro pacote recebido pela nova interface.

- *Handover Execution Delay*
  Tempo desde o envio do BU pelo MN para o seu HA até a recepção do primeiro pacote pela nova interface.

Para o caso do IEEE 802.21 temos:

- Tempos relativos a cada fase no processo de *handover*
  - Tempo de iniciação.
  - Tempo de preparação.
  - Tempo de execução.
  - Tempo de conclusão.

Relativamente à existência de tráfego pode-se obter:

- *Delay.*
- *Jitter.*
- *Bitrate.*
- Pacotes perdidos.
- Pacotes fora de ordem.

Relativamente às métricas de Qualidade de Experiencia (QoE), para o caso de estarmos perante o tráfego VoIP, é obtido o *Mean Opinion Score* (MOS), tratando-se este de um método subjectivo de avaliação da qualidade de tráfego. Este é utilizado para quantificar a qualidade subjectiva de voz, baseado na média de pontos atribuídos por um conjunto de pessoas, com base na qualidade percebida. Esta medição depende principalmente do *delay*, do número de pacotes perdidos durante a transmissão de tráfego e do *codec* utilizado. Através do MOS é permitido quantificar a transmissão de VoIP em cinco níveis:

1. *Poor*.
2. *Low*.
3. *Medium*.
4. *High*.
5. *Best*.

Com o QoE é possível ter uma percepção da satisfação do usuário que faz uso do tráfego de voz. Este é calculado com base no E-MODEL.

Para a obtenção das métricas pretendidas torna-se então necessário o desenvolvimento de um módulo para que estas possam ser obtidas de forma automatizada, o que por sua vez implica a

necessidade de interacção do módulo com as implementações do protocolo de mobilidade (UMIP) e do *Mobility Manager* presente no HA.

3.4.1. Arquitectura

De forma a enquadrar o módulo das métricas na arquitectura geral já referida (Figura 3.1-1) é apresentada a Figura 3.4.1-1.

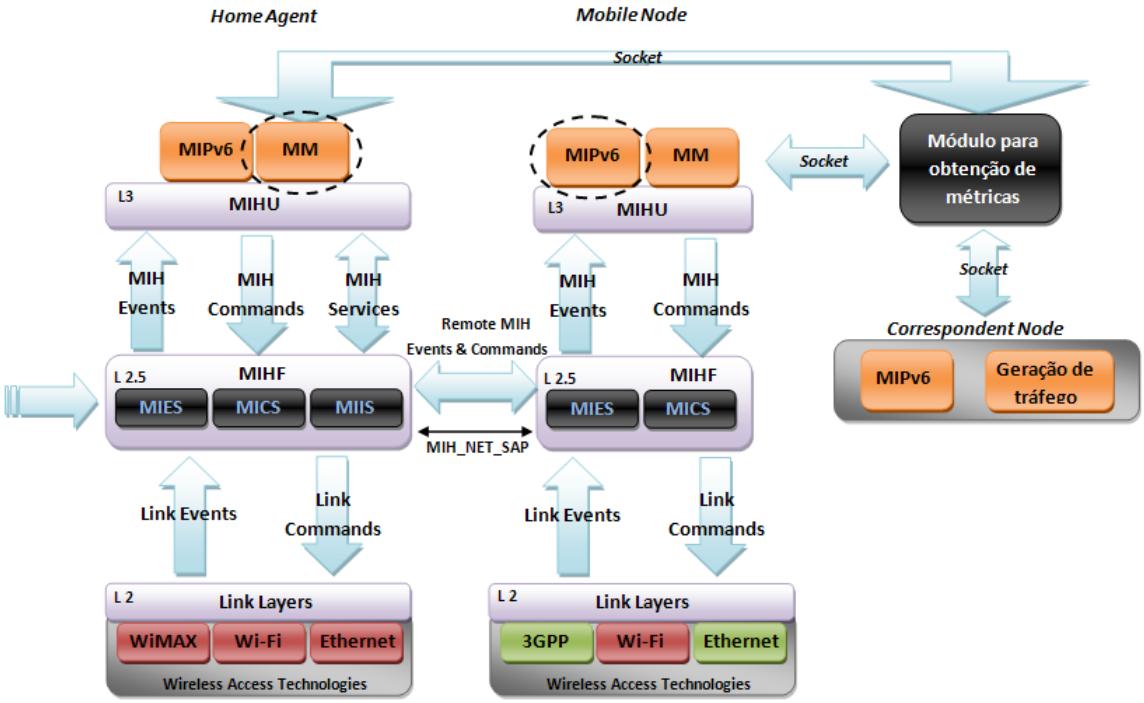

Figura 3.4.1-1: Enquadramento do módulo para obtenção de métricas

A Figura 3.4.1-1 apresenta a interacção do módulo para a obtenção das métricas, com o HA, MN e CN, sendo estas as entidades com o qual este interage.

Uma vez que o módulo necessita de comunicar tanto com o UMIP bem como com o MM presente no HA, para possibilitar que este tenha controlo no processo de iniciação de *handover* de ambas as formas, torna-se necessário desenvolver um método para que seja possível interagir com o MM presente no HA. Para o caso do MIPv6, esta necessidade já foi tida em consideração na secção 3.2.2.

Relativamente ao CN, este é utilizado para que o módulo consiga iniciar o tráfego de forma automatizada, existindo também neste caso a necessidade de interacção entre o módulo e o CN. Torna-se então necessário a implementação de uma função no CN para que seja possível a interacção com o módulo e para que este consiga iniciar o tráfego pretendido.

3.5. Resumo

Nesta secção foi apresentada a arquitectura implementada bem como o seu funcionamento.

Através da apresentação do funcionamento interno de algumas das principais entidades existentes na arquitectura foi possível identificar um conjunto de modificações necessárias para que seja possível controlar todo o processo de *handover.*

É identificada também a necessidade de interacção entre o UMIP e o MM presente no MN.

Como análise final foi definido um conjunto de métricas a obter para que seja possível efectuar uma análise a nível do processo do *handover* bem como a nível de QoS e QoE. Para esta análise foi ainda apresentada a arquitectura do módulo desenvolvido.

4. Implementação

Existindo a necessidade de controlar o processo de *handover* torna-se fulcral proceder a modificações tanto na implementação do protocolo de mobilidade (UMIP) como na implementação do *Mobility Manager* presente no MN (Figura 3.1-1).

Através deste capítulo é apresentado um conjunto de soluções, modificações e implementações para que seja possível atingir os objectivos já previamente mencionados.

Numa primeira análise, são apresentadas na secção 4.1 todas as modificações/implementações efectuadas no UMIP, seguindo-se a apresentação das funções desenvolvidas na implementação do *Mobility Manager* presente no MN, para que este possa interagir com o UMIP, secção 4.2.

Através da secção 4.3 são apresentados todos os passos e configurações necessárias para a implementação de um ambiente de mobilidade.

Na secção 4.4 é apresentado o desenvolvimento de um módulo capaz de obter as métricas tanto a nível do processo de *handover* como a nível do QoS e QoE, tendo sido estas mencionadas na secção 3.4.

Por fim, na secção 4.5, são apresentadas um conjunto de conclusões referentes a este capítulo.

Uma vez que alguns dos aspectos em consideração durante as modificações/implementações efectuadas levam em conta a utilização de um computador, são apresentadas todas as modificações necessárias e implementadas, sempre que necessário, para o caso de se utilizar um telemóvel (com o sistema operativo *Android* OS) como terminal móvel.

4.1. Modificações Efectuadas no UMIP

4.1.1. Comunicação com o UMIP

Como uma das principais necessidades temos a comunicação com o UMIP. Esta comunicação deverá tornar possível, a qualquer instante, indicar ao UMIP a necessidade de se efectuar um *handover* bem como a interface para onde este se deverá realizar. Sem esta comunicação não seria possível atingir os restantes objectivos.

Existem vários processos de comunicação que nos possibilitam este tipo de interacção. Neste caso foi tido como opção a utilização de *sockets* como modo de transmissão entre um "cliente" e um "servidor".

Os *sockets* utilizados são baseados na ligação e têm as seguintes características:

- Utilizam ligações TCP.
- Necessitam que o "cliente" se conecte ao "servidor" antes de começar a transmitir.

- As mensagens enviadas pelo “cliente” são recebidas pelo “servidor” exactamente pela mesma ordem que são enviadas.
- Após o estabelecimento da ligação e a troca das mensagens é necessário terminar a mesma.

A comunicação entre *sockets* necessita da existência das seguintes fazes:

1) Criar o socket “servidor” para que este fique a aguardar pela comunicação do “cliente”.
2) Criar a socket “cliente” e tentar comunicar com o servidor.
3) O “servidor” tem de aceitar o pedido de ligação.
4) Troca de mensagens/dados.
5) Terminação das ligações criadas [39].

Estando o modo de comunicação definido, tem-se de especificar a informação que é necessária enviar ao servidor implementado no UMIP, bem como a informação que este deve dispor ao “cliente” que entre em comunicação com ele, tratando-se neste caso do MM presente no MN.

Para se poder iniciar o processo de *handover* optou-se por enviar ao UMIP o endereço MAC da interface para a qual se pretende “migrar”. Esta opção deve-se ao facto do agente que irá comunicar com o UMIP apenas conseguir identificar as interfaces existentes através do endereço MAC. Surge então um problema, que está relacionado com o facto de o UMIP não utilizar o MAC das interfaces para as identificar, mas sim os seus nomes ou índices que lhes é atribuído. Torna-se então necessário efectuar a conversão entre o endereço MAC e o respectivo nome.

Para além da capacidade de efectuar o *handover*, foi acrescentada a opção do “cliente” poder obter informação relativa à interface em que se encontra o MN.

Como resposta aos pedidos efectuados, caso seja um pedido de *handover,* o servidor deverá responder com a confirmação ou não confirmação da realização deste. Caso seja um pedido de informação relativamente à interface onde se encontra o MN, é devolvido o endereço MAC da interface correspondente.

De forma a ilustrar o servidor desenvolvido temos o diagrama da Figura 4.1.1-1.

Inicialmente, procede-se a todas as configurações relativas ao processo de comunicação, tais como o porto pelo qual se irá estabelecer a ligação, o protocolo de endereçamento utilizado, etc. Estando este processo concluído, o servidor ficará constantemente a aguardar por uma possível ocorrência de ligação. Ao estabelecer-se uma ligação, os dados enviados pelo “novo” cliente serão armazenados num *buffer* presente no servidor para uma análise posterior.

Para converter o endereço MAC no nome da interface correspondente, bem como o processo inverso, foi desenvolvida uma função que se limita a obter essa informação através de um ficheiro criado pelo próprio sistema operativo UBUNTU. Esta função devolve dois vectores, um com os endereços MAC e outro com o nome das interfaces existentes. Após a obtenção dos vectores basta efectuar uma simples comparação de forma a obter ou o MAC ou o nome da interface

pretendida. Estes dois vectores apenas são criados ao se iniciar o UMIP, de forma a não efectuar repetidamente o mesmo processo desnecessariamente.

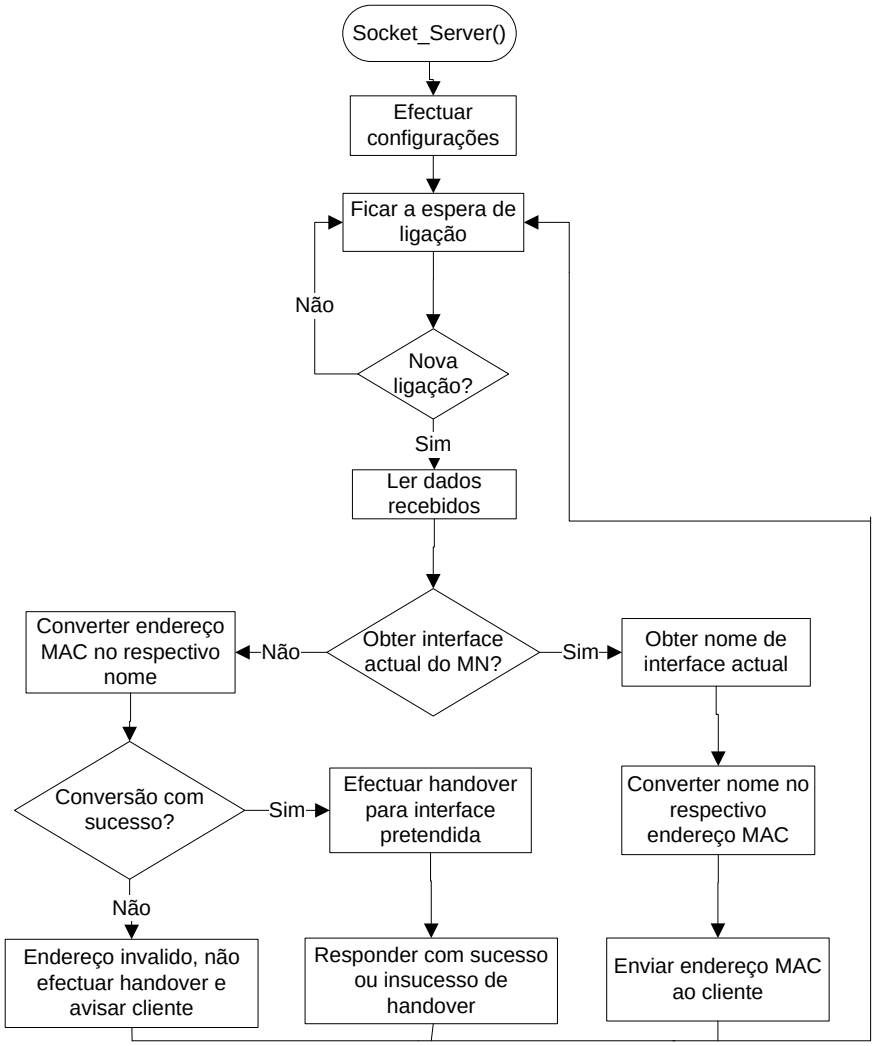

Figura 4.1.1-1: Diagrama do socket servidor implementado no UMIP

A descoberta da interface em que o MN se encontra é feita através da chamada de uma função desenvolvida no ficheiro *mn.c* que se limita a obter essa informação através de uma variável que é actualizada sempre que o MN muda de interface.

Para iniciar o processo de *handover* é chamada a função *mn_force_handover()*, também ela desenvolvida no ficheiro *mn.c*, esta contém um conjunto de variáveis de controlo de forma a forçar este processo. Deste modo passamos a não necessitar de efectuar a quebra de ligação para que o MN detecte movimento e execute o *handover*. Para forçar o *handover*, as variáveis de controlo são tidas em consideração tanto na função mn*_make_ho_verdict()* como na função mn*_ge_iface()* tal como será apresentado mais à frente. Após a activação das variáveis de controlo, a função *mn_force_handover()* espera pela confirmação da execução ou não execução do *handover*.

Este servidor será colocado no ficheiro *main.c* do UMIP e será executado após a iniciação deste, estando constantemente à escuta de uma nova ligação.

4.1.2. Controlo no Processo de *handover*

A função que é chamada pelo *socket* servidor para forçar o *handover* pode ser representada pela Figura 4.1.2-1, a esta é passado como parâmetro o nome da interface para a qual se pretende efectuar o *handover*.

Figura 4.1.2-1: Diagrama da função *mn_force_handover()*

A função utilizada para esperar pela confirmação ou não confirmação da realização do *handover* utiliza variáveis de condição para que seja permitido que esta fique à espera de receber um sinal que pode ser proveniente tanto da função que analisa os BA como devido ao nome da interface indicada não existir ou se tratar da interface actual onde se encontra o MN.

Seguem-se as modificações efectuadas tanto na função mn_*make_ho_verdict()* como na função mn_*get_iface()*. Estas têm como objectivo, tal como já foi referido anteriormente, permitir que o MN não tenha preferência constante pela sua HN, mas sim apenas no início de todo o processo, e fazer com que o MN efectue o *handover* para uma determinada interface mesmo tendo ligação com a rede em que se encontra.

Na Figura 4.1.2-2 e Figura 4.1.2-3/Figura 4.1.2-4 podem-se visualizar as alterações efectuadas às funções mn_*make_ho_verdict()* e *mn_get_iface(),* respectivamente.

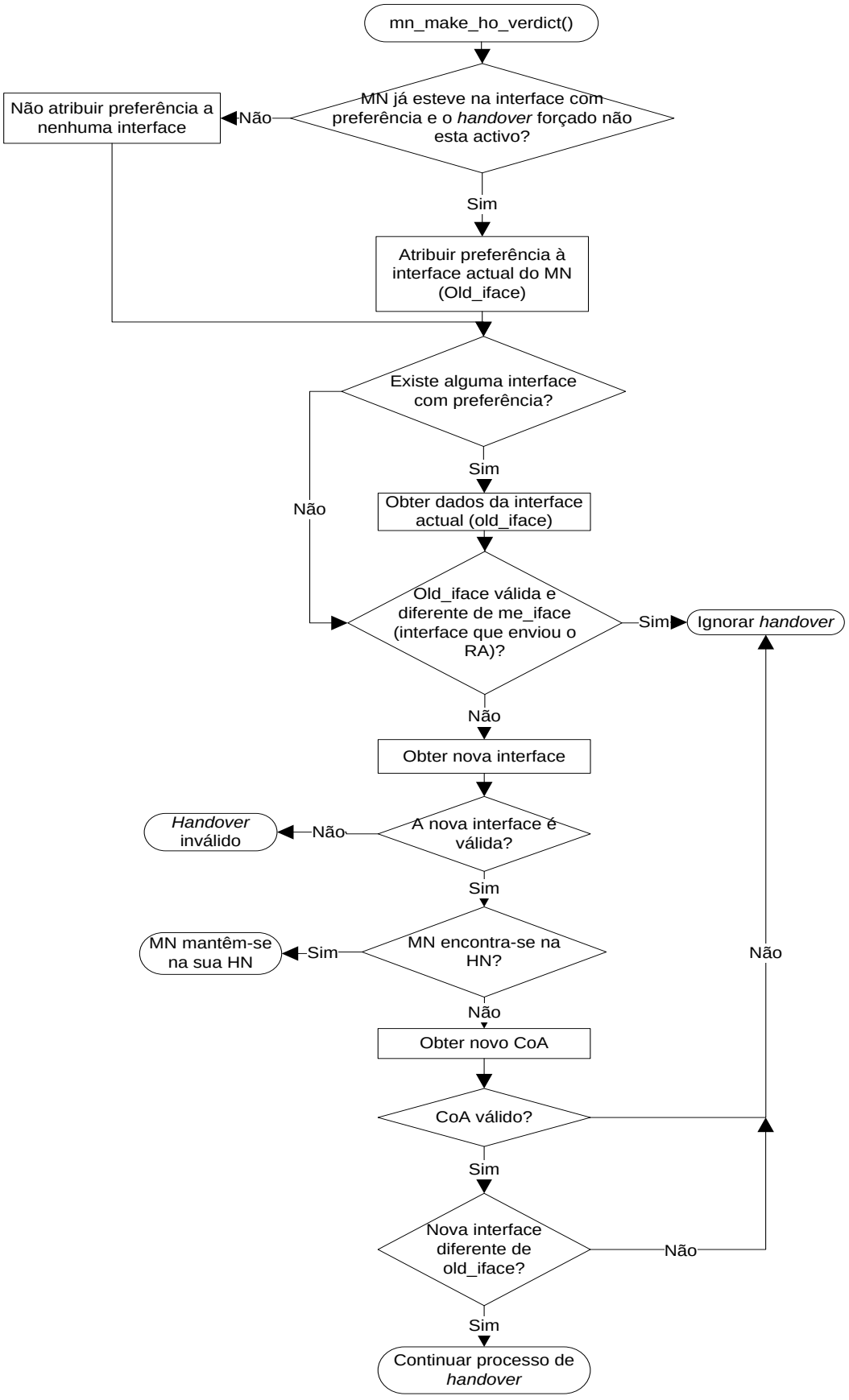

Figura 4.1.2-2: Diagrama da função *mn_make_ho_verdict()* com modificações

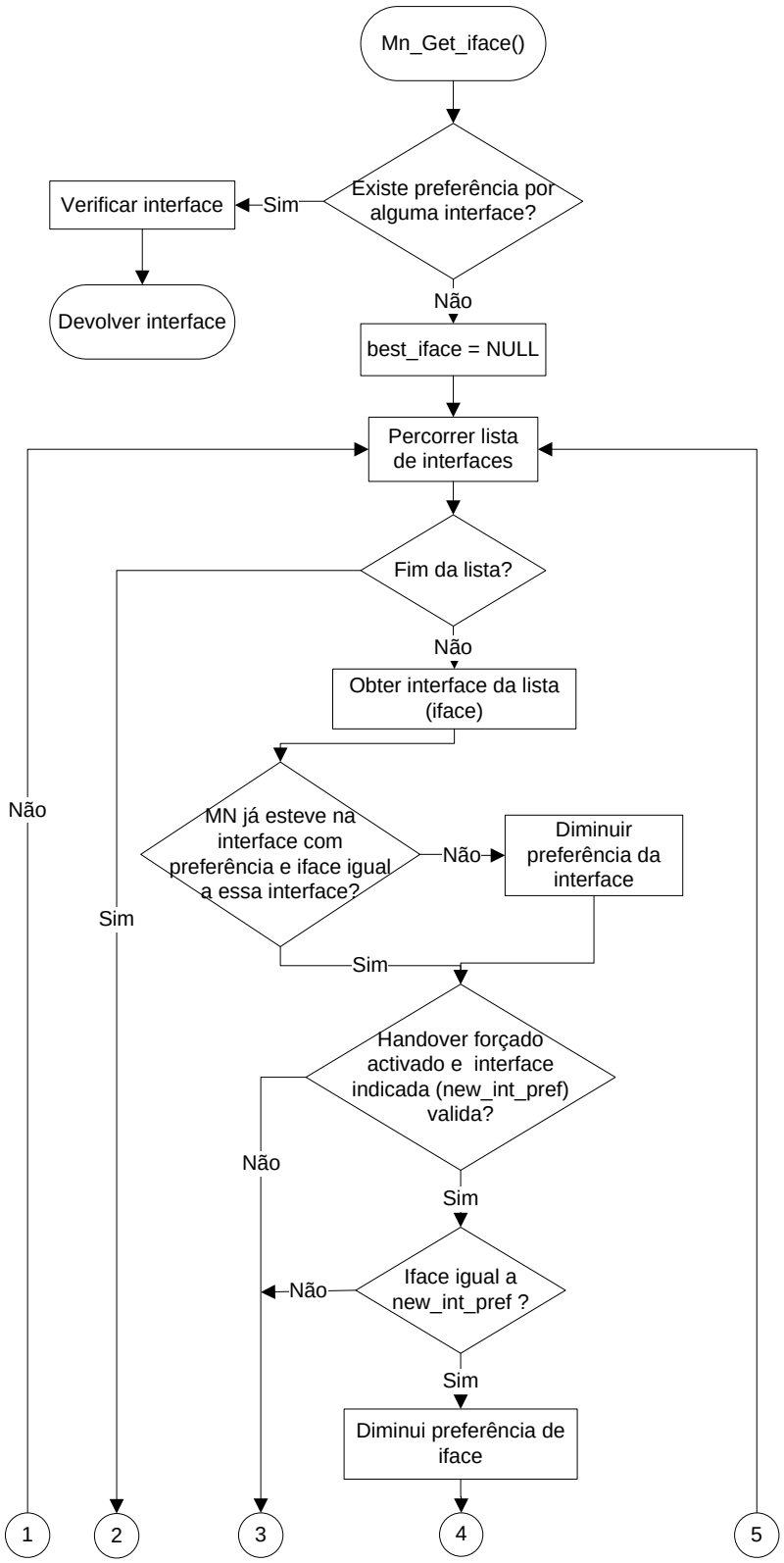

Figura 4.1.2-3: Diagrama da função *mn_get_iface()* com modificações

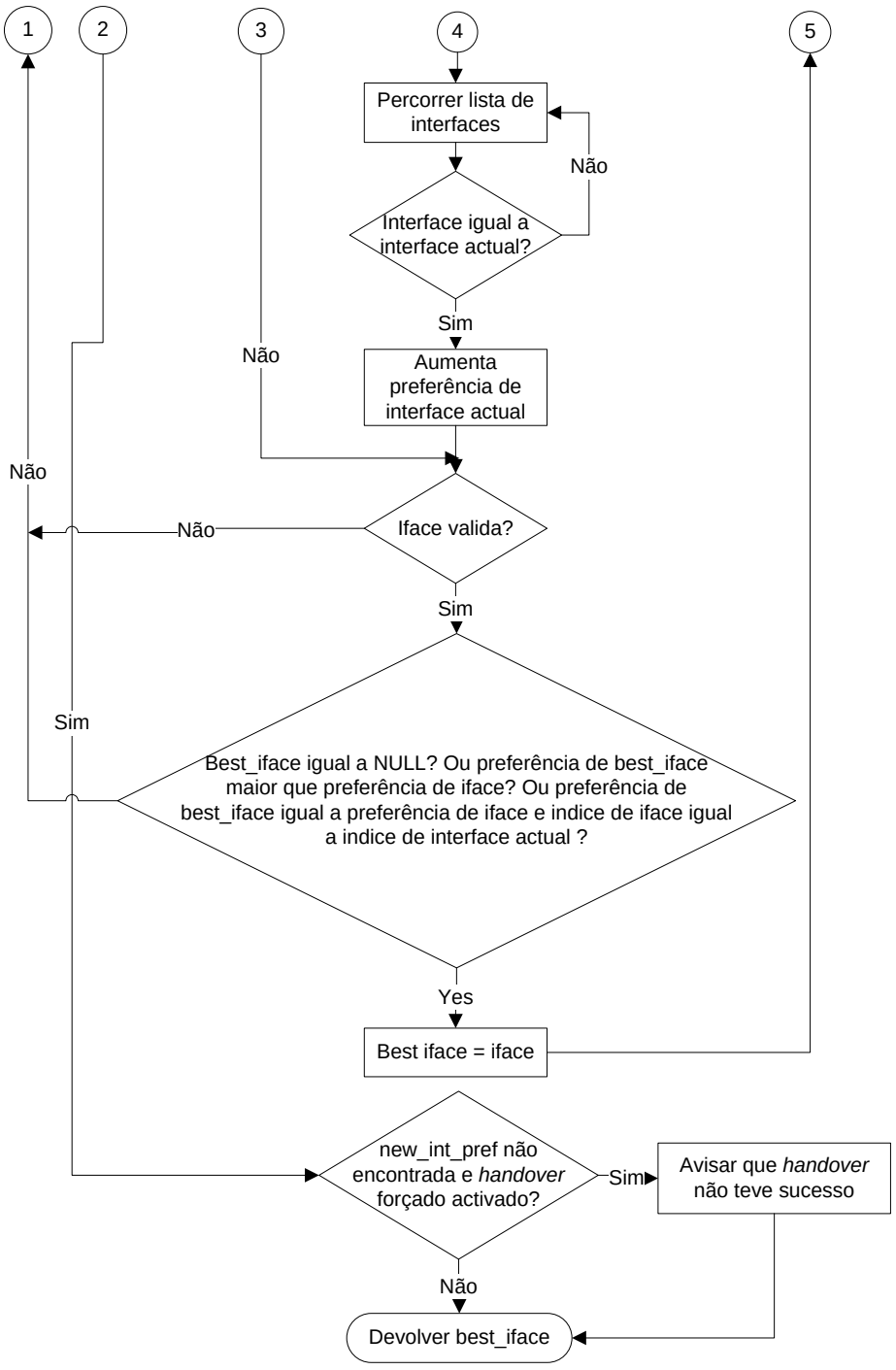

Figura 4.1.2-4: Diagrama da função *mn_get_iface()* com modificações (continuação)

Analisando a Figura 4.1.2-2 as principais diferenças relativamente à função original são:

- Ao iniciar a função, esta vai verificar se o MN já esteve numa interface pré-definida e se o *handover* forçado não está activo. Deste modo, tem-se a capacidade de decidir em qual interface se pretende que o MN inicie, podendo esta se tratar da interface que faz ligação com a HN. De notar que após o MN estar na interface pré-definida, esta verificação passa

a estar sempre válida, passando a verificação a ser controlada apenas pela activação ou não do *handover* forçado. Deste modo pode-se garantir que o MN inicia sempre na interface que faz ligação com a sua HN, ou mesmo noutra interface, e que sempre que se pretender verificar a preferência das interfaces (definida por cada interface num campo apropriado) para efectuar posteriormente um *handover*, basta activar as variáveis de controlo através da função *mn_force_handover*(), passando deste modo a não atribuir preferência à interface actual do MN. Com este processo é obtido controlo na preferência pela interface em que o MN se encontra, sendo que esta apenas é tida em consideração aquando da não activação do *handover* forçado, pois para além de se retirar a preferência pela HN, ao indicarmos que se pretende forçar um *handover*, o MN será forçado a não atribuir preferência à interface em que se encontra.

- A verificação relativa ao MN se encontrar na HN ou ter ligação com esta é feita após a obtenção da nova interface. Deste modo elimina-se a preferência que o MN tinha pela sua HN passando a verificar sempre as interfaces existentes e suas preferências.

Na Figura 4.1.2-3 e Figura 4.1.2-4 podemos observar as seguintes diferenças relativamente à função original *mn_get_iface()* :

- De forma a forçar o MN a se iniciar numa determinada interface pré-definida, ao iniciar-se o processo de percorrer a lista de interfaces é sempre verificado se o MN já esteve nessa interface. Caso este ainda não tenha estado diminui-se a preferência da interface em questão. Se pelo contrário o MN já esteve na interface pré-definida não se altera a preferência desta. De notar que, quanto menor o valor da preferência, maior será a preferência por essa interface.

- Segue-se uma verificação à activação do *handover* forçado. Caso este esteja activo e a interface indicada para efectuar o *handover* seja válida, é verificado se a interface obtida da lista (a iface) é igual à interface indicada e caso seja, é diminuída a sua preferência e aumentada a preferência da interface onde se encontra o MN. Este último passo é efectuado para garantir que todas as interfaces mantêm a mesma preferência de forma a garantir que o *handover* é efectuado para a interface correcta. Caso nenhuma das verificações seja válida passa-se directamente à verificação da interface obtida da lista, como já ocorria na função original.

- Relativamente à comparação de interfaces foi efectuada uma pequena modificação relativamente ao caso das interfaces terem a mesma preferência. Neste caso será sempre feita uma comparação com o índice da interface actual, independentemente de existir preferência ou não por uma determinada interface. Esta modificação torna-se necessária, pois para se poder verificar as preferências de cada interface é “simulado” que a interface em que se encontra o MN não existe, ou seja, não lhe é atribuída preferência. Deste modo, com o código original, em vez de se comparar com o índice da interface actual

comparava-se com o valor zero devido a este assumir que para chegar a esta fase a interface não exista, o que provocava a devolução da primeira interface existente na lista.

- No caso do *handover* forçado estar activo e a interface indicada para a realização deste não ter sido encontrada ou ser igual à interface actual do MN, é indicado que o *handover* não foi efectuado.

De forma a demonstrar de um modo mais simplificado o funcionamento geral desenvolvido, relativamente ao processo de controlo do *handover* temos a Figura 4.1.2-5.

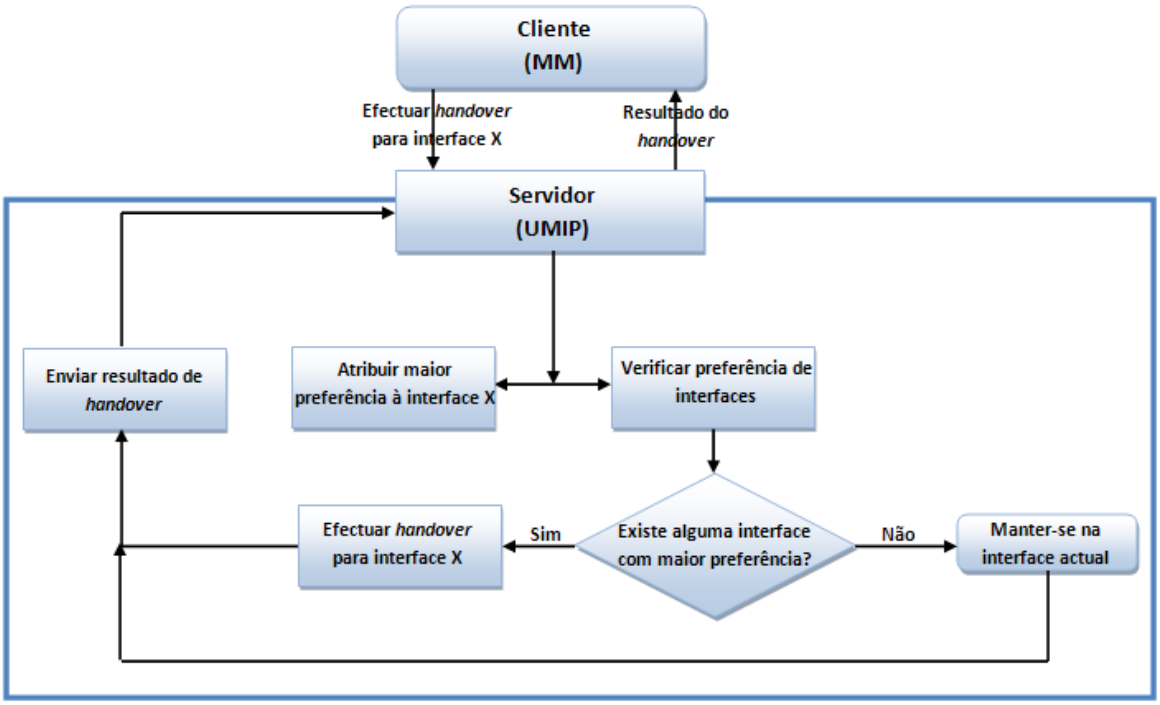

Figura 4.1.2-5: Diagrama de funcionamento para forçar *handover* (simplificado)

4.1.3. Optimização de Rota

Ao analisar o processo de *handover* com optimização de rota foi identificada uma falha neste processo, independentemente das modificações implementadas.

- Após a detecção de movimentação por parte do MN, independentemente de ter sido devido a perda de ligação ou ter sido forçada, após o envio do BU por parte do MN para o seu HA, este tenta iniciar o processo de *return routability* seguido do respectivo envio do BU para o CN sem que o seu novo CoA esteja validado pelo seu HA, e sem que a criação/modificação do túnel esteja completa. Devido a este processo, o envio da mensagem *mn_rr_cond_start_cot* para iniciar o processo de optimização irá falhar. Após o MN receber um BA por parte do seu HA, este irá tornar

a tentar iniciar o processo de optimização, o qual não será efectuado devido ao MN detectar que este foi iniciado recentemente e devido ao *timeout* pré-definido não ter sido ultrapassado. Só após se ultrapassar este *timeout* (5 segundos) é que o MN irá iniciar novamente o processo de optimização e concretizá-lo.

- No caso de se tratar de pacotes UDP, dado que estamos a forçar o *handover* sem que exista perda de ligação, ou seja, ficando sempre com a interface anterior onde se encontrava o MN disponível, não é possível ao CN detectar a movimentação efectuada pelo MN, pois este apenas recebe os pacotes sem que tenha de confirmar a sua recepção. Enquanto o MN não comunicar com o CN pela sua nova interface, este nunca se aperceberá da ocorrência do *handover*.

Torna-se assim necessário modificar o código do UMIP para que sempre que o *handover* seja efectuado de um modo forçado, este inicie o processo de optimização apenas quando o endereço da nova interface já estiver validado, podendo deste modo corrigir as limitações existentes neste campo.

Para o suporte de optimização de rota aquando a realização do *handover* de modo forçado, foi desenvolvido uma nova função no ficheiro *retrout.c* do UMIP designada por *force_CoTi_and_HoTi()*. Esta função tem como parâmetros de entrada dois inteiros que funcionarão como *flags* de controlo.

A função *force_CoTi_and_HoTi()* será chamada em apenas dois pontos do ficheiro *mn.c*, no inicio da função *mn_force_handover()* e na função que analisa a recepção dos BA (*mn_recv_ba()*).

Inicialmente, quando é executado o *handover* através da função *mn_force_handover()*, esta irá efectuar uma chamada à função *force_CoTi_and_HoTi()* por forma a que o processo de optimização nunca seja iniciado a menos que seja pedido. Para isso são utilizadas variáveis de condição que bloqueiam este processo.

Após a recepção do BA enviado pelo HA em resposta ao BU é novamente chamada a função *force_CoTi_and_HoTi()* por forma a que reactive o processo de optimização de rota e force o envio das mensagens *Home Test Init* e *Care-of Test Init,* sempre que seja necessário. Seguidamente à recepção da resposta às mensagens enviadas é enviado um BU por parte do MN para o CN, para que este actualize o CoA utilizado pelo MN na sua *Binding Cache*.

4.1.4. Modificações necessárias para adaptação ao telemóvel quando utilizado como terminal móvel

Todas as modificações apresentadas no que diz respeito ao UMIP têm em consideração que estas são implementadas em máquinas Linux, mais concretamente em computadores. Para o caso de se tratar de um telemóvel com o sistema operativo Android OS estas praticamente mantêm-se, mas no entanto torna-se necessário efectuar uma pequena alteração no processo utilizado para converter o endereço MAC, passado ao terminal móvel para efectuar o *handover*, no nome

da interface correspondente. Neste processo é utilizado um ficheiro criado de forma automática pelo sistema operativo UBUNTU, o qual não é criado no telemóvel. Para ultrapassar este problema, foi definido um ficheiro idêntico ao ficheiro existente no UBUNTU contendo as interfaces existentes no telemóvel bem como os respectivos endereços MAC.

Para o caso do telemóvel foi ainda implementada a capacidade de terminar o UMIP através de uma entidade/aplicação externa. Neste caso deixa-se de ser necessário ter o telemóvel ligado a um computador para poder terminar este processo. Esta funcionalidade é permitida através da chamada de uma função de terminação a partir do servidor desenvolvido na função *main.c* do UMIP. A função de terminação mencionada trata-se de uma função já utilizada pelo UMIP aquando a sua terminação pelo processo normal.

4.2. Modificações efectuadas no *Mobility Manager*

Para se poder forçar o processo de *handover* no UMIP através do MM presente no MN foi desenvolvido um *socket* "cliente" capaz de comunicar com o *socket* "servidor" implementado no UMIP.

Ao *socket* "cliente" é passado o endereço MAC da interface para a qual se pretende efectuar o *handover*. Este por sua vez irá comunicar com o *socket* "servidor" presente no UMIP, passando a interface indicada. Após o envio da informação pretendida, o socket "cliente" ficará a aguardar a recepção de uma mensagem com informação relativa ao sucesso ou insucesso do *handover*. Se por outro lado não for passado o endereço MAC mas sim um pedido de obtenção do MAC da interface onde se encontra actualmente o MN, este também é suportado, sendo que o processo é idêntico ao caso anterior, a única modificação é que em vez de se enviar um MAC para se efectuar um *handover* é enviada uma *string* "get_iface".

Relativamente ao funcionamento do módulo já indicado na secção 3.4, este necessita de conseguir comunicar com o MM presente no HA para o caso de se pretender iniciar todo o processo de *handover* utilizando a implementação do protocolo IEEE 802.21. Para que este processo de comunicação se torne possível é desenvolvido um "servidor" no MM presente no HA. A este "servidor" é apenas possível indicar o MAC da interface para a qual se pretende realizar o *handover*, e caso este seja válido, o MM utiliza essa informação para iniciar todo o processo.

4.3. Configurações Necessárias a um Ambiente de Mobilidade

De forma a se poder estar perante um ambiente de mobilidade IPv6 são sempre necessárias três entidades distintas, tal como já foi mencionado na secção 2.2.3:

- *Mobile Node*
- *Home Agent*
- *Correspondent Node*

A utilização do *Correspondent Node* apenas se torna necessária caso se pretenda utilizar a optimização de rota; caso contrário todas as suas configurações não se tornam necessárias.

Existindo a necessidade de comunicação entre todas as entidades indicadas, torna-se crucial que estas tenham suporte de mobilidade IPv6, a qual depende do kernel utilizado. Para este caso é utilizada a versão 2.6.30.6, que já apresenta o tipo de suporte pretendido.

Após se garantir o suporte de mobilidade é necessária a activação de reencaminhamento de pacotes sempre que uma entidade se encontre entre duas redes e possa ter a funcionalidade de "intermediária" num processo de comunicação, situação que acontece com o HA. Esta activação é efectuada através do comando: *echo "net.ipv6.ip_forward = 1" >> /etc/sysctl.conf*.

Para que seja possível a detecção de mobilidade é necessária a existência de, pelo menos, um *default router* em cada rede capaz de anunciar a rede em que se encontra. Para este processo são utilizados os *Routers Advertisements*, permitindo deste modo indicar tanto o prefixo da rede como o endereço do router ao qual o MN tem acesso. Estas mensagens são também utilizadas após a configuração do endereço *link-local* por parte do MN para que este possa obter o seu endereço global no modo de auto-configuração *stateless*. Para se ter suporte a este tipo de mensagens é utilizado o *Linux IPv6 Router Advertisement Daemon* (Radvd), que após a sua instalação necessita da respectiva configuração (ficheiro radvd.conf).

Para a realização desta dissertação foram considerados dois tipos de configuração, uma para o caso de se tratar da entidade HA e outra para as restantes entidades.

No caso de se tratar do HA temos:

```
interface virtual1
{
        AdvSendAdvert on;
        MaxRtrAdvInterval 1;
        MinRtrAdvInterval 0.5;
        AdvIntervalOpt off;

        AdvHomeAgentFlag on;
        AdvHomeAgentInfo on;
        HomeAgentLifetime 10000;
        HomeAgentPreference 20;
        AdvMobRtrSupportFlag on;

        prefix 2001:106:4444::3/64
        {
                AdvRouterAddr on;
                AdvOnLink on;
                AdvAutonomous on;
                AdvPreferredLifetime 10000;
                AdvValidLifetime 12000;
        };
};
```

Figura 4.3-1:Configuração do Radvd – *Home Agent*

No caso de se tratar de outro tipo de entidade temos, a título de exemplo:

```
interface eth1
{
        AdvSendAdvert on;
        MaxRtrAdvInterval 1;
        MinRtrAdvInterval 0.5;
        AdvIntervalOpt off;

        AdvHomeAgentFlag off;
        AdvHomeAgentInfo off;
        HomeAgentLifetime 10000;
        HomeAgentPreference 20;

        prefix 2001:106:3333::3/64
        {
                AdvRouterAddr on;
                AdvOnLink on;
                AdvAutonomous on;
                AdvPreferredLifetime 10000;
                AdvValidLifetime 12000;
        };
};
```

Figura 4.3-2: Configuração do Radvd – Entidades em geral

Como pontos principais nas configurações presentes na Figura 4.3-1e Figura 4.3-2, temos:

- *Interface* – permite definir a interface para a qual se pretende enviar os RA.

- *MaxRtrAdvInterval* e *MinRtrAdvInterval* – através destas duas variáveis torna-se possível definir o tempo máximo e mínimo entre cada RA enviado periodicamente, ou seja, de modo não solicitado, permitindo assim melhorar os tempos de detecção de movimento, que melhoram com a diminuição destes.

- *AdvHomeAgentFlag* – quando activa permite indicar à entidade que recebe o RA que quem envia a mensagem é o HA. Esta deve estar activa na entidade HA.

- *AdvHomeAgentInfo* – permite fornecer informações relativas ao HA, tais como preferências, *lifetimes*, etc.

- *AdvMobRtrSupportFlag* – quando activa permite que o registo do MN seja feito segundo o *Network Mobility* (NEMO) *Basic Support Protocol*.

- *Prefix* – permite indicar tanto o prefixo da rede, como o endereço da interface pela qual é enviado o RA. Sempre que é enviado o endereço da interface é necessário activar a variável AdvRouterAddr.

Seguidamente passa-se à instalação do UMIP. Como já foi indicado, a versão utilizada é a 0.4 (*mipv6-deamon-umip-0.4*). Este terá de ser instalado nas três principais entidades indicadas, ou

seja, no HA, no MN e no CN. Após a sua instalação é necessário proceder à respectiva configuração (ficheiro *mip6d.conf*) dependente de cada entidade.

HA:

```
NodeConfig HA;
DoRouteOptimizationCN enabled;
UseCnBuAck enabled;
Interface "virtual1";
UseMnHaIPsec disabled;
```

Figura 4.3-3: UMIP – configuração do HA

CN:

```
NodeConfig CN;
Interface "eth0";
DoRouteOptimizationCN enabled;
UseMnHaIPsec disabled;
```

Figura 4.3-4: UMIP - configuração do CN

MN:

```
NodeConfig MN;
DoRouteOptimizationCN enabled;
DoRouteOptimizationMN enabled;
UseMnHaIPsec disabled;
SendMobPfxSols enabled;
UseCnBuAck enabled;
MnDiscardHaParamProb enabled;

Interface "ath0" ;
MnHomeLink "ath0" {
      HomeAddress 2001:106:4444::2/64;
      HomeAgentAddress 2001:106:4444::3;

}
Interface "eth0";
```

Figura 4.3-5: UMIP – configuração do MN

Através das Figura 4.3-3, Figura 4.3-4 e Figura 4.3-5 pode-se destacar o campo *interface*, em que este é utilizado para indicar qual a interface que funcionará como entidade respectiva. Para o caso da configuração do MN pode-se ainda destacar o campo *MnHomeLink*, que permite definir a interface física de ligação ao HA, o *HomeAddress*, utilizado para indicar o endereço global que será utilizado pelo MN para que este possa estar sempre acessível e contactável (este endereço mantêm-se estático ao longo da movimentação do MN) e o campo *HomeAgentAddress* que é utilizado para indicar o endereço do HA respectivo ao MN em questão. Relativamente ao campo *interface*, no caso do MN este permite indicar quais as interfaces que o MN deverá ficar à "escuta" pelos RAs, ou seja, quais as interfaces a ter em consideração para a detecção de movimento.

Após todas estas configurações e estando garantida a comunicação entre todas as entidades, através da criação de rotas ou mesmo através da criação de túneis, caso seja necessário, é iniciado o UMIP, utilizando o ficheiro executável criado após a sua instalação em cada entidade e pela seguinte ordem: 1) CN, 2) HA, 3) MN.

Esta ordem torna-se extremamente importante para o correcto funcionamento do UMIP (devido aos processos de registos). No caso de se iniciar primeiro o UMIP no MN do que no seu HA, o MN já não se conseguirá registar no seu HA devido ao facto de este ainda não "existir".

4.4. Métricas de QoS e QoE

Tornando-se fundamental a obtenção de dados referentes a todo o processo de mobilidade, foi desenvolvido um programa capaz de o fazer de forma automatizada, as *probes* móveis, obtendo todas as métricas mencionadas na secção 3.4.

A estrutura do programa desenvolvido pode ser visualizada através do diagrama da Figura 4.4-1/Figura 4.4-2:

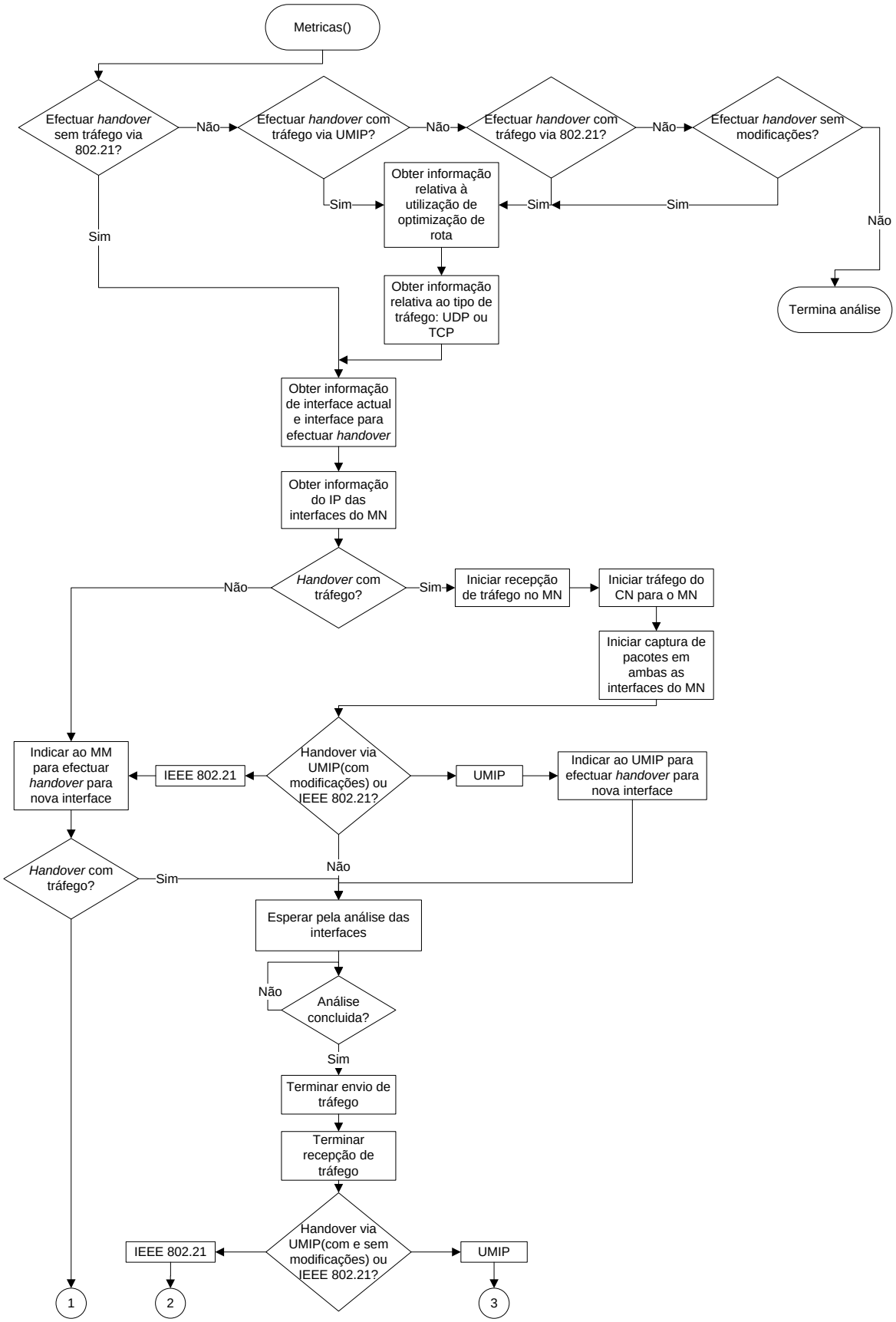

Figura 4.4-1: Diagrama do programa para obtenção de métricas

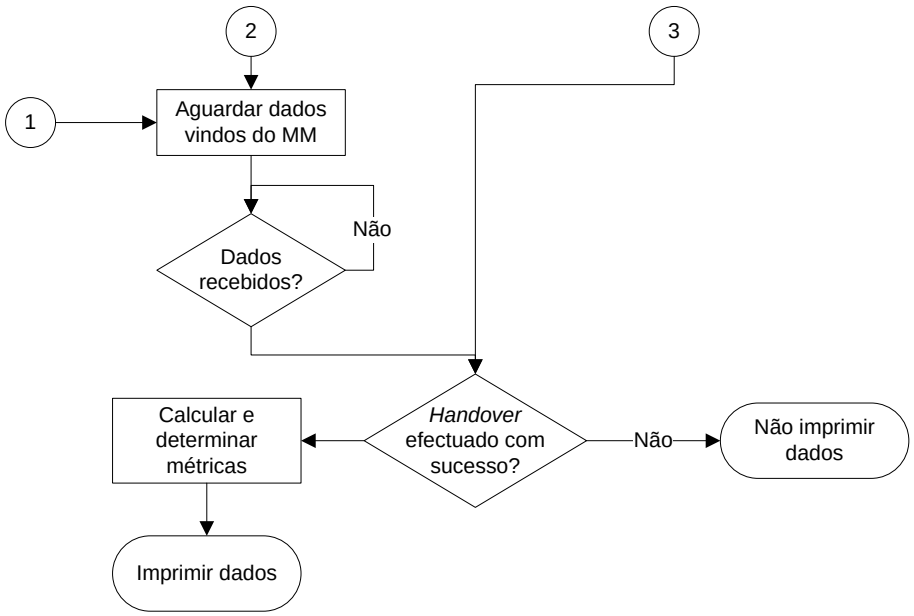

Figura 4.4-2: do programa para obtenção de métricas (continuação)

Como se pode ver pela Figura 4.4-1/Figura 4.4-2 o programa desenvolvido permite-nos obter o valor das métricas para quatro casos distintos:

- *Handover* sem tráfego
  Neste caso apenas são tidos em conta as métricas fornecidas pelo MM, que incluem os tempos das diversas fases de *handover*.

- *Handover* com tráfego iniciado directamente pelo UMIP
  Para este tipo de *handover* são tidos em conta apenas as métricas obtidas pelo programa, que incluem:
  - *Handover Execution Delay.*
  - *Handover Delay*.
  - *Delay.*
  - *Jitter.*
  - Número de pacotes perdidos.
  - *Bitrate*.
  - MOS.
  - Número de pacotes fora de ordem.

- *Handover* com tráfego iniciado pelo IEEE 802.21, mais concretamente pelo MM presente no HA.
  Para este tipo de *handover* são obtidas todas as métricas mencionadas.

- *Handover* com tráfego iniciado pela quebra de ligação da interface usada pelo MN.

Este processo destina-se a efectuar medições utilizando a implementação original do UMIP para a detecção de movimentação, ou seja, sem que se proceda às modificações mencionadas. Deste modo torna-se possível a obtenção de um ponto de comparação para que se possa realçar a necessidade de se proceder a modificações. As métricas obtidas neste caso são as mesmas que no caso em que usamos o UMIP com modificações.

Após efectuada a decisão relativamente ao processo usado para iniciar o *handover*, caso este seja efectuado na presença de tráfego é necessário que o utilizador indique se este é realizado com ou sem optimização de rota e de que tipo de tráfego se trata, se UDP ou se TCP.

Independentemente de se utilizar tráfego ou não, é introduzido pelo utilizador o nome da interface para o qual se pretende iniciar o *handover,* sendo que as restantes informações relativas às interfaces são obtidas automaticamente.

Caso se opte por obter as métricas sem a presença de tráfego apenas é indicado ao MM presente no HA, através de *sockets*, a necessidade de iniciar este processo bem como o endereço MAC da interface para o qual se deve executar, ficando o programa à espera da resposta do MM com os tempos pretendidos, ou seja, os tempos de cada fase de *handover* efectuados pelo IEEE 802.21. Após a recepção dos tempos, estes serão apresentados ao utilizador. Se por outro lado se pretender obter as métricas com a presença de tráfego é iniciada a recepção de pacotes no MN por parte do *DISTRIBUTED INTERNET TRAFFIC GENERATOR* (D-ITG) e indicado a um servidor desenvolvido no CN para que este inicie o tráfego para o MN, sendo este processo baseado na chamada de *system calls* para que seja permitido iniciar o D-ITG com o tráfego pretendido. Seguidamente é iniciada a captura de pacotes em ambas as interfaces do MN, ou seja, na interface em que ele se encontra e na interface para a qual será efectuado o *handover,* tornando-se esta numa das principais funções deste processo. Através desta função é obtido o tempo de *Handover Execution Delay*, *Handover Delay*, *jitter* e o número de pacotes fora de ordem.

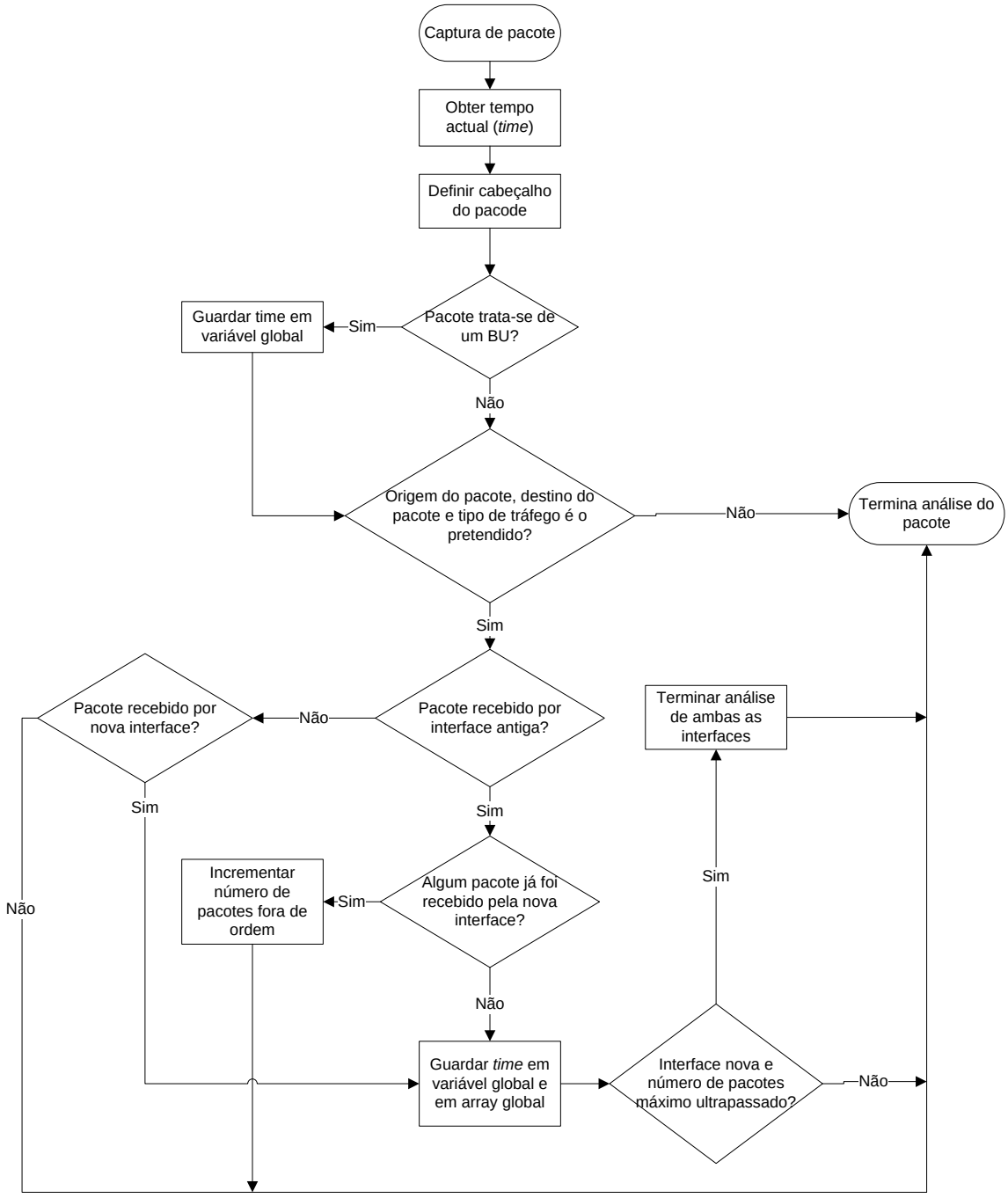

Figura 4.4-3: Métricas – processo de análise de pacotes

Para proceder à captura de pacotes é utilizado como auxilio as bibliotecas *pcap*. Sempre que uma determinada interface recebe um pacote, é chamada a função descrita na Figura 4.4-3. Esta permite obter os instantes de recepção de cada pacote, guardando esse mesmo valor sempre que se trata de um pacote pretendido. Para se poder verificar de forma correcta se o pacote é realmente o pretendido tem-se de ter alguns aspectos em consideração:

- Pacote recebido e optimização de rota activa.
- Pacote recebido e optimização de rota inactiva.

- Pacote recebido através de um túnel ipv6-ipv6.
- Pacote recebido sem utilização de túnel ipv6-ipv6.
- Pacote recebido através de um túnel ipv4-ipv6.
- Pacote recebido sem utilização de túnel ipv4-ipv6.
- Pacote recebido quando o MN se encontra na HN.

Em todos estes casos o cabeçalho do pacote recebido é diferente, o que torna necessário a adição dos bytes correspondentes aquando a definição do cabeçalho de cada pacote, para que se possa comparar os campos pretendidos. Estes campos referem-se à origem e destino do pacote, bem como ao tipo de protocolo utilizado, se UDP ou TCP.

Para o caso da análise do pacote BU, torna-se ainda necessário a criação do *mobility header* para que seja possivel verificar se de facto se trata de um BU.

Dependendo da entidade escolhida para iniciar o processo de *handover*, é indicado ao UMIP ou ao MM presente no HA para iniciarem este processo. Esta indicação é feita recorrendo a um *socket* "cliente" que entra em comunicação com um "*socket"* servidor presente tanto no UMIP como no MM presente no HA. Através deste é indicado o endereço MAC da interface para a qual se pretende efectuar o *handover*.

Para o caso de se estar perante a obtenção de métricas utilizando o UMIP sem qualquer tipo de modificações torna-se necessário efectuar a quebra de ligação da interface onde se encontra o MN para que este inicie o processo de *handover*. Dado que neste caso não existe qualquer tipo de comunicação com a implementação do protocolo de mobilidade, não é possível indicar a este a necessidade de se efectuar o *handover*.

Após a conclusão da análise das interfaces, que ocorre após a obtenção dos tempos/medições pretendidas, é terminada a geração de tráfego no CN e a recepção de tráfego por parte do MN. Para que seja possível analisar os dados produzidos pelo D-ITG é necessário que a terminação da recepção dos pacotes no MN seja feita de modo correcto, para isso é obtido o identificador do processo do D-ITG e enviado para este o sinal *INT*, o qual é assumido no código do D-ITG para terminar correctamente.

Terminado o processo da análise de tráfego podem ocorrer duas situações, caso o *handover* tenha sido iniciado pelo MM presente no HA, tem de se aguardar pelos dados vindos deste; se por outro lado o *handover* se tenha iniciado pelo UMIP, ou caso os dados vindos do MM já tenham sido enviados para o MN, é apresentado ao utilizador os dados do UMIP, do IEEE 802.21 e os de QoE, sendo todos estes dados, incluindo os de QoS, guardados paralelamente em ficheiros para uma análise posterior.

Para a obtenção do MOS (QoE) são utilizados tanto os valores de *delay* como o número de pacotes perdidos, obtidos directamente e de forma automatizada a partir do ficheiro que contém os dados de QoS e que é gerado pelo D-ITG. De notar o facto desta medida apenas ser obtida para o caso de termos o VoIP como tráfego em análise.

De realçar que todos os processos mencionados são efectuados de forma automática, sendo necessário apenas indicar a interface para a qual se pretende efectuar o *handover,* se este é efectuado com optimização de rota ou não e o tipo de tráfego que vai ser transmitido.

4.4.1. Modificações necessárias para adaptação ao telemóvel quando utilizado como terminal móvel

Para que seja possível a obtenção de métricas de uma forma optimizada aquando da utilização do telemóvel como terminal móvel, foram efectuadas um conjunto de modificações ao programa desenvolvido para a obtenção das métricas bem como a correcção de alguns problemas existentes.

Um dos problemas que surgiu prende-se com a utilização das *system calls*. Este problema deve-se ao facto de as bibliotecas utilizadas serem Linux e a chamada de algumas funções presentes na definição do comando *systemcall()* utilizar ficheiros presentes no sistema operativo. Sendo assim, existem ficheiros necessários que se encontram em localizações diferentes, dependendo do sistema operativo utilizado. Para contornar este problema foi definido no próprio módulo das métricas a função *systemcall()*, alterando os caminhos de determinados ficheiros, sempre que necessário. Deste modo é utilizada a *systemcall()* definida e não a existente na biblioteca.

De forma a tornar o processo de obtenção de métricas mais optimizado tornou-se possível definir o número de vezes que se pretende efectuar as medidas, não necessitando de executar o programa sempre que se pretende obter as métricas. Neste caso temos de efectuar sempre um *handover* de 3G para Wi-Fi e de Wi-Fi para 3G, de forma contínua, até se atingir o número de medidas definidas.

Com a capacidade de se executar a obtenção de métricas de uma forma sequencial, surge um problema com a utilização do D-ITG. O ficheiro de análise de tráfego criado pelo D-ITG, aquando da utilização do mesmo fluxo, efectua uma média de todos os *handovers* durante a obtenção das métricas, o que não é pretendido devido a termos sempre de efectuar um *handover* de 3G para Wi-Fi e de Wi-Fi para 3G, tornando deste modo os resultados independentes do tipo de *handover*. De forma a ultrapassar este problema, o CN em vez de iniciar apenas um fluxo de dados passou a gerar vários fluxos de dados, tendo em consideração a sincronização de todo o processo, ou seja, enviando o mesmo fluxo o tempo suficiente para a realização do *handover*. Deste modo o D-ITG passa a efectuar a análise dos dados dependendo do fluxo em questão.

4.5. Conclusões

Neste capítulo foram apresentadas as funções desenvolvidas bem como modificações às já existentes.

Como breve resumo, relativamente ao UMIP foram permitidas as seguintes acções:

- Comunicação do UMIP com o "exterior".
- Capacidade de iniciar o *handover* a qualquer momento.
- Capacidade de definir a interface para a qual se pretende efectuar o *handover*.
- Capacidade de efectuar o handover sem que tenha de existir quebra de ligação.

- Fornecer informação relativa à execução do *handover*.
- Fornecer informação relativa à interface actual onde se encontra o MN.
- Suportar optimização de rota para o caso do *handover* ser forçado e para o caso de se tratar de tráfego UDP.

Já para a implementação do *Mobility Manager* presente no MN foram permitidas as seguintes acções:

- Comunicação do MIHU (MM) com o UMIP
- Capacidade de indicar ao UMIP a necessidade de efectuar o *handover* para uma determinada interface.
- Capacidade de obter informação relativa à interface actual onde se encontra o MN.

Relativamente à quantificação do processo de *handover* é apresentado todo o processo desenvolvido para a que seja possível a obtenção de métricas de desempenho do *handover* entre redes heterogéneas bem como medidas de QoS e QoE.

Durante a apresentação das modificações e implementações efectuadas foram apresentadas, sempre que necessário, as modificações a efectuar para que seja possível a utilização do telemóvel como terminal móvel.

Estando esta fase concluída torna-se então possível a mobilidade dos utilizadores de forma optimizada, bem como a quantificação de todo este processo.

5. Demonstrador de Mobilidade e Avaliação de Desempenho

Através da secção 5.1 é apresentado o demonstrador implementado bem como algumas modificações necessárias para se obter todos os dados pretendidos.

Na secção 5.2 é efectuada uma descrição relativa aos pontos fundamentais que influencia directamente o processo de *handover* bem como os tipos de *handover* que se pretende efectuar. Nesta secção é ainda efectuada uma descrição dos vários modos efectuados para a obtenção das métricas pretendidas, seguida de uma análise ao tipo de tráfego utilizado.

A secção 5.3 apresenta todos os resultados obtidos para que se possa quantificar todo o processo de *handover*, bem como uma descrição e justificação de cada um dos casos apresentados.

Como análise final deste capítulo é apresentada uma conclusão deste na secção 5.4.

5.1. Testbed

De forma a tornar possível a obtenção de um conjunto de métricas torna-se necessário o desenvolvimento de um cenário capaz de suportar vários tipos de tecnologias para a realização do *handover*.

As tecnologias a suportar são:

- Wi-Fi
- WiMAX
- 3G

A tecnologia Ethernet apenas poderá ser utilizada aquando do uso do portátil como terminal móvel devido ao telemóvel não suportar esta tecnologia.

Pela Figura 5.1-1 podemos visualizar a esquematização da *testbed* implementada.

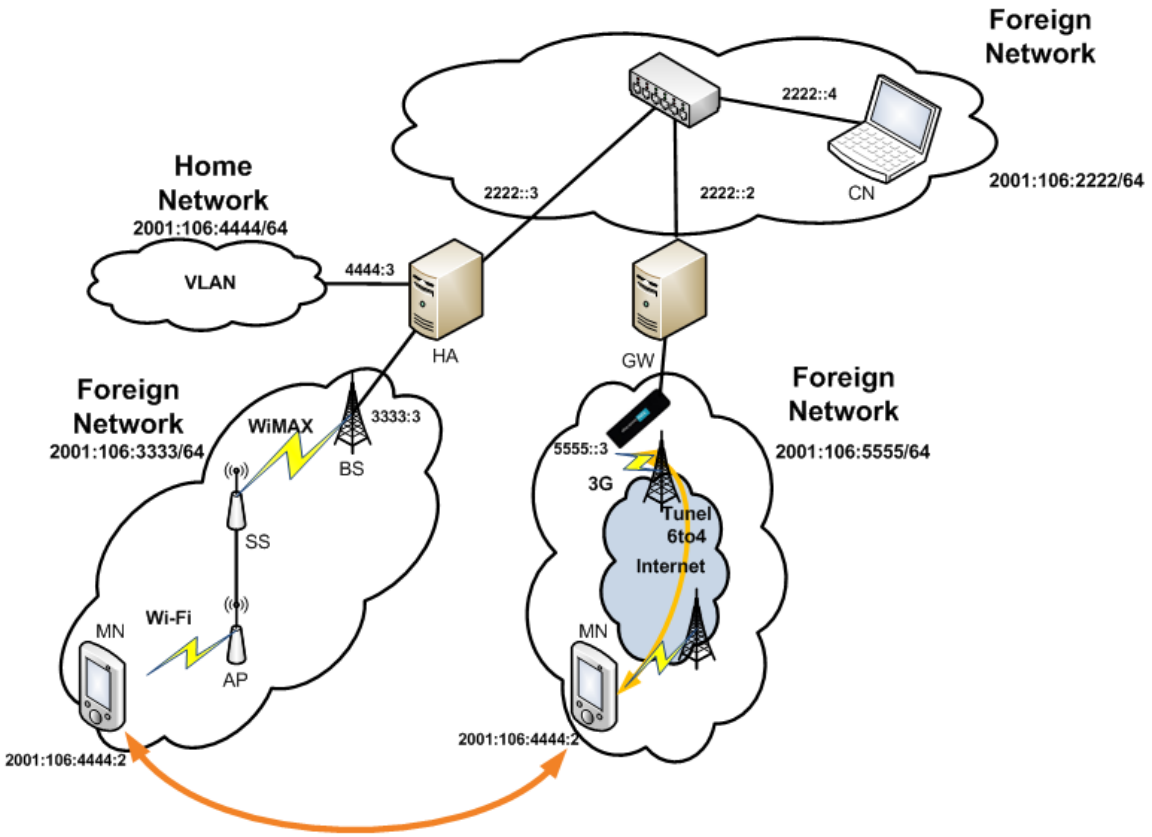

Figura 5.1-1: Esquema da *testbed* implementada – *handover* de FN para FN

Como se pode observar pela Figura 5.1-1, a *testbed* é composta por quatro redes distintas:

- A rede onde se encontra o *Correspondent Node*, o qual é utilizado para comunicar com o *Mobile Node* de forma a podermos gerar tráfego na rede.

- A rede *Home Network*, onde é registado o MN e onde se encontra o seu *Home Agent*, responsável por toda a gestão de mobilidade para que o MN se encontre sempre alcançável pelas restantes redes.

- Uma *Foreign Network* que proporciona um acesso via Wi-Fi. Como *backbone* desta rede é utilizada uma ligação WiMAX fixa composta por uma *Base Station* e uma *Subscriber Station* conectada ao *Access Point* do Wi-Fi. Neste caso o WiMAX é utilizado para permitir a reserva de fluxos.

- Uma *Foreign Network* que proporciona acesso a uma rede comercial da TMN 3G utilizando endereçamento IPv4. Com a utilização da rede 3G surgiram alguns inconvenientes relativos ao espaço de endereçamento. Dado que estamos a efectuar todo o estudo utilizando como espaço de endereçamento o IPV6 e dado que o 3G ainda utiliza o espaço de endereçamento IPv4, torna-se incompatível a comunicação entre ambos. Para contornar este problema foi necessário efectuar a implementação de um túnel do *GateWay* para o *Mobile Node*. O túnel implementado é do tipo 6to4 de forma a

permitir a comunicação de duas redes IPv6 (redes do *GateWay* e do *Mobile Node*) através de uma rede IPv4 (3G). A necessidade deste túnel vai de certo modo afectar os tempos de *handover* devido à necessidade de mais processamento por parte do GW e do MN para encapsular e desencapsular os pacotes.

Relativamente aos componentes utilizados e ao suporte a nível de software temos:

- *Home Agent* – Computador com sistema operativo UBUNTU 9.04 a correr o kernel 2.6.30 com suporte ao protocolo MIPv6.
    - IEEE 802.21
    - UMIP
    - WiMAX QoS Manager
    - *Mobility Manager*

- *Mobile Node* – Telemóvel (HTC Google Nexus One) com sistema operativo Android OS versão 2.1 e um Kernel Linux 2.6.32.9, também este com suporte ao protocolo MIPv6 e aos túneis *IPv6-in-IPv4.* Este terminal tem ainda a particularidade de poder ter múltiplas interfaces activas, 3G e Wi-Fi, bem como várias ligações activas em simultâneo. As entidades presentes neste terminal são:
    - IEEE 802.21
    - UMIP
    - *Mobility Manager*
    - D-ITG

- *GateWay* - Computador com sistema operativo UBUNTU 9.04 a correr o kernel 2.6.30.
    - IEEE 802.21
    - *Information Server*

- *Correspondent Node* - Computador com sistema operativo UBUNTU 9.04. Este contém as entidades:
    - UMIP
    - D-ITG

    Esta entidade suporta MIPv6 para que seja possível a optimização de rota.

Com esta *testbed* vão ser efectuados os seguintes tipos de *handover*:

- *Handover* de Wi-Fi para 3G
- *Handover* de 3G para Wi-Fi

A realização dos *handovers* mencionados, tal como se pode observar pela Figura 5.1-1, vão ser efectuados sempre de FN para FN no qual serão obtidas todas as métricas referidas ao longo desta dissertação para os vários casos. Para o caso das métricas indicadas para o IEEE 802.21, ou

seja, as várias fases de *handover* por este executado, apenas será apresentada a fase de execução.

Embora ao longo desta dissertação todos os processos apresentados tenham em conta tanto a utilização de um computador como a de um telemóvel como terminal móvel, a obtenção de dados será apenas efectuada para o caso de se ter um telemóvel como terminal móvel. Esta opção deve-se ao facto de se tratar de uma análise mais realista e devido à utilização do computador não acrescentar informação relevante, pois acrescia apenas a capacidade de realização de *handover* entre a rede Ethernet. Um factor condicionante a esta opção deve-se também ao facto de a implementação do protocolo IEEE 802.21 utilizada apenas suportar eventos reais a nível da camada L2 para o caso do telemóvel; no caso do computador estes teriam de ser simulados.

Para que seja possível a obtenção de métricas para os mesmos tipos de *handover* já mencionados, mas agora considerando que são efectuados da HN para uma FN e de uma FN para a HN, foi necessário proceder a algumas modificações na *testbed* da Figura 5.1-1, tal como se pode visualizar Figura 5.1-2.

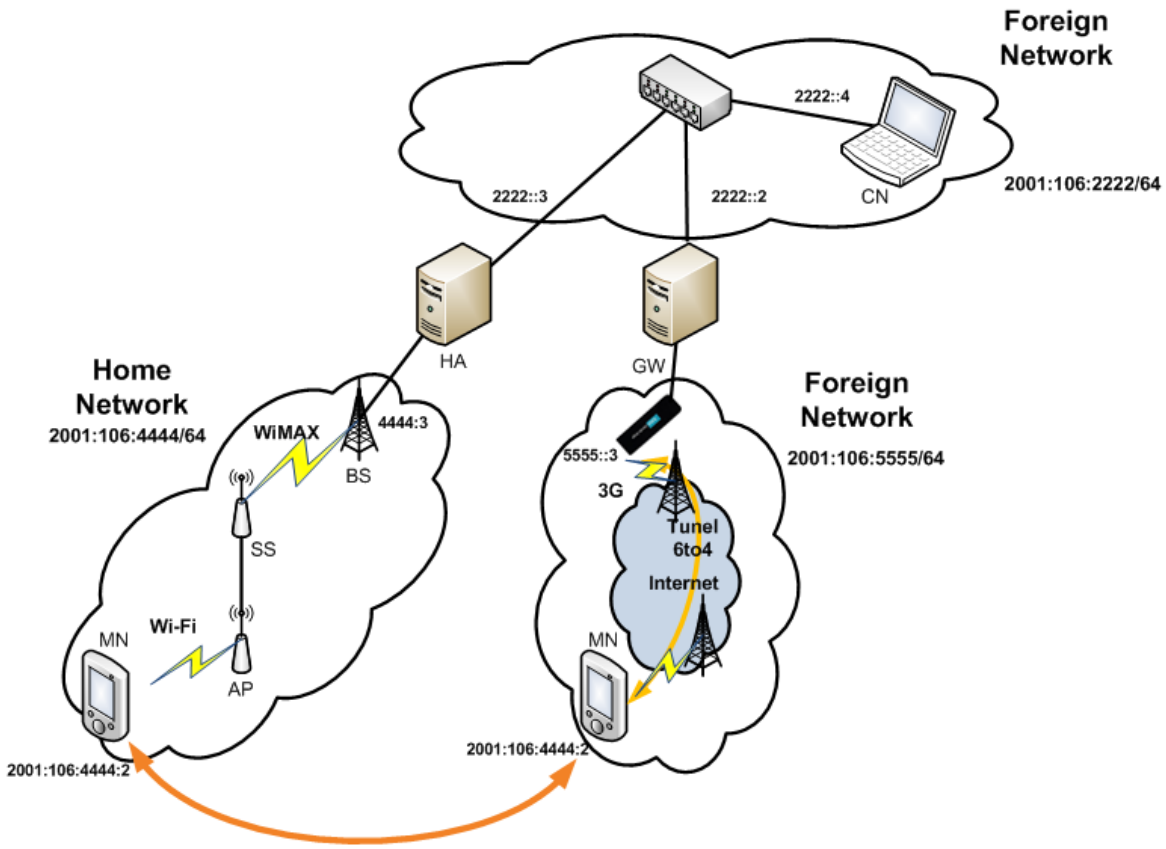

Figura 5.1-2: Esquema da *testbed* implementada – *handover* de HN para FN e de FN para HN

Neste caso serão apenas apresentados os resultados da utilização das modificações implementadas, utilizando o IEEE 802.21 para iniciar o processo de *handover*, e sem se proceder à optimização de rota, devido aos restantes casos terem uma análise análoga.

5.2. Metodologias

Para que seja possível efectuar uma análise mais pormenorizada e de forma a podermos identificar e realçar todas as vantagens das modificações efectuadas, as métricas vão ser obtidas para diferentes casos, nomeadamente:

- Obtenção de métricas sem a implementação das modificações, ou seja, com a implementação original do protocolo de mobilidade. Neste caso as métricas relativas ao protocolo IEEE 802.21 não se vão poder obter devido a não existir comunicação com o UMIP.

- Obtenção das métricas com a execução do *handover* iniciado pelo IEEE 802.21 mas sem optimização de rota.

- Obtenção das métricas com a execução do *handover* iniciado pelo IEEE 802.21 e com optimização de rota.

Em cada um destes casos indicados as métricas serão obtidas para diferentes tipos de tráfego efectuando para cada um deles 10 *handovers,* nos quais serão obtidas 30 amostras (antes, durante e após o *handover)* durante 10 segundos. Todos os intervalos de confiança apresentados são de 95%.

Para além dos casos mencionados convém ter em atenção os diferentes tipos de *handover* possíveis:

- *Handover* da HN para a FN.
- *Handover* da FN para outra FN.
- *Handover* da FN para a HN.

Estes três tipos de *handover* são relevantes, pois em cada um deles são efectuados processos diferentes, o que vem de um certo modo afectar os tempos referentes às métricas.

Sempre que se efectua um *handover* da HN para uma FN, é necessário efectuar um proxy *Duplicate Address Detection* (DAD) de forma a garantir que o prefixo da rede móvel é único, seguido de um DAD para que o endereço atribuído ao MN não seja duplicado.

Para o caso de se tratar de um *handover* de uma FN para outra FN, apenas é necessário efectuar o DAD, dado que a unicidade do endereço móvel já está garantida.

Quando o MN regressa à sua HN não é necessário efectuar qualquer tipo de verificações, dado que o HA "protege" sempre o *Home Address* do MN.

Para além destas diferenças existem ainda processos diferentes no que diz respeito à intercepção de pacotes por parte do HA bem como à utilização do túnel entre o MN e o HA, sendo estas apresentadas ao longo da secção 5.3.

5.2.1. Geração de Tráfego

A geração de tráfego será sempre efectuada do CN para o MN (*downlink*), sendo que este é controlado através do programa de métricas mencionado na secção 4.4. Para a geração do tráfego é utilizado o software D-ITG.

Sempre que se pretender iniciar a obtenção das métricas com a presença de tráfego, o MN irá indicar ao servidor desenvolvido no CN para que este inicie o envio de tráfego. Como processo principal, este executa a seguinte *systemcall*: *ITGSend script.s*

Por sua vez, este comando irá utilizar um *script* previamente configurado de forma a definir o tipo de tráfego que se pretende enviar.

Através da Tabela 1 é possível apresentar algumas das principais características de cada tráfego, a nível de valores médios.

Tipo de tráfego	*Bitrate* (Kbit/s)	Taxa de pacotes (pkt/s)
Vídeo	128	16
Vídeo	256	32
Vídeo	512	64
Vídeo	1024	128
Quake3	74	146
VoIP	70	50
FTP	128	16

Tabela 1: Tráfego utilizado para obtenção de métricas – valores médios

5.3. Resultados

Nesta secção é apresentado um conjunto de métricas já mencionadas na secção 3.4 para diversos tipos de *handover* e diferentes tipos de tráfego (secção 5.2). Esta análise é apresentada para a realização de *handover* entre as tecnologias Wi-Fi e 3G de forma a quantificar este processo e efectuar uma análise, a nível de QoS e QoE, referente a todos os passos que envolvem este processo.

Todos os dados apresentados são obtidos na presença do tráfego indicado e usando como terminal móvel o telemóvel (HTC Google Nexus One).

5.3.1. *Handover* de *Foreign Network* para *Foreign Network*

Através desta secção são apresentados todos os valores obtidos a nível do UMIP sem suporte IEEE 802.21, com suporte IEEE 802.21, o tempo da fase de execução do IEEE 802.21 e os valores de QoS e QoE. A *testbed* utilizada para a obtenção destes valores é a apresentada na Figura 5.1-1.

5.3.1.1. UMIP

Nesta subsecção apenas são apresentadas as métricas referentes ao processo do UMIP para três situações distintas: através da utilização do UMIP sem suporte IEEE 802.21, ou seja, sem modificações; através da utilização do UMIP com suporte IEEE 802.21 e sem optimização de rota; através da utilização do UMIP com suporte IEEE 802.21 e com optimização de rota.

5.3.1.1.1. UMIP sem Suporte IEEE 802.21

Para que se possa ter um termo de comparação relativamente aos tempos de *Handover Delay*, *Handover Execution Delay* e número de pacotes perdidos, procedeu-se à obtenção destes utilizando a implementação original do protocolo de mobilidade. Deste modo será possível demonstrar toda a necessidade e importância das modificações implementadas para utilizar o IEEE 802.21 como suporte ao processo de *handover*.

Handover Delay:

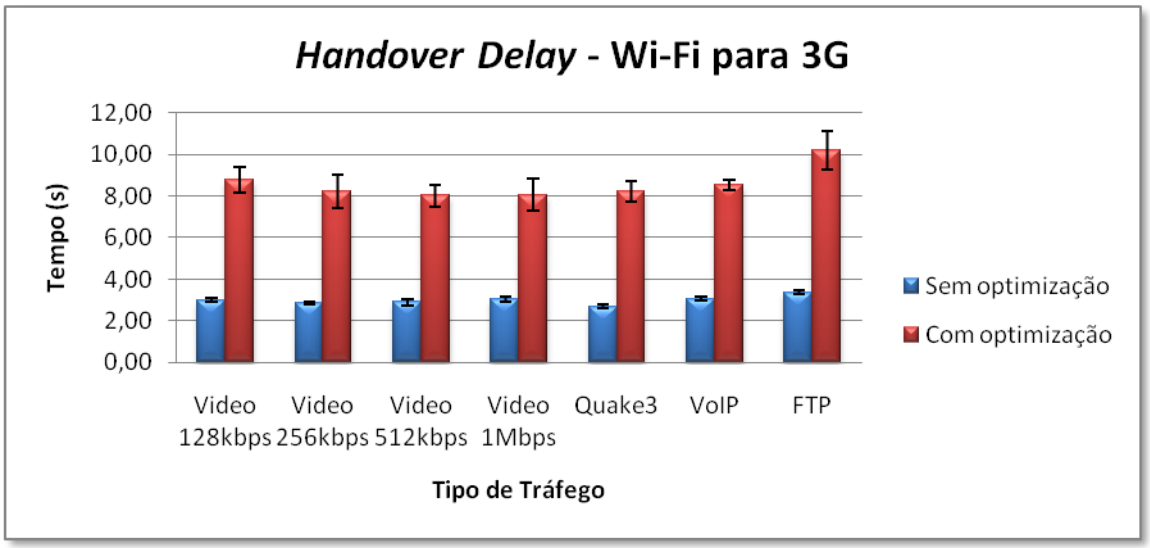

Figura 5.3.1.1.1-1:UMIP sem suporte IEEE 802.21 - *Handover Delay* de Wi-Fi para 3G

Observando a Figura 5.3.1.1.1-1 que apresenta o *Handover Delay* para vários tipos de tráfego pode-se notar uma discrepância grande entre o caso de termos optimização de rota e o caso de não termos optimização de rota. Para o caso de não termos optimização de rota, após se quebrar a ligação da rede onde se encontra o MN, este terá inicialmente de detectar a perda de ligação ou de receber uma indicação vinda da camada de ligação. Estando a detecção de movimentação por parte do MN efectuada procede-se à aquisição do novo CoA e actualização deste no respectivo HA. Após este processo é então recebido o primeiro pacote pela nova interface do MN.

Para o caso de se ter optimização de rota é acrescentado mais um processo ao caso de não termos optimização. Neste caso, após se enviar o BU para o HA a indicar o novo CoA, é iniciado o processo de optimização de rota já mencionada anteriormente.

Convém referir que para o caso de não se ter as modificações implementadas, existe o problema com a optimização de rota já referido na secção 4.1.3

Handover Execution Delay

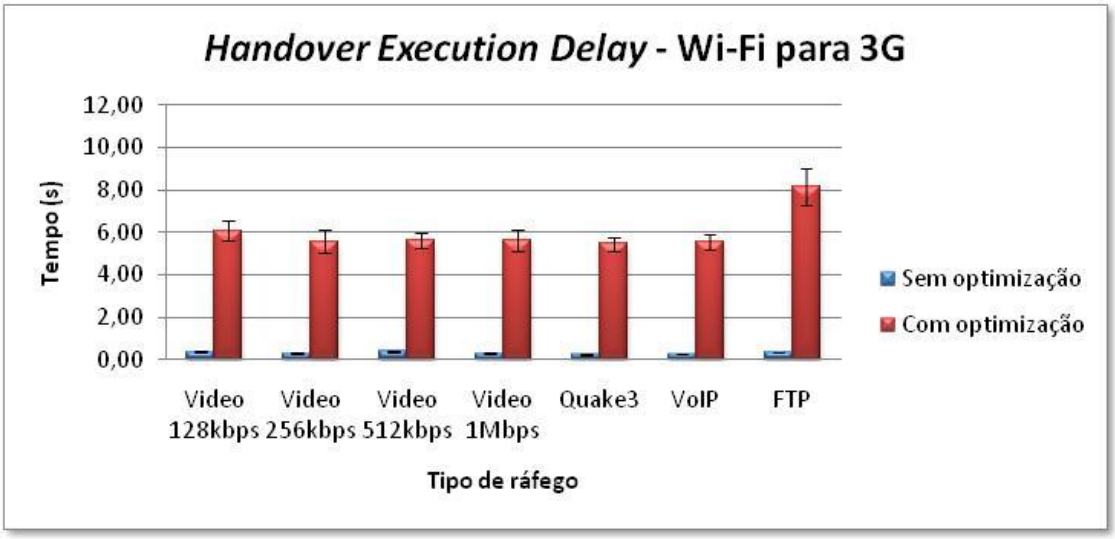

Figura 5.3.1.1.1-2: UMIP sem suporte IEEE 802.21 - *Handover Execution Delay* de Wi-Fi para 3G

Relativamente ao *Handover Execution Delay,* presente na Figura 5.3.1.1.2-2, comparando os gráficos com optimização e sem optimização, mais uma vez se pode notar uma grande discrepância entre ambos, sendo que a justificação a esta situação é a mesma que foi apresentada para o caso do *Handover Delay.*

Comparando a Figura 5.3.1.1.1-1 e a Figura 5.3.1.1.1-2, no caso de não se ter optimização de rota pode-se concluir que o processo de detecção de movimentação e de obtenção do novo CoA são os maiores "responsáveis" pelo tempo de *Handover Delay,* uma vez que desde o BU para o HA até à recepção do primeiro pacote pela nova interface (*Handover Execution Delay*) temos um tempo muito inferior a este. Para o caso da optimização de rota ocorre a situação inversa, sendo que o tempo de detecção de movimentação e obtenção do novo CoA é menor que o de envio do BU para o HA até à recepção do primeiro pacote pela nova interface, mais uma vez devido ao

processo de optimização. Neste caso, de forma a demonstrar que os resultados se apresentam coerentes, pode-se observar o facto de o *Handover Execution Delay* ser aproximadamente o valor de *Handover Delay* com optimização menos o tempo de detecção de movimentação e obtenção de endereço, que é aproximadamente a diferença entre o *Handover Delay* e *Handover Execution Delay* sem optimização de rota.

Para os vários tipos de tráfego é observável que tanto o *Handover Delay* como o *Handover Execution* Delay se mantém aproximadamente constantes com a excepção do caso do FTP. Neste caso, devido a se estar mais tempo sem ligação, existe maior perda de pacotes, o que faz com que o FTP, uma vez que é TCP, reduza o número de pacotes por segundo, aumentando a probabilidade de se capturar o primeiro pacote pela nova interface do MN mais tardiamente.

Pacotes Perdidos:

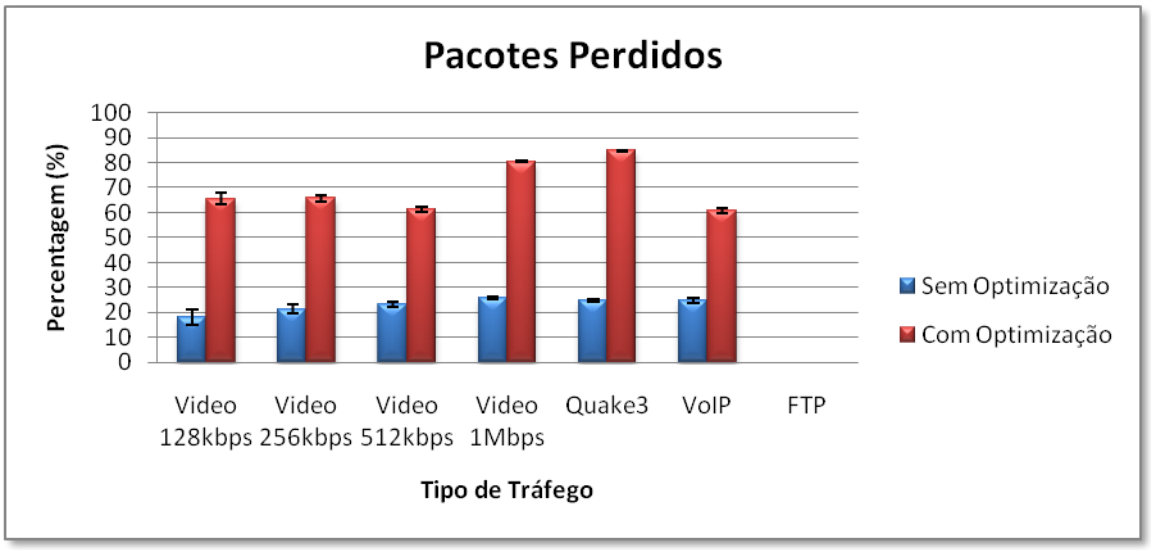

Figura 5.3.1.1.1-3: UMIP sem suporte IEEE 802.21 - Percentagem de pacotes perdidos

Relativamente à percentagem de pacotes perdidos (Figura 5.3.1.1.1-3), tal como era esperado, existem mais perdas para o caso de termos optimização de rota, uma vez que é nesta situação que estamos mais tempo sem ligação.

Analisando os vários tipos de tráfego é possível observar que independentemente do tráfego as percentagens de perdas mantêm-se aproximadamente constantes.

No caso do FTP não existem perdas devido a se tratar de um tráfego TCP, ou seja, este sempre que um pacote é perdido torna a reenviá-lo, permitindo deste modo que não existam efectivamente perdas.

Para uma melhor visualização dos momentos de obtenção tanto do *Handover Delay* como do *Handover Execution Delay* bem como dos principais procedimentos efectuados temos a Figura 5.3.1.1.1-4.

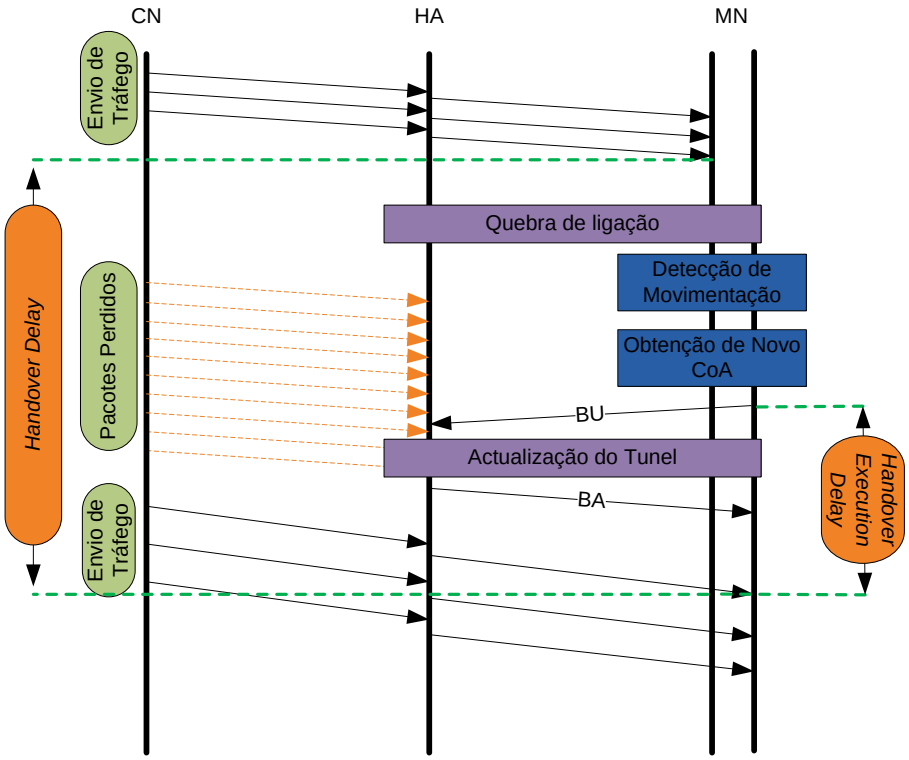

Figura 5.3.1.1.1-4: Exemplo de *Handover* de Wi-Fi para 3G sem suporte IEEE 802.21 e sem optimização de rota – Principais Processos

5.3.1.1.2. *Handover* Iniciado pelo IEEE 802.21 e sem Optimização de Rota

Handover Delay:

Analisando a Figura 5.3.1.1.2-1 podemos realçar a grande discrepância a nível de *Handover Delay* existente entre o *handover* de 3G para Wi-Fi e de Wi-Fi para 3G

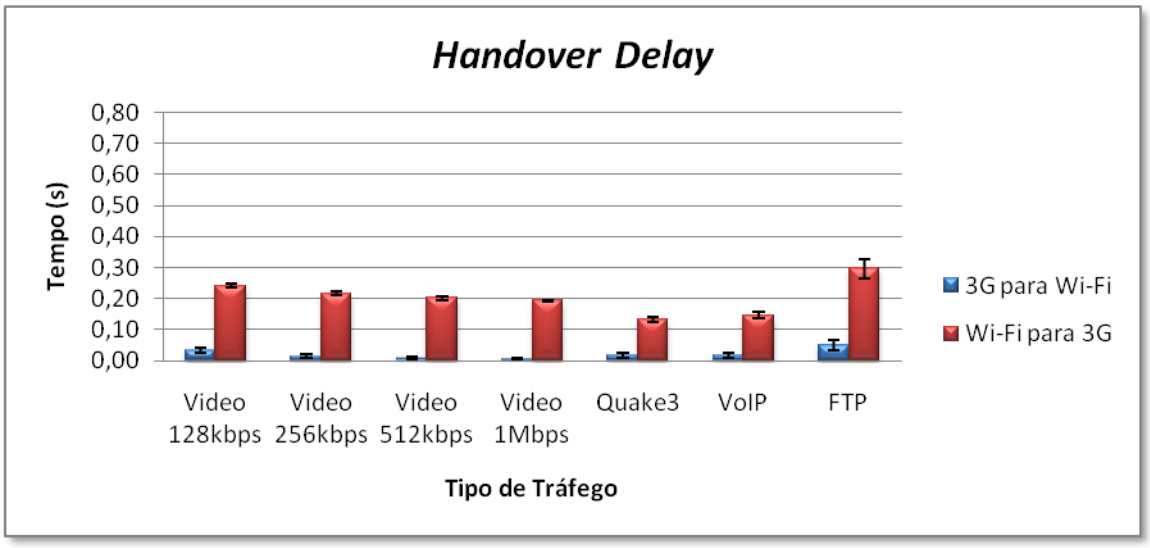

Figura 5.3.1.1.2-1: *Handover Delay* - sem optimização de rota

Esta diferença prende-se com o facto de na rede 3G termos um *delay* muito maior do que na rede Wi-Fi. Considerando o *Handover* de 3G para Wi-Fi, após a sua execução o MN continua a receber os pacotes pela interface antiga até que a nova interface possa ser utilizada. Como a rede 3G tem um maior *delay*, o último pacote recebido pelo MN será capturado mais tarde, comparativamente com o Wi-Fi. Após se ter a interface do Wi-Fi totalmente configurada, e sabendo que esta tem um menor *delay,* o primeiro pacote capturado pelo MN será mais rápido, comparativamente com o caso do 3G. Este processo torna o *Handover Delay* para o caso do *handover* de 3G para Wi-Fi muito menor do que no caso de Wi-Fi para 3G, sendo que a justificação para este último é a inversa à indicada.

Com a existência de perda de pacotes, tanto o tempo de *Handover Delay* como o tempo de *Handover Execution Delay* tornam-se muito dependentes do facto da perda existente ser referente ao último pacote da interface antiga ou ao primeiro da interface nova.

Pode-se observar que quanto maior for a taxa de pacotes (pkt/s), menor é o tempo de *handover delay*. Este comportamento era o esperado pois aumentando o número de pacotes por segundo torna-se mais tardia a captura do último pacote pela interface antiga, e mais rápida a captura do primeiro pacote pela nova interface.

Comparando o tráfego FTP com o vídeo 128kbps pode-se notar que, embora o FTP tenha a mesma taxa de pacotes por segundo, aproximadamente, este tem um maior tempo de *Handover Delay,* causado pelo maior *delay* e *jitter*. O FTP, ao se aperceber que está a perder pacotes diminui a taxa de envio destes, influenciando deste modo o tempo de *Handover Delay.*

Um ponto a ter em consideração é o facto de não termos qualquer tipo de controlo na rede 3G, estando limitados ao estado actual, a nível de qualidade, a que ela se encontra no momento de cada medição.

Handover Execution Delay:

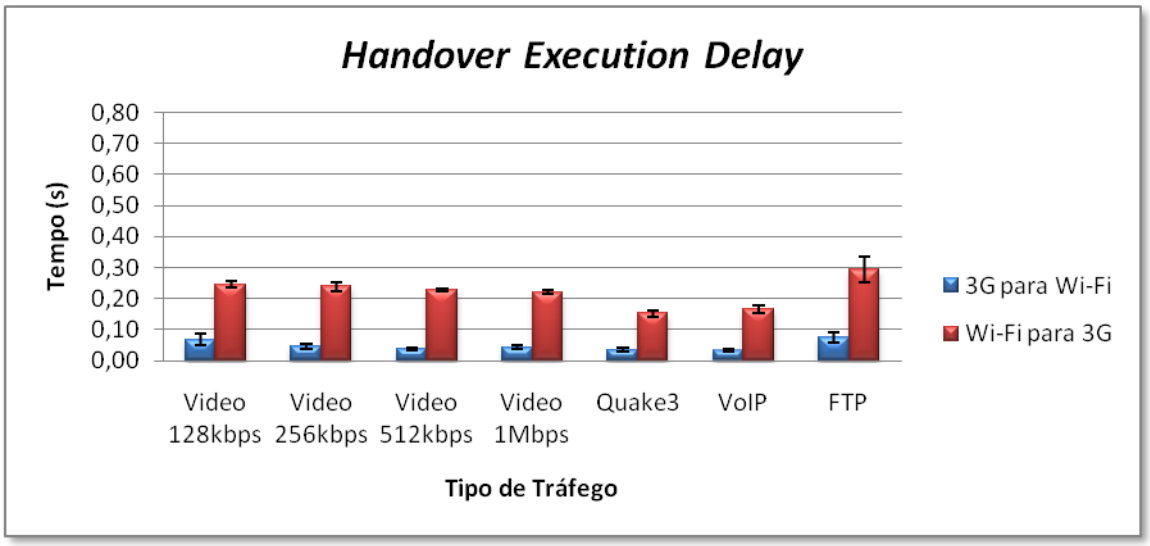

Figura 5.3.1.1.2-2: *Handover Execution Delay* - sem optimização de rota

Para os tempos de *Handover Execution Delay* é esperado que estes sejam superiores aos tempos de *Handover Delay*, o que de facto se pode confirmar pela Figura 5.3.1.1.2-2. Esta diferença de tempos é causada pelo facto do *Handover Execution Delay* não depender da recepção do último pacote pela interface antiga, mas sim do envio do BU por parte do MN para o HA.

As diferenças de tempos entre os dois tipos de *handover* continuam a ser causadas pela discrepância entre os *delays* das duas tecnologias, mas agora apenas devido à recepção do primeiro pacote pela nova interface, que será mais demorada aquando da realização do *handover* de Wi-Fi para 3G.

Através da Figura 5.3.1.1.2-3 são apresentados os principais processos efectuados para o caso de se ter a implementação das modificações e não se ter a optimização de rota. Neste caso é ainda possível identificar o instante de obtenção tanto do *Handover Delay* como do *Handover Execution Delay.*

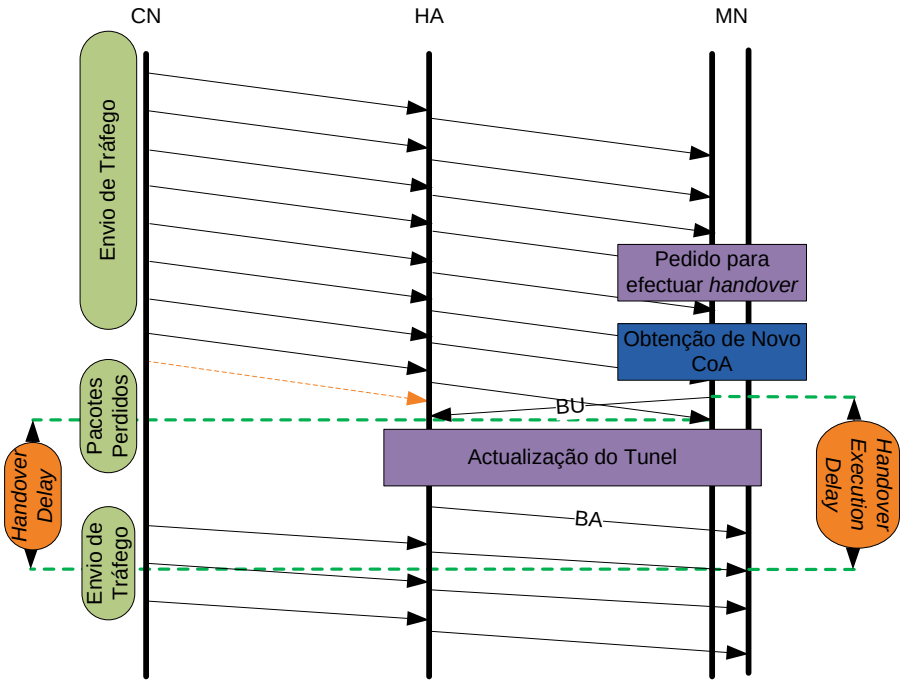

Figura 5.3.1.1.2-3: Exemplo de *Handover* de 3G para Wi-Fi iniciado pelo IEEE 802.21 e sem optimização de rota – Principais Processos

5.3.1.1.3. *Handover* Iniciado pelo IEEE 802.21 e com Optimização de Rota

Handover Delay:

Comparando os valores de *Handover Delay* com optimização de rota, Figura 5.3.1.1.3-1, e sem optimização de rota (Figura 5.3.1.1.2-1) pode-se concluir, como já era esperado, que não existe grande discrepância entre estes. Embora seja necessário mais tempo para efectuar a o processo de optimização o MN continua a receber pacotes pela interface antiga, não afectando de forma significativa o *Handover Delay*.

A restante análise é análoga ao caso em que não existe optimização de rota.

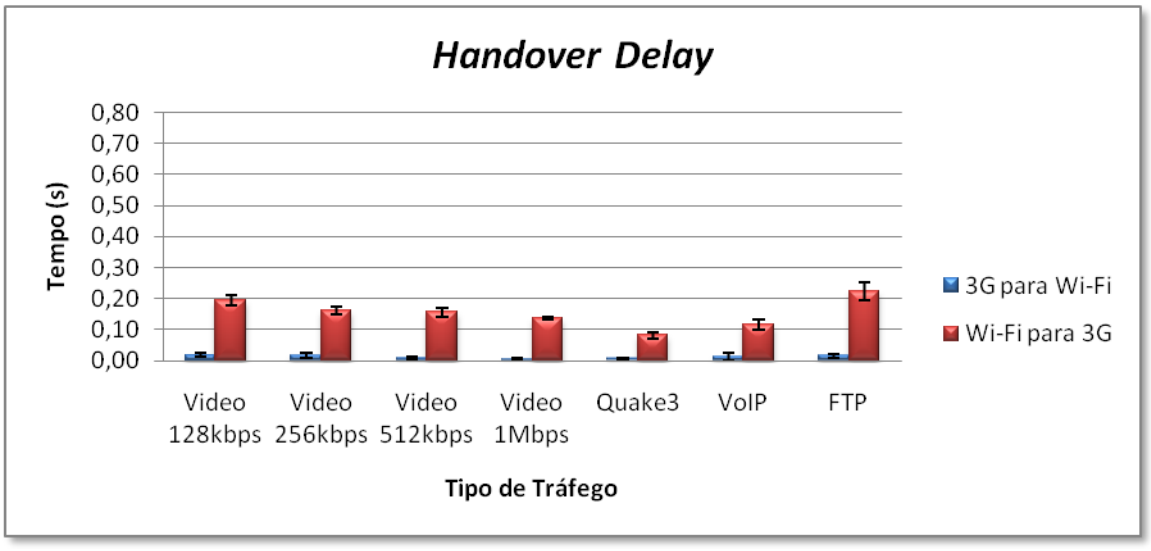

Figura 5.3.1.1.3-1: *Handover Delay* - com optimização de rota

Handover Execution Delay:

Para o caso do *Handover Execution Delay* com optimização de rota, Figura 5.3.1.1.3-2, comparativamente ao caso em que a optimização de rota não existe (Figura 5.3.1.1.2-2), este irá sofrer alterações significativas devido à fase de optimização de rota, que tarda a recepção do primeiro pacote pela nova interface.

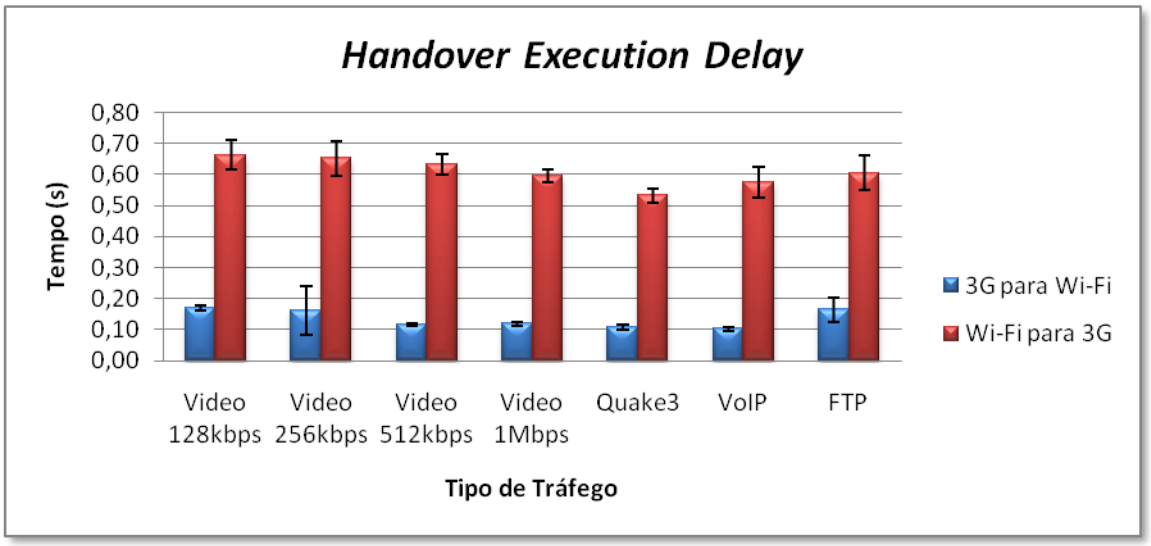

Figura 5.3.1.1.3-2: *Handover Execution Delay* - com optimização de rota

Através da Figura 5.3.1.1.3-3 pode-se visualizar os principais processos executados bem como o instante de obtenção dos tempos para o caso de se ter optimização de rota e para o caso de se ter as modificações implementadas.

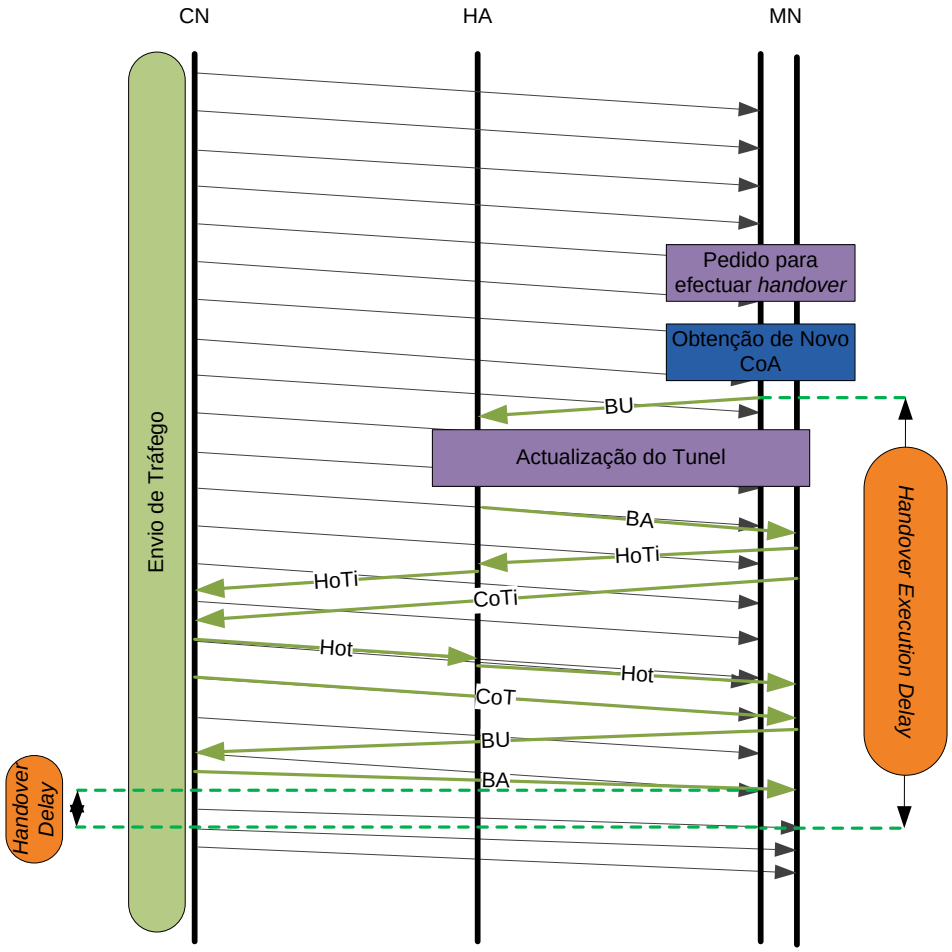

Figura 5.3.1.1.3-3: Exemplo de *Handover* de Wi-Fi para 3G iniciado pelo IEEE 802.21 e com optimização de rota – Principais Processos

Comparando os valores obtidos relativamente ao caso do UMIP não ter suporte ao IEEE 802.21 com o caso de este ter suporte ao IEEE 802.21, pode-se observar que existe uma grande discrepância entre estes dois casos, tornando-se possível justificar a necessidade do UMIP interagir com o IEEE 802.21. Relativamente ao caso de se iniciar o *handover* no UMIP através IEEE 802.21, tanto a nível de *Handover Delay* e *Handover Execution Delay* pode-se observar uma descida acentuada destes, independentemente de se estar sem optimização de rota ou com optimização de rota, sendo que para este ultimo caso a diferença ainda se torna mais acentuada.

5.3.1.2. IEEE 802.21: Fase de Execução

Nesta subsecção é apresentado os tempos envolventes em uma das quatro fases efectuadas pelo IEEE 802.21, a fase de execução.

O tempo da fase de execução (Figura 5.3.1.2-1) toma em consideração o tempo desde o pedido para efectuar *handover,* efectuado pelo MM presente no HA, até à recepção de uma confirmação enviada pelo MM presente no MN ao MM no HA.

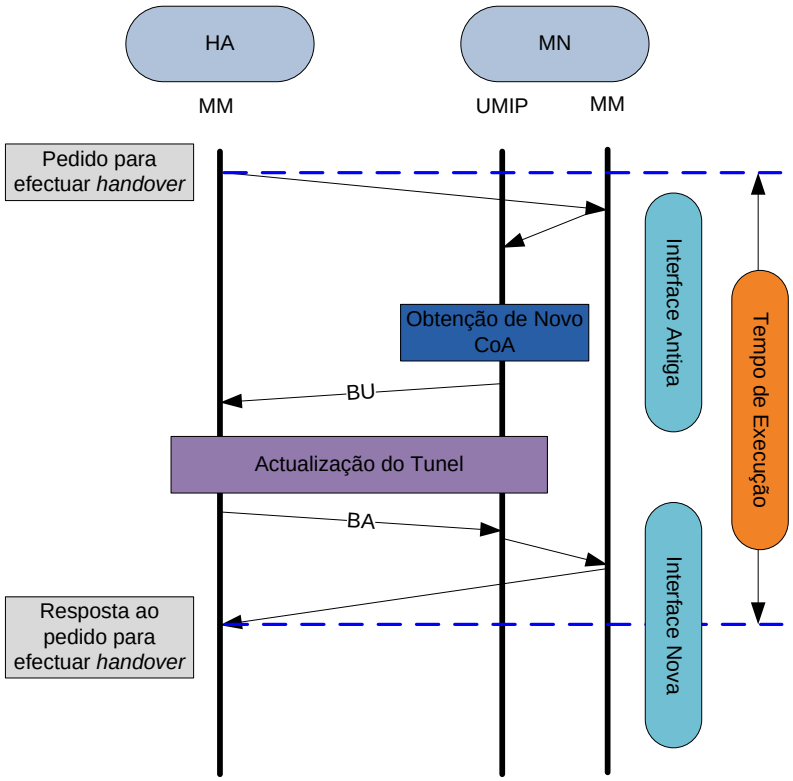

Figura 5.3.1.2-1: Tempo da fase de Execução

5.3.1.2.1. Tempo da Fase de Execução sem Optimização de Rota

Através da Figura 5.3.1.2.1-1 pode-se visualizar os tempos da fase de execução com a presença de diversos tipos de tráfego. Estes são referentes ao caso de se realizar *handover* de 3G para Wi-Fi e de Wi-Fi para 3G, respectivamente, e sem se considerar a utilização de optimização de rota.

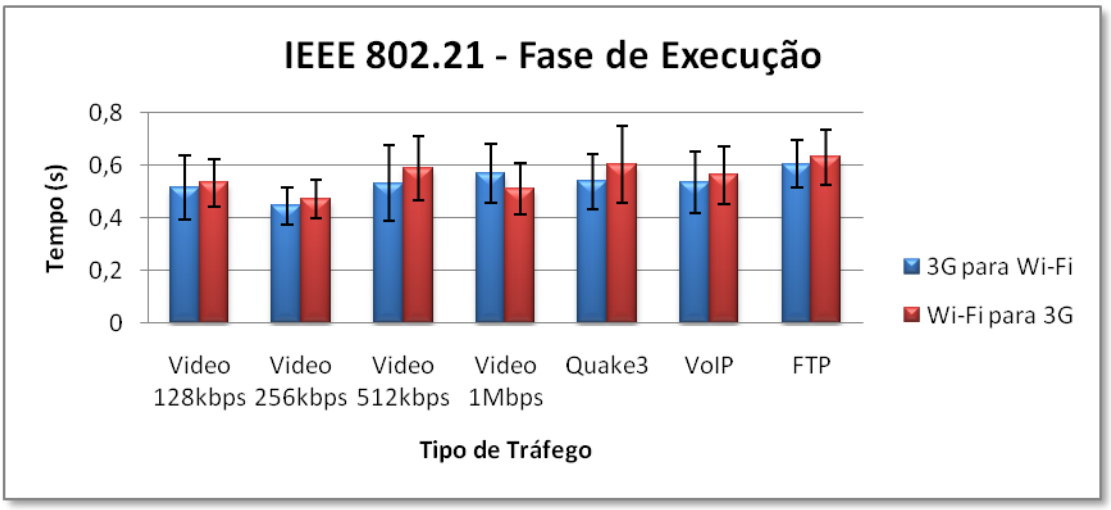

Figura 5.3.1.2.1-1: IEEE 802.21- Tempo de execução de *handover* sem optimização de rota

Dado que a mensagem de pedido de *handover* é enviada pela interface antiga e a resposta pela nova interface, e sabendo que o BA é enviado pela interface para a qual é efectuado o *handover,* é de esperar que os tempos de execução sejam aproximadamente iguais.

5.3.1.2.2. Tempo da Fase de Execução com Optimização de Rota

A análise à Figura 5.3.1.2.2-1 é análoga ao caso da Figura 5.3.1.2.1-1. De notar o facto de os tempos, por norma, serem ligeiramente menores, devendo-se ao facto da troca de mensagens e tráfego passar a ser efectuada directamente com o MN, não congestionando tanto o HA.

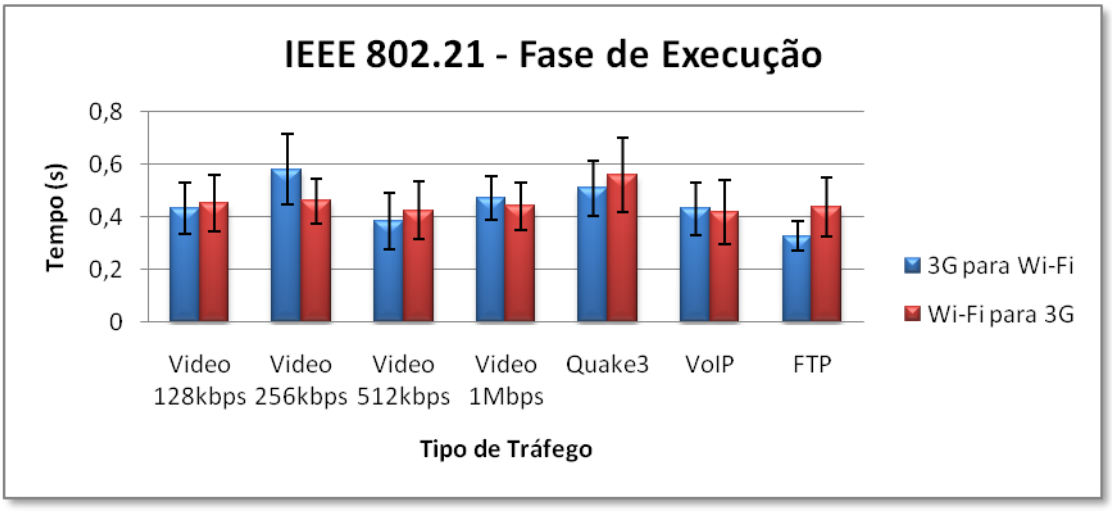

Figura 5.3.1.2.2-1: Tempo de execução de *handover* de 3G para Wi-Fi com optimização de rota

5.3.1.3. Métricas de QoS para *Handover* Iniciado pelo IEEE 802.21

Nesta subsecção são apresentadas as métricas referentes ao QoS para os vários tipos de tráfego em análise, sendo estas obtidas durante a execução do respectivo *handover* com o auxilio do IEEE 802.21. Neste caso tem-se em consideração a utilização ou não da optimização de rota para a realização de *handover* de 3G para Wi-Fi e de Wi-Fi para 3G, considerando que este é executado de uma FN para outra FN.

5.3.1.3.1. Métricas sem Optimização de Rota

Delay:

Através da Figura 5.3.1.3.1-1, Figura 5.3.1.3.1-2, Figura 5.3.1.3.1-3 e Figura 5.3.1.3.1-4 pode-se observar o *delay* obtido durante a execução do *handover* sem optimização de rota para os vários tipos de tráfego.

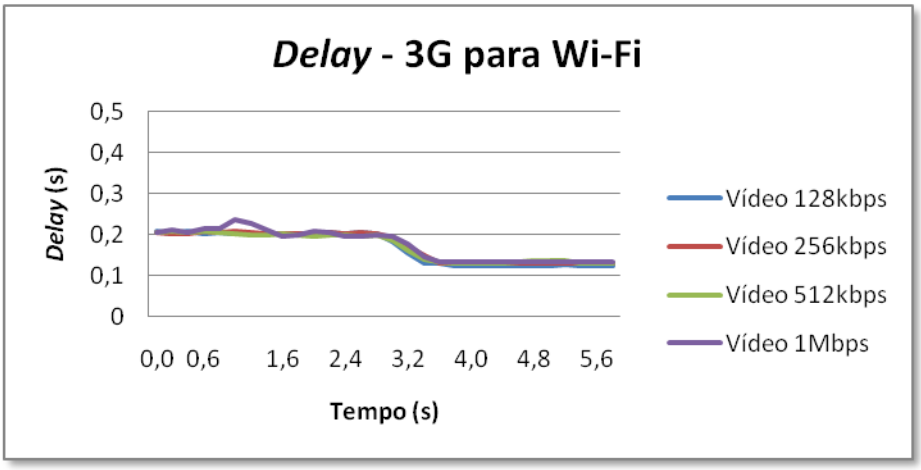

Figura 5.3.1.3.1-1: Tráfego de vídeo – *Delay* (3G para Wi-Fi sem optimização de rota)

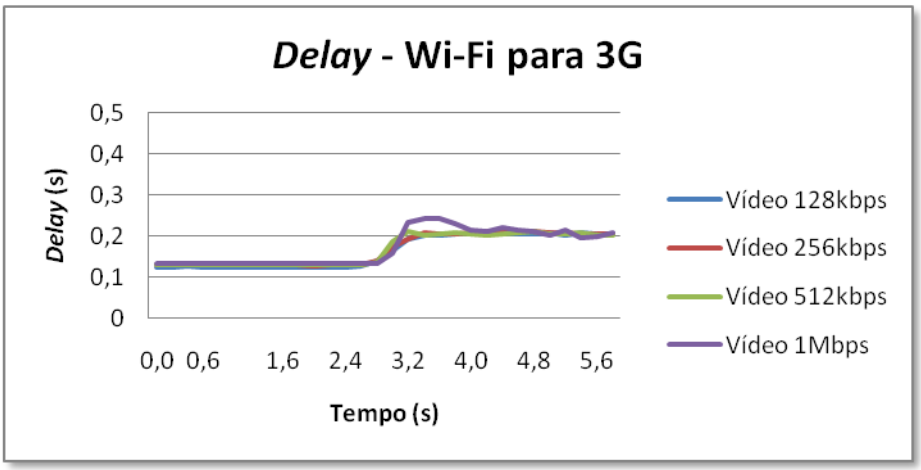

Figura 5.3.1.3.1-2: Tráfego de vídeo – *Delay* (Wi-Fi para 3G sem optimização de rota)

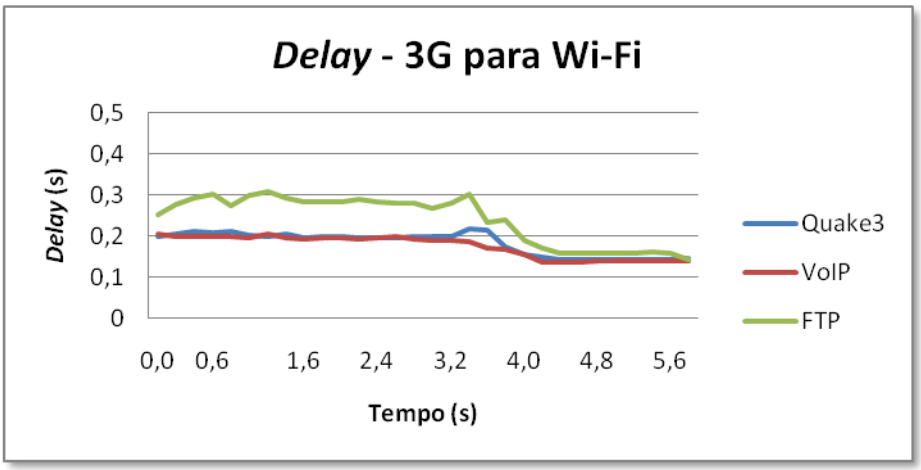

Figura 5.3.1.3.1-3: Quake3/VoIP/FTP – *Delay* (3G para Wi-Fi sem optimização de rota)

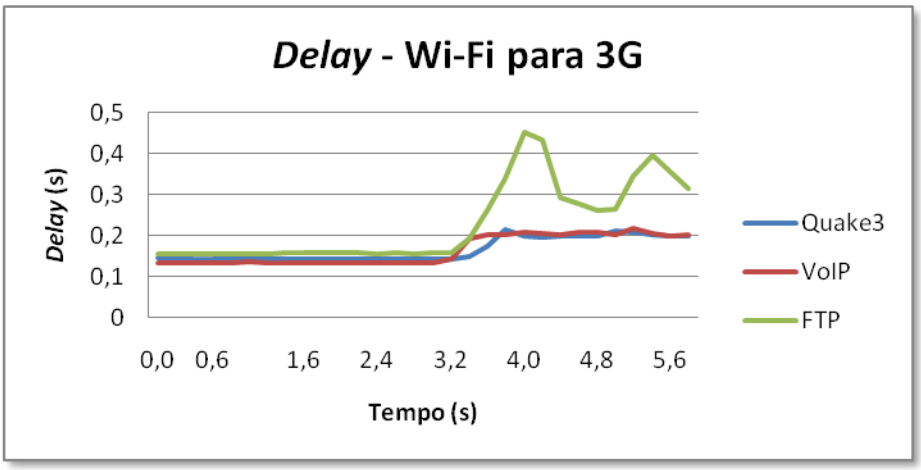

Figura 5.3.1.3.1-4: Quake3/VoIP/FTP – *Delay* (Wi-Fi para 3G sem optimização de rota)

Como era esperado, o *delay* em todos os tipos de tráfego é superior no caso da rede 3G, podendo-se distinguir facilmente o instante de execução do *handover*.

Para o caso do tráfego FTP pode-se destacar a grande variação existente após este entrar na rede 3G, a qual se justifica pela perda de pacotes existentes.

Jitter:

Seguidamente são apresentados os gráficos do *Jitter* através da Figura 5.3.1.3.1-5 e Figura 5.3.1.3.1-6 para as mesmas circunstâncias do *delay*.

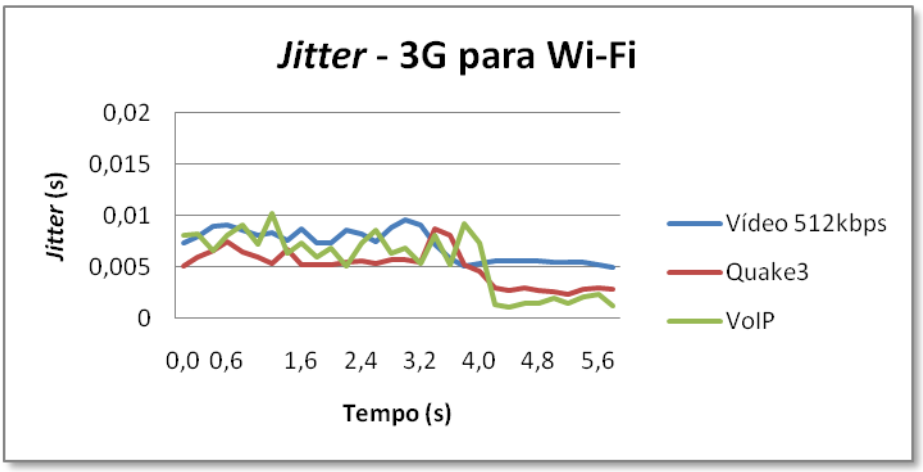

Figura 5.3.1.3.1-5: Vídeo 512kbps/Quake3/VoIP – *Jitter* (3G para Wi-Fi sem optimização de rota)

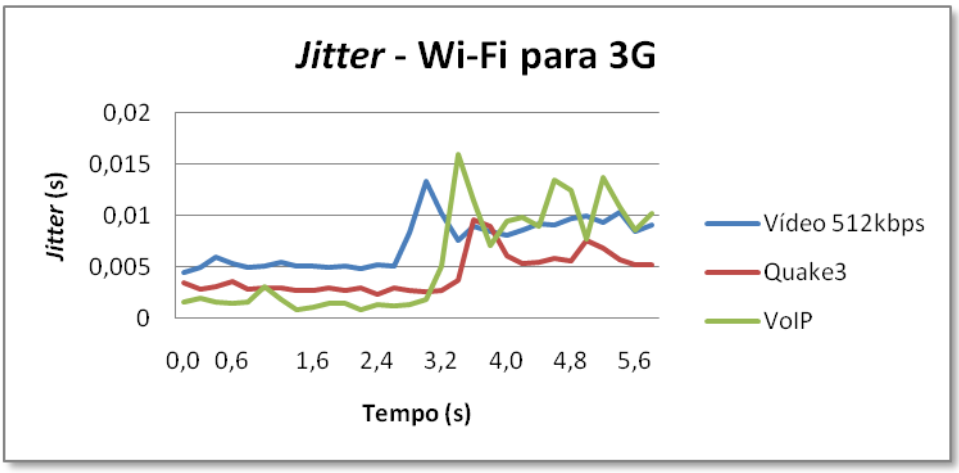

Figura 5.3.1.3.1-6: Vídeo 512kbps/Quake3/VoIP – *Jitter* (Wi-Fi para 3G sem optimização de rota)

Para os tempos de *jitter* apenas são apresentados alguns tipos de tráfego dado que os restantes se tornam análogos. Neste caso ocorre a mesma situação idêntica ao *delay*, onde podemos notar maiores tempos para o caso da tecnologia 3G.

Sempre que se executa o *handover* de Wi-Fi para 3G pode-se notar um aumento instantâneo que mais tarde estabiliza, tal acontecimento deve-se ao facto de se efectuar um *handover* de uma rede com menor *delay* para uma com maior *delay*. Deste modo, uma vez que o *jitter* é o tempo existente entre a recepção de dois pacotes, após o *handover* existe sempre uma maior diferença no primeiro pacote, tal como se pode justificar pela Figura 5.3.1.3.1-7.

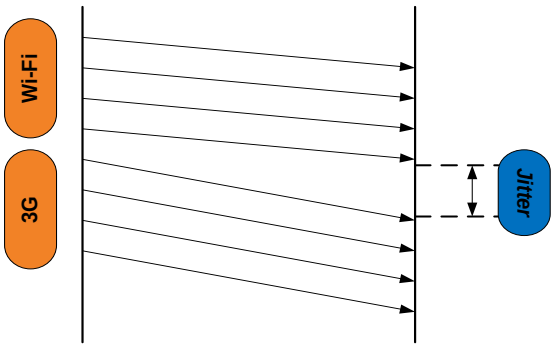

Figura 5.3.1.3.1-7: Representação do valor do *Jitter*

Para além deste problema, também a perda de pacotes vem agravar esta situação.

Bitrate:

Através da Figura 5.3.1.3.1-8 e Figura 5.3.1.3.1-9 são apresentados os gráficos do *bitrate* para todos os tráfegos utilizados.

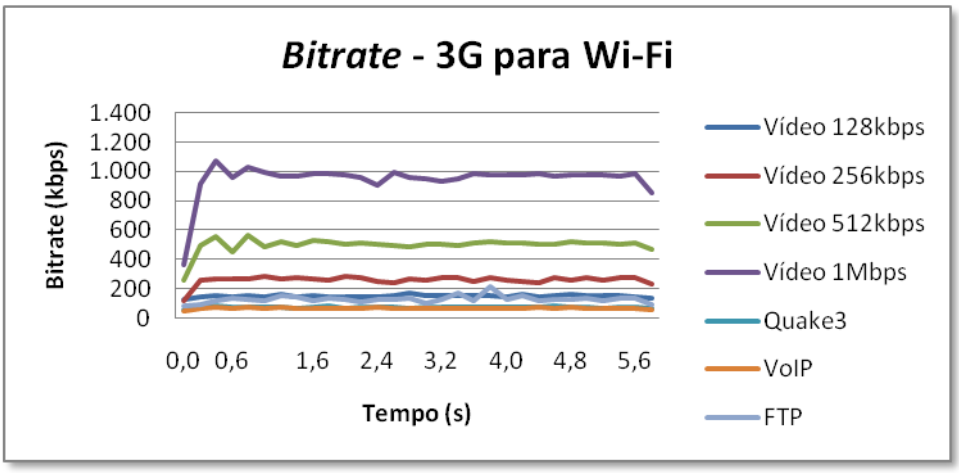

Figura 5.3.1.3.1-8: *Bitrate* (3G para Wi-Fi sem optimização de rota)

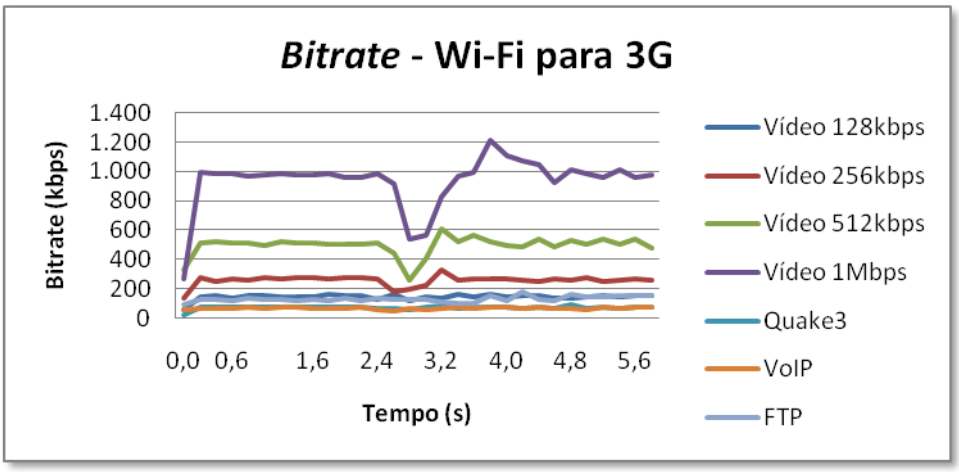

Figura 5.3.1.3.1-9: *Bitrate* (Wi-Fi para 3G sem optimização de rota)

Como se pode vizualizar, os valores do *bitrate* encontran-se dentro do esperado. De notar o *bitrate* para o caso da Figura 5.3.1.3.1-9 que tem um pico descendente nos vários tipos de tráfego, principalmente para os de maior *bitrate*, e que se deve ao facto de se efectuar o *handover* para a rede 3G (HSPA). Uma vez que não existe qualquer tipo de controlo nesta rede, não se torna possivel efectuar nenhum tipo de reserva de recursos através da implementação do IEEE 802.21. Deste modo, após a transição de Wi-Fi para 3G, o *bitrate* diminui drasticamente uma vez que a rede 3G não consegue dar "resposta" ao *bitrate* imposto instantaniamente pelo tráfego em questão. Após a recepção dos primeiro pacotes, uma vez que se trata da tecnologia HSPA, esta inicia um processo de reserva de recursos de forma dinâmica para que possa garantir os serviçes necessários durante todo o serviço.

Embora o *bitrate* diminua após o *handover*, no que diz respeito ao emissor, este continua a enviar o tráfego com um *bitrate* apróximadamente constante. O receptor, neste caso a rede 3G (HSPA), ao não conseguir dar "resposta" a este vai adicionando os pacotes que lhe vão chegando a um *buffer* para os ir tratando à medida que lhe é permitido. Esta situação irá provocar que a um determinado momento os pacotes existentes no *buffer* sejam enviados em "rajada" de forma a compensar a descida do *bitrate*. Este comportamento é observavel através do pico ascendente presente na Figura 5.3.1.3.1-9.

Pacotes perdidos e fora de ordem:

A existência de perda de pacotes deve-se à necessidade de efectuar modificações do túnel existente entre o HA e o MN. Deste modo torna-se possível que o HA receba pacotes sem que ainda tenha o túnel "pronto a utilizar", o que provocará a perda destes mesmos pacotes.

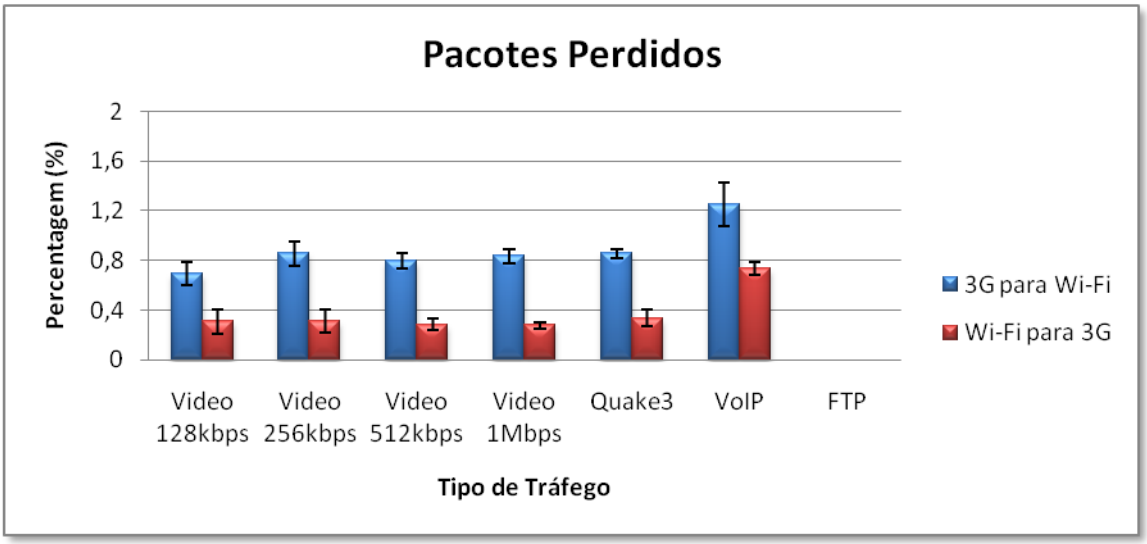

Figura 5.3.1.3.1-10: Percentagem de Pacotes Perdidos – *Handover* sem optimização de rota

Para o caso de se estar perante um *handover* de Wi-Fi para 3G, este apenas tem perdas durante a actualização do túnel existente entre o MN e o HA e não devido aos pacotes fora de ordem, devido a isto, tal como se pode visualizar pela Figura 5.3.1.3.1-10, existe maior perda de

pacotes de 3G para Wi-Fi. De referir o facto de quanto maior o número de pacotes por segundo, maior a perda destes, embora a percentagem se mantenha aproximadamente constante.

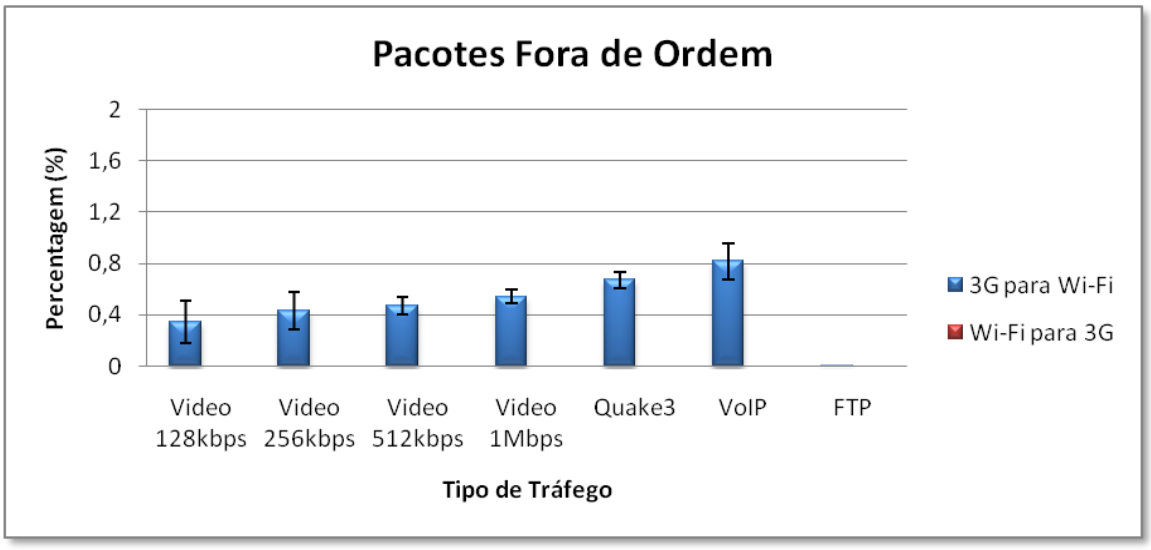

Figura 5.3.1.3.1-11: Percentagem de Pacotes Fora de Ordem – *Handover* sem optimização de rota

Outro factor que influência a perda de pacotes aquando da realização do *handover* de 3G para Wi-Fi são os pacotes fora de ordem, Figura 5.3.1.3.1-11. Estes surgem devido à rede 3G ter um elevado *delay* comparativamente com a rede Wi-Fi.

De forma a representar um *handover* de 3G para Wi-Fi, mas dando maior ênfase ao processo de pacotes fora de ordem, é apresentada a Figura 5.3.1.3.1-12.

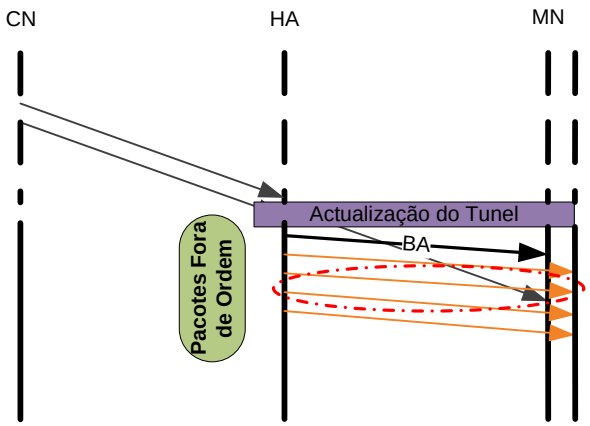

Figura 5.3.1.3.1-12: Demonstração simplificada de perda de pacotes durante *Handover* de 3G para Wi-Fi

5.3.1.3.2. Métricas com Optimização de Rota

Delay:

Através da Figura 5.3.1.3.2-1, Figura 5.3.1.3.2-2, Figura 5.3.1.3.2-3 e Figura 5.3.1.3.2-4 são apresentados os gráficos do *delay* obtidos durante a realização de *handover*, mas agora para o caso de termos a optimização de rota activa.

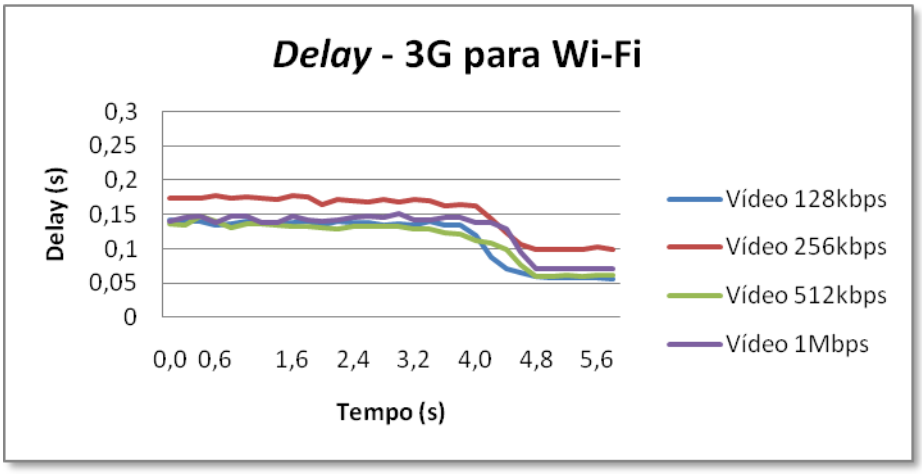

Figura 5.3.1.3.2-1: Tráfego de vídeo – *Delay* (3G para Wi-Fi com optimização de rota)

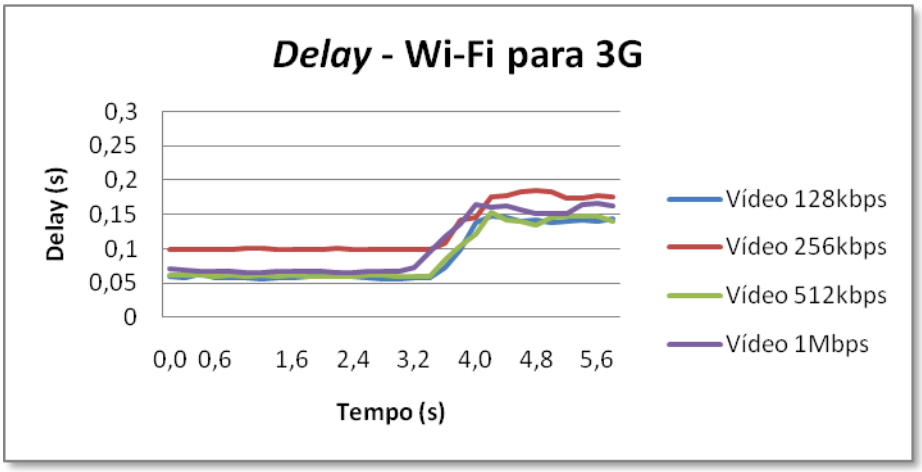

Figura 5.3.1.3.2-2: Tráfego de vídeo – *Delay* (Wi-Fi para 3G com optimização de rota)

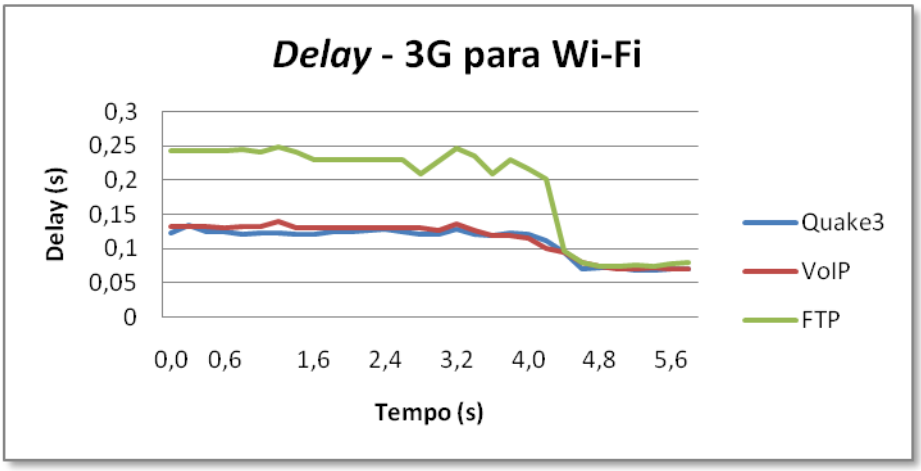

Figura 5.3.1.3.2-3: Quake3/VoIP/FTP – *Delay* (3G para Wi-Fi com optimização de rota)

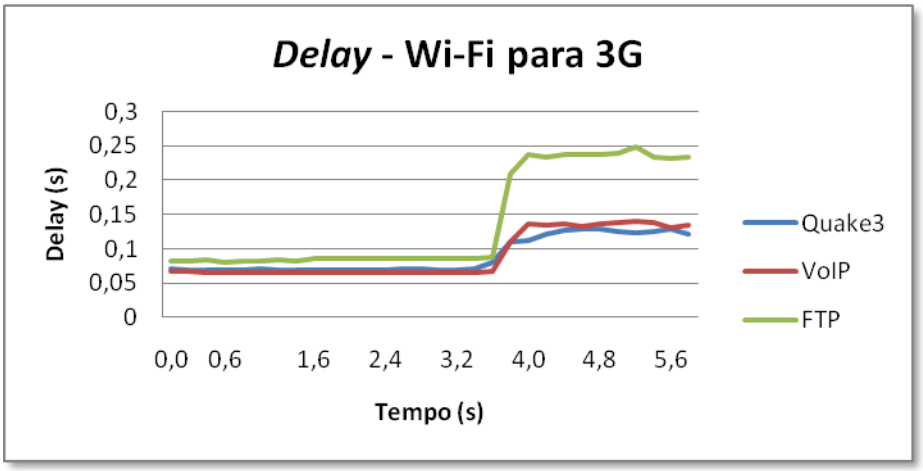

Figura 5.3.1.3.2-4: Quake3/VoIP/FTP – *Delay* (Wi-Fi para 3G com optimização de rota)

Para qualquer tipo de tráfego pode-se constatar que existe uma diminuição no valor do *delay,* comparativamente ao caso em que não temos optimização de rota. Isto deve-se ao facto de o envio de tráfego ser efectuado directamente entre o CN e o MN e já não existir a necessidade de se ter o HA como "intermediário", ou seja, a interceptar e reenviar os pacotes com destino ao MN.

Jitter:

Segue-se a representação dos gráficos do *Jitter*, através da Figura 5.3.1.3.2-5 e Figura 5.3.1.3.2-6, obtidos nas mesmas condições do *delay*, ou seja, perante a utilização de optimização de rota.

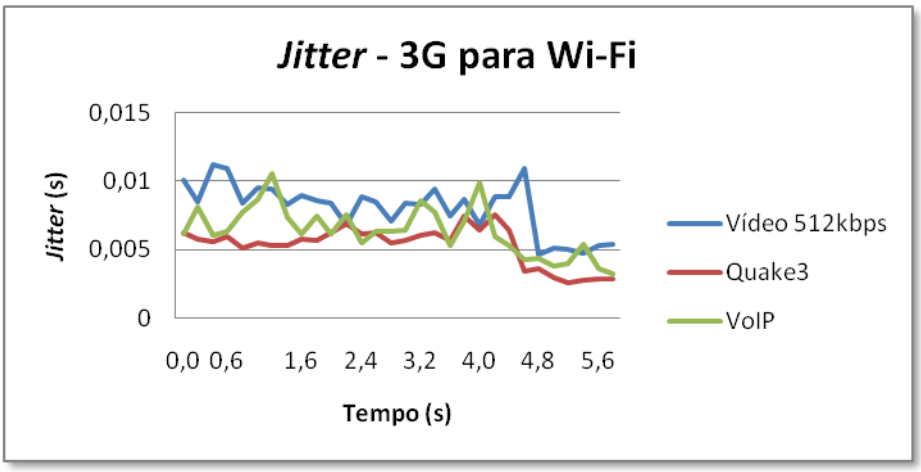

Figura 5.3.1.3.2-5: Vídeo 512kbps/Quake3/VoIP – *Jitter* (3G para Wi-Fi com optimização de rota)

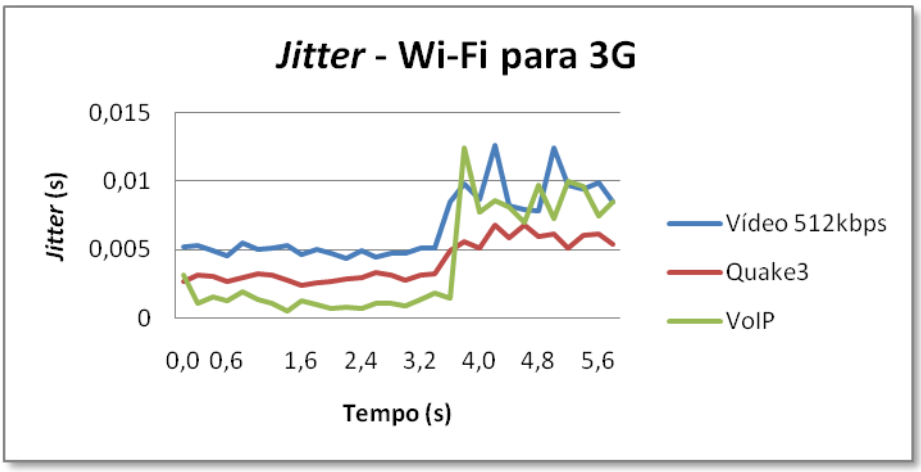

Figura 5.3.1.3.2-6: Vídeo 512kbps/Quake3/VoIP – *Jitter* (Wi-Fi para 3G com optimização de rota)

Relativamente ao *jitter*, estes mantêm-se aproximadamente idênticos ao caso em que não existe optimização de rota.

Bitrate:

Como se pode verificar através da Figura 5.3.1.3.2-7 e Figura 5.3.1.3.2-8, o *bitrate* apresenta valores próximos dos teóricos. Para o caso da Figura 5.3.1.3.2-8, os picos descendentes e ascendentes que esta apresenta são justificados de igual modo como já acontecia para o caso do *bitrate* sem optimização de rota.

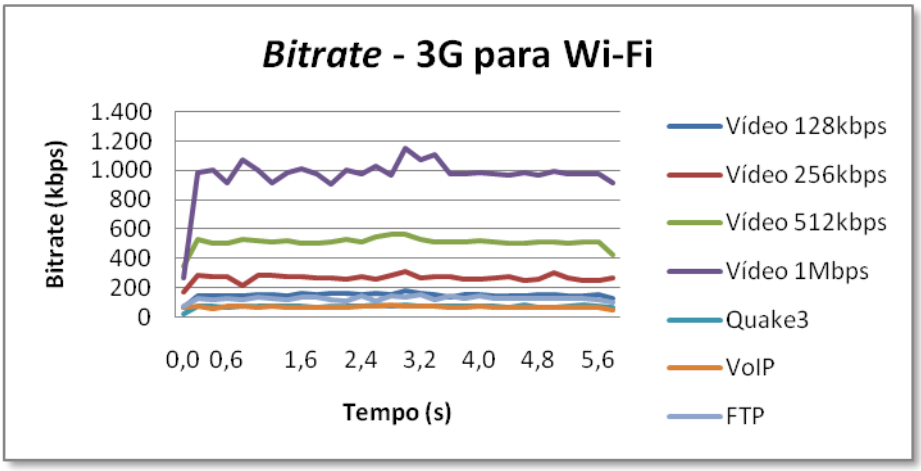

Figura 5.3.1.3.2-7: *Bitrate* (3G para Wi-Fi com optimização de rota)

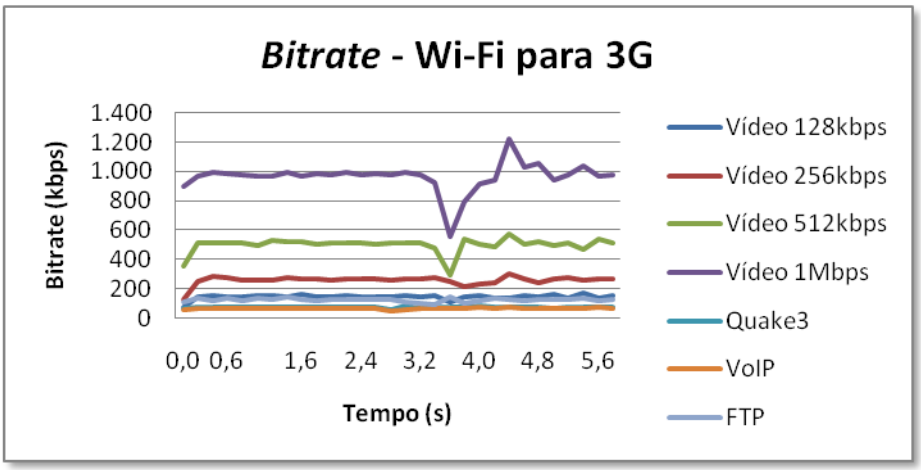

Figura 5.3.1.3.2-8: *Bitrate* (Wi-Fi para 3G com optimização de rota)

Pacotes perdidos e fora de ordem:

Para o caso de utilizarmos optimização no processo de *handover* pode-se verificar que existem reduções significativas nas perdas de pacotes, Figura 5.3.1.3.2-9. Esta redução deve-se ao facto de não existirem as perdas causadas pela actualização do túnel entre o MN e o HA, uma vez que o CN durante este processo continua a comunicar com o MN. As perdas existentes são causadas pelos pacotes fora de ordem, como se pode verificar pela Figura 5.3.1.3.2-10. Deste modo apenas existem perdas no *handover* de 3G para Wi-Fi, sendo que para o caso do *handover* de Wi-Fi para 3G não existe qualquer tipo de perdas.

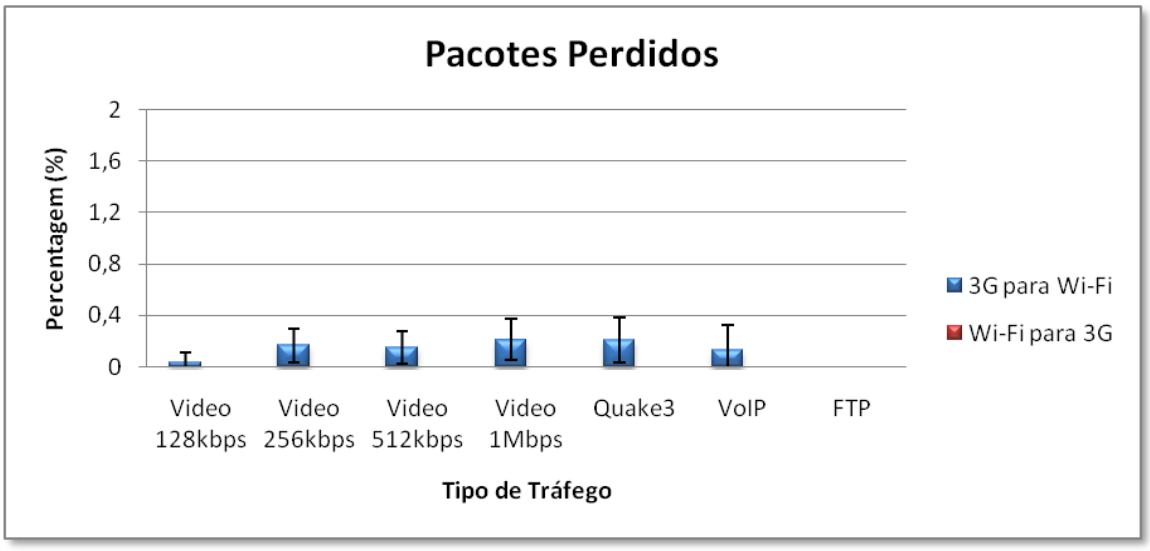

Figura 5.3.1.3.2-9: Percentagem de Pacotes Perdidos – *Handover* com optimização de rota

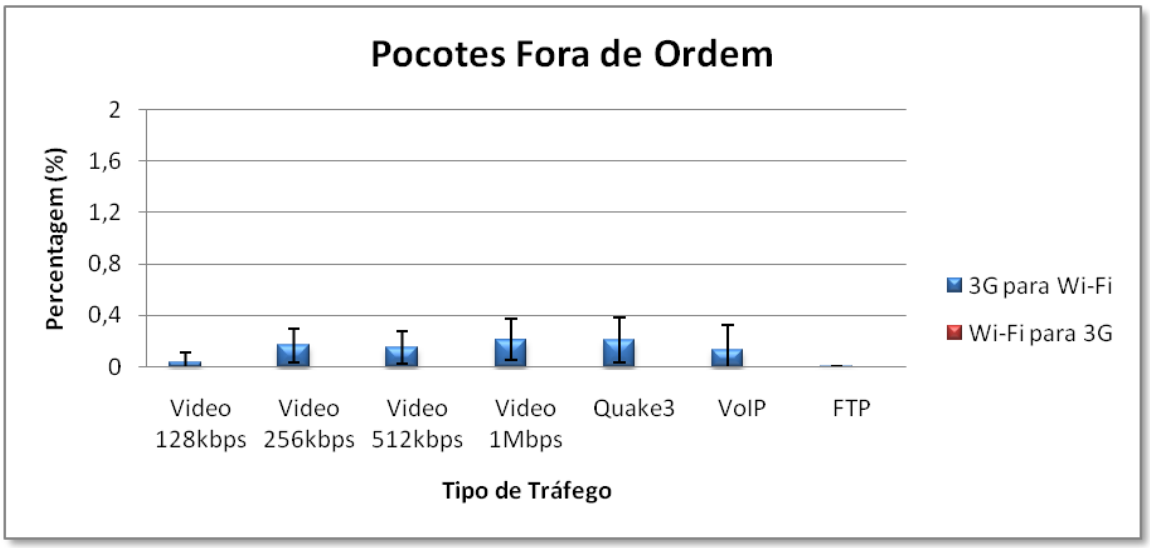

Figura 5.3.1.3.2-10: Percentagem de Pacotes Fora de Ordem – *Handover* com optimização de rota

Comparando os valores obtidos relativamente ao caso do UMIP não ter suporte ao IEEE 802.21 com o caso de este ter suporte ao IEEE 802.21, relativamente à perda de pacotes, mais uma vez pode-se observar que existe uma grande discrepância entre estes dois casos. Relativamente ao caso de se iniciar o *handover* no UMIP através IEEE 802.21 é observável uma grande diminuição de perda de pacotes, podendo mesmo se considerar uma perda insignificante para o caso de se efectuar *handover* de 3G para Wi-Fi com optimização de rota. Para o caso de se efectuar um *handover* de Wi-Fi para 3G com optimização de rota, esta perda é eliminada.

5.3.1.4. Métricas de QoE para Tráfego VoIP

Através desta secção é apresentado o MOS tanto para o caso de não termos suporte IEEE 802.21 para iniciar o processo de *handover* no UMIP como para o caso de este ser suportado.

No caso de não se ter suporte IEEE 802.21 apenas é apresentado o MOS para realização de *handover* de Wi-Fi para 3G, o que se deve ao facto de este se tratar do melhor caso e ser suficiente a nível de comparação.

UMIP sem Suporte IEEE 802.21:

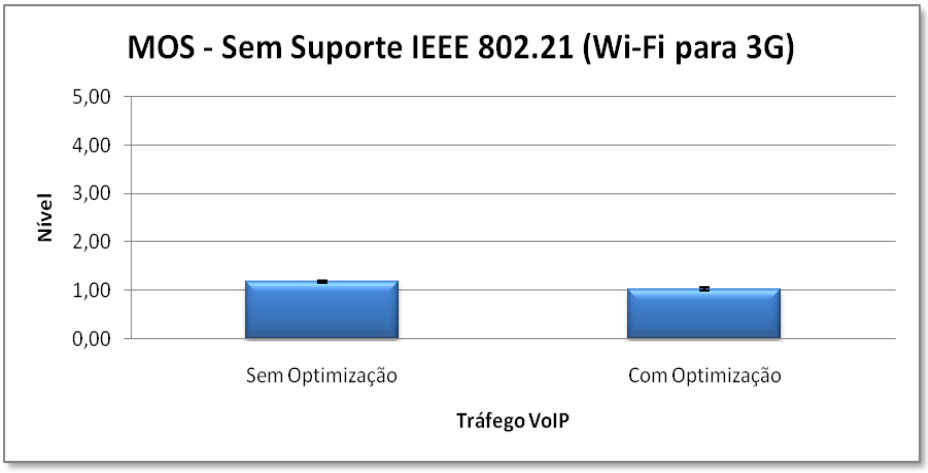

Figura 5.3.1.4-1: MOS para Tráfego VoIP sem suporte IEEE 802.21

UMIP com Suporte IEEE 802.21:

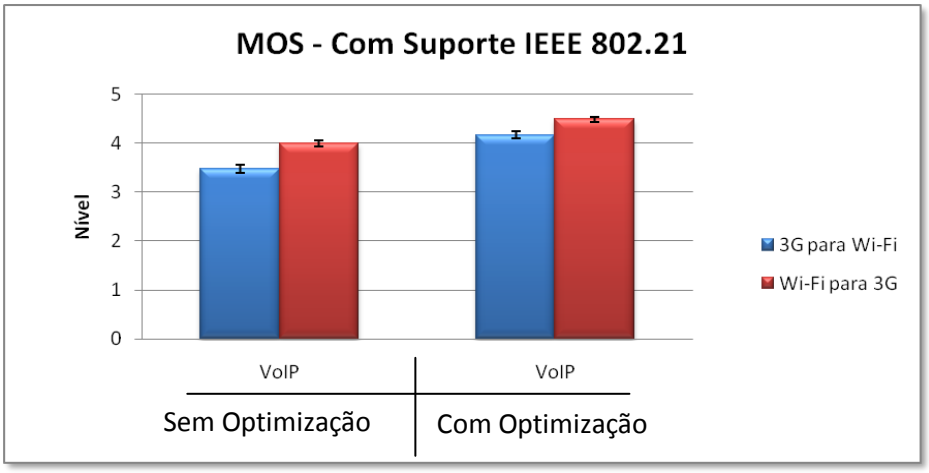

Figura 5.3.1.4-2: MOS para Tráfego VoIP com suporte IEEE 802.21

Analisando as Figura 5.3.1.4-1 e Figura 5.3.1.4-2 é possível verificar que para o caso de o *handover* se realizar sem suporte IEEE 802.21, a qualificação do tráfego VoIP torna-se inaceitável para os utilizadores, o que contrasta com o caso de se realizar o *handover* através do IEEE 802.21.

Neste caso a quantificação do MOS encontra-se entre o nível *High* e *Best*, ou seja, o tráfego VoIP apresenta uma óptima percepção para o utilizador.

Relativamente ao caso de se usar ou não optimização de rota, Figura 5.3.1.4-2, pode-se verificar que a utilização desta permite uma ligeira melhoria na quantificação do MOS.

No que diz respeito aos tipos de *handover*, é possível verificar através da Figura 5.3.1.4-2 que se tem melhores resultados para o caso de este ser realizado de Wi-Fi para 3G. Esta constatação deve-se ao facto de o MOS depender principalmente do *Delay* e da percentagem de pacotes perdidos, os quais são favorecidos neste tipo de *handover.*

5.3.2. *Handover* de *Home Network* para *Foreign Network* e de *Foreign Network* para *Home Network* Iniciado pelo IEEE 802.21

Uma vez que o processo de *handover* contém algumas diferenças dependendo do caso deste ser realizado de uma FN para outra FN, de uma HN para uma FN e de uma FN para uma HN, é apresentado um estudo relativo aos dois últimos processos referidos. Para estes casos apenas são obtidas algumas da principais métricas a nível do processo de *handover* iniciado pelo IEEE 802.21 e sem optimização de rota. A *testbed* utilizada para a obtenção destes valores é a apresentada na Figura 5.1-2.

5.3.2.1. *Handover* Iniciado pelo IEEE 802.21 e sem Optimização de Rota

Handover Delay:

Relativamente ao *Handover Delay*, Figura 5.3.2.1-1, pode-se observar que este é ligeiramente inferior ao caso da execução do *handover* de FN para FN sem optimização, Figura 5.3.1.1.2-1. Embora os processos executados durante a fase de obtenção do *delay* sejam idênticos, o *delay* dos pacotes pela interface Wi-Fi é menor devido a estes serem enviados directamente para o MN sem necessidade de intervenção do HA.

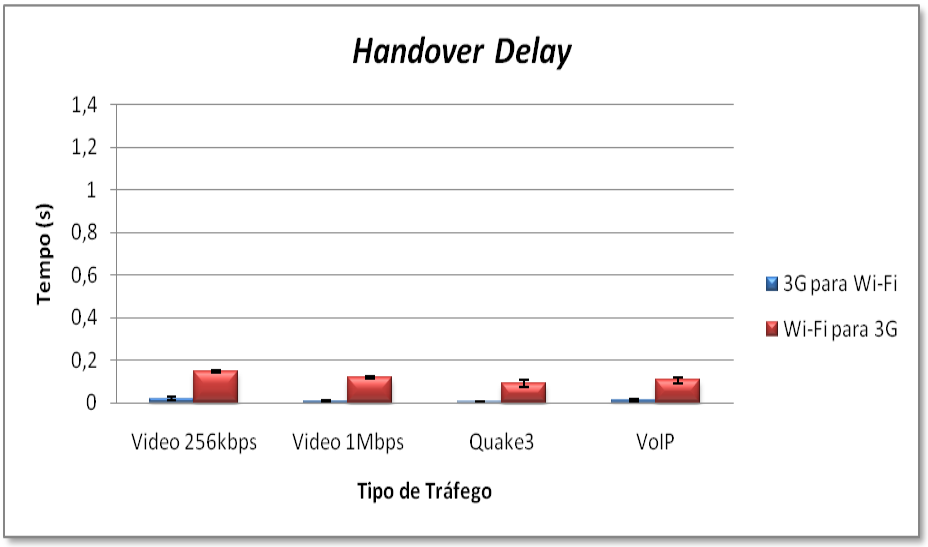

Figura 5.3.2.1-1: *Handover Delay* - sem optimização de rota

Handover Execution Delay:

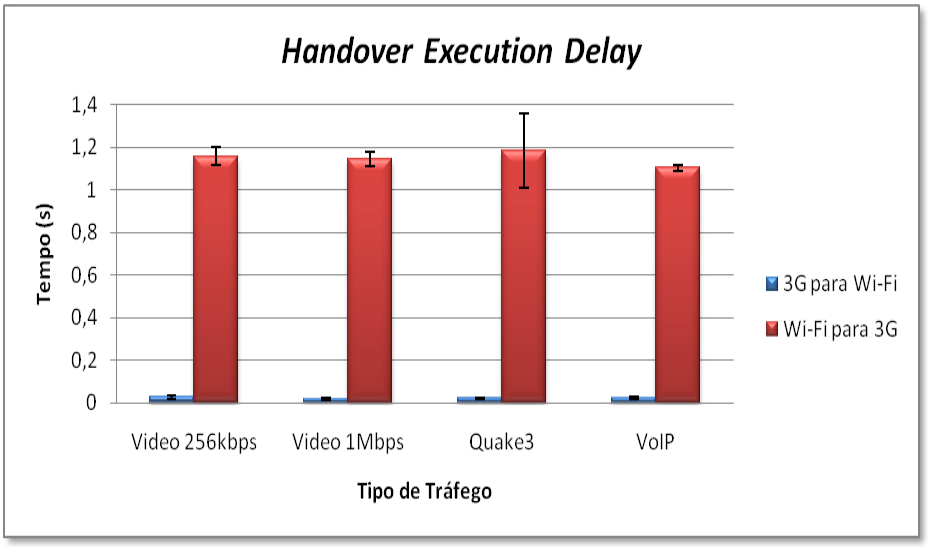

Figura 5.3.2.1-2: *Handover Execution Delay* - sem optimização de rota

Analisando o *Handover Execution Delay*, Figura 5.3.2.1-2, e comparando-o com o caso do *handover* de FN para FN sem optimização de rota, Figura 5.3.1.1.2-2, é possível denotar uma elevada discrepância tanto no *handover* de 3G para Wi-Fi como para o caso de Wi-Fi para 3G. Dado que o *Handover Execution Delay* é obtido desde o BU enviado pelo MN para o seu HA até à recepção do primeiro pacote pela nova interface é de esperar as diferenças apresentadas, uma vez que são executados processos diferentes. Para o caso da realização do *handover* de 3G para Wi-Fi, ou seja, quando o MN retorna à sua HN, este ao detectar tal situação envia um BU ao seu HA para que este deixe de utilizar o túnel e de interceptar os seus pacotes. Já na realização do *handover* de Wi-Fi para 3G, uma vez que o MN se desloca da HN para uma FN, o seu HA necessita de tornar a interceptar os pacotes destinados ao MN.

5.3.2.2. Métricas de QoS para *Handover* Iniciado pelo IEEE 802.21

Através da Figura 5.3.2.2-1 e Figura 5.3.2.2-2 pode-se observar o *delay* obtido durante a execução do *handover* sem optimização de rota para os vários tipos de tráfego e para o caso deste ser executado da FN para a HA e da HN para a FN, respectivamente.

Delay:

Analisando a Figura 5.3.2.2-1 e a Figura 5.3.2.2-2 e comparando-as com as respectivas figuras para o caso do *handover* de FN para FN sem optimização de rota (Figura 5.3.1.3.1-1, Figura 5.3.1.3.1-2, Figura 5.3.1.3.1-3 e Figura 5.3.1.3.1-4), é possível observar uma elevada discrepância no que diz respeito aos tempos do *delay* na rede Wi-Fi. Esta diferença é causada pelo facto de se utilizar a rede Wi-Fi como HN. Neste caso, sempre que o MN se encontrar na rede Wi-Fi este não necessita que os pacotes que lhe são enviados sejam interceptados e reencaminhados pelo seu HA, sendo que neste caso a comunicação com o MN é efectuada como um processo normal de encaminhamento sem qualquer tipo de mobilidade. Relativamente ao caso da rede 3G, esta mantém aproximadamente os mesmos valores de *delay*, uma vez que o processo de transmissão dos pacotes é idêntico. As pequenas discrepâncias existentes devem-se ao facto das medidas não terem sido obtidas no mesmo dia. Dado que não se tem qualquer tipo de controlo no caso da rede 3G, as medições efectuadas através desta dependem sempre da sobrecarga nesta existente, causada por exemplo pelo número de utilizadores no respectivo instante.

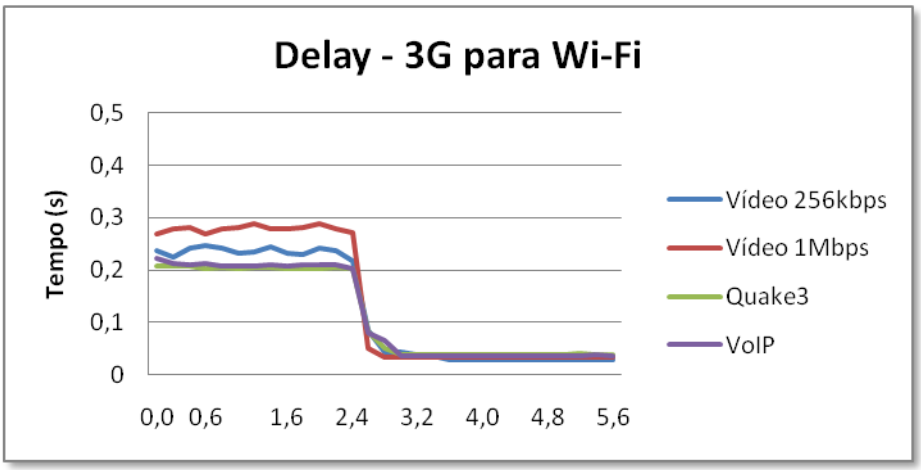

Figura 5.3.2.2-1: *Delay* - 3G para Wi-Fi sem optimização de rota

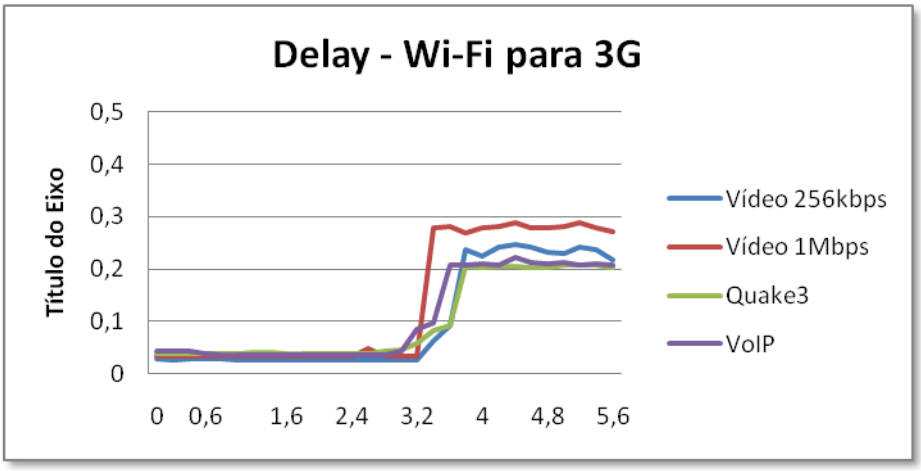

Figura 5.3.2.2-2: *Delay* - Wi-Fi para 3G sem optimização de rota

Pacotes perdidos e fora de ordem:

Observando a Figura 5.3.2.2-3, que representa a percentagem de pacotes perdidos, pode-se observar que para o caso da execução do *handover* de Wi-Fi para 3G não existe perda de pacotes. Este caso torna-se idêntico ao caso do *handover* de FN para FN mas com optimização de rota. Uma vez que o MN encontra-se inicialmente na sua HN, o envio de pacotes é efectuado directamente para o MN sem que seja necessário a utilização do túnel entre o MN e o HA, eliminando neste caso a perda de pacotes durante a actualização do túnel.

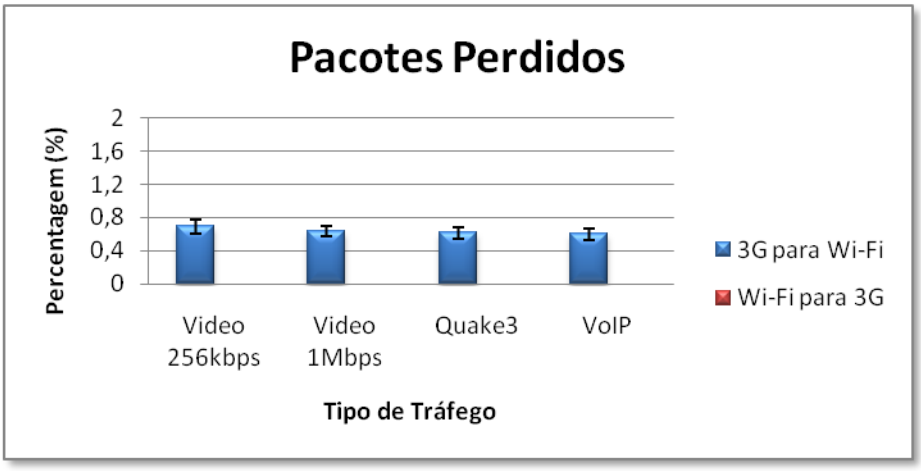

Figura 5.3.2.2-3: Percentagem de Pacotes Perdidos – *Handover* sem optimização de rota

Para o caso do *handover* de 3G para Wi-Fi é possível observar que existe uma pequena diminuição na perda de pacotes. Neste caso, dado que é efectuado um *handover* de FN para HN, deixa de ser necessário alterar o túnel, passando-se só a indicar que este não deve ser utilizado, através do envio do BU.

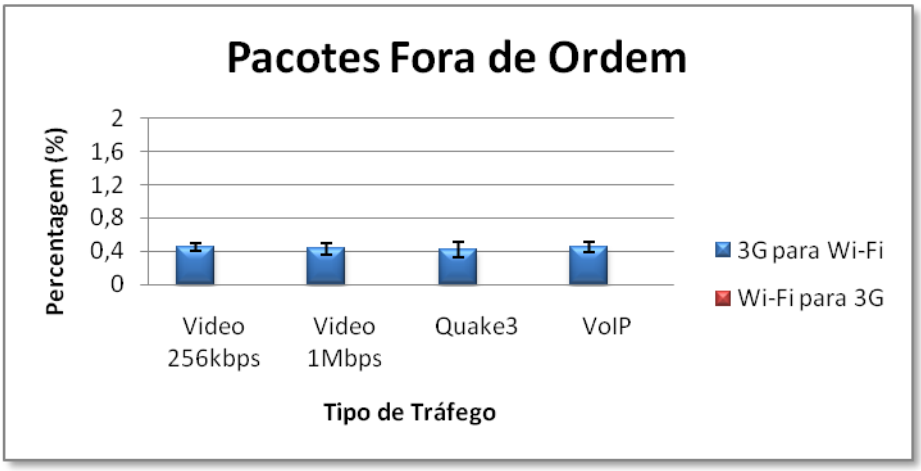

Figura 5.3.2.2-4: Percentagem de Pacotes Fora de Ordem– *Handover* sem optimização de rota

Relativamente aos pacotes fora de ordem existente, Figura 5.3.2.2-4, como já era esperado estes apenas existem para o caso da realização do *handover* de 3G para Wi-Fi devido ao maior *delay* existente na rede 3G, tal como já foi referido anteriormente.

5.4. Conclusões

Neste capítulo foi efectuado um estudo referente ao processo de *handover* com e sem auxilio do IEEE 802.21 entre as redes 3G e Wi-Fi, de forma a se poder obter valores que quantifiquem todo este processo.

A obtenção de dados foi efectuada para vários tipos de tráfego, para o caso de se efectuar ou não optimização de rota, para o caso de se efectuar *handover* entre FNs ou entre FN e HN e para o caso de este ser iniciado através de quebra de ligação ou através do IEEE 802.21.

Com dos dados obtidos foi possível verificar as limitações existentes na rede 3G, tanto a nível do *delay* como a nível do número de pacotes perdidos, sendo ambos os valores maiores para esta tecnologia, comparativamente com o Wi-Fi.

Comparando os valores de *Handover Delay*, *Handover Execution Delay* e número de pacotes perdidos para o caso de se utilizar apenas o UMIP sem suporte ao IEEE 802.21 e para o caso do uso deste mas com suporte ao IEEE 802.21, é possível verificar a enorme variação de valores em qualquer uma das medidas mencionadas. Esta variação permite demonstrar a verdadeira necessidade da interacção entre o UMIP e o IEEE 802.21, uma vez que sem este suporte o processo apresenta elevadas perdas de pacotes, bem como tempos de *Handover Delay* e *Handover Execution Delay* inaceitáveis para situações reais que pretendam continuidade de serviços. Com os valores de MOS apresentados, para o caso do VoIP, é possível dar ainda mais ênfase à necessidade de interacção entre estas duas entidades, uma vez que para o caso de esta não ser suportada o suporte ao tráfego de VoIP é inaceitável para a percepção dos utilizadores. Para o caso da interacção ser suportada os valores de MOS atingem valores óptimos de percepção.

Para o caso da optimização de rota pode-se verificar que esta apresenta um número elevado de vantagens aquando a sua utilização. A execução do *handover* (de FN para FN) com a optimização de rota activa permite reduzir tanto o tempo de *delay* como o *jitter*, que por sua vez melhoram o *Handover Delay*. Para além disto, a optimização de rota permite reduzir de uma forma significativa o número de pacotes perdidos em qualquer tipo de tráfego. A única contrapartida relativa à utilização da optimização de rota deve-se ao aumento do tempo de *Handover Execution Delay*. Este factor não terá grande impacto caso se consiga detectar com alguma antecedência, através do IEEE 802.21, a necessidade de se efectuar o *handover,* uma vez que o MN continua a receber os pacotes pela interface antiga.

Relativamente à execução de *handover* da HN para a FN e da FN para a HN, pode-se concluir que estes apresentam melhorias tanto a nível do *Handover Delay* como a nível do número de pacotes perdidos, comparativamente com o caso de *handover* de FN para FN e sem optimização de rota. A única contrapartida prende-se com a execução do *handover* da HN para a FN que apresenta um maior *Handover Execution Delay.* As melhorias deste processo, resumidamente, devem-se ao facto de se tratar de um *handover* "semi-optimizado", ou seja, caso o MN se encontre na sua HN, os pacotes são enviados directamente para este; se por outro lado o MN se encontrar numa FN, os pacotes já terão de ser reencaminhados, através do HA, para o MN.

6. Conclusão

6.1. Conclusão Final

Esta dissertação apresenta um estudo relativo ao desenvolvimento de um demonstrador de mobilidade entre redes de acesso heterogéneas composta pelas redes Wi-Fi e 3G, utilizando como auxilio o protocolo de optimização de mobilidade IEEE 802.21.

Para que se tornasse possível este estudo relativo à mobilidade de utilizadores entre redes heterogéneas era necessária a existência de cooperação entre a implementação do protocolo de mobilidade (UMIP) e a implementação do protocolo de optimização de mobilidade, a qual não era suportada. Esta interacção estava limitada por motivos presentes em ambas as implementações, no caso do UMIP este não suportava qualquer tipo de interacção com entidades externas nem tornava possível a tomada de decisão no processo de *handover,* ou seja, não era possível intervir activamente na decisão da realização do *handover*, nem na escolha da interface para o qual seria executado. Para o caso do IEEE 802.21 tornava-se necessário que este pudesse comunicar com o UMIP de forma a intervir neste processo, podendo indicar o melhor momento para a realização do *handover* e a melhor interface para o efectuar.

Para se poder ultrapassar todos estes obstáculos procedeu-se a alterações tanto a nível do UMIP como a nível da implementação do IEEE 802.21. No caso do UMIP foi necessário alterar a forma como este analisava as suas interfaces, bem como o modo de atribuição de preferência a determinadas interfaces. A esta entidade foi ainda implementado um "servidor" de forma a poder interagir com entidades externas. Após estas modificações tornou-se possível a realização de *handover* sem que existisse necessidade de perder qualquer tipo de ligação com a interface antiga do MN e de uma forma controlada. Para o caso do UMIP foram ainda detectados alguns problemas a nível da implementação da optimização de rota, os quais foram resolvidos através do controlo deste mesmo processo. Seguidamente procedeu-se ao desenvolvimento de um "cliente" na implementação do protocolo IEEE 802.21 para que este possa comunicar com o "servidor" existente no UMIP, tornando possível a intervenção por parte do IEEE 802.21 no processo de *handover*.

Estando concluído todo o processo de controlo no que diz respeito ao *handover* e à comunicação entre o UMIP e o IEEE 802.21, tornou-se necessário quantificar todo este processo. Para esta quantificação foram implementadas *probes* móveis que pudessem controlar o processo de handover, injectando diferentes serviços na rede, para obter métricas como *Handover Delay*, *Handover Execution Delay*, o tempo de execução de *handover* do IEEE 802.21, *delay*, *jitter*, *bitrate*, número de pacotes perdidos e número de pacotes fora de ordem referentes a este. Para o caso do VoIP foi ainda obtido o MOS. Através do desenvolvimento das *probes* móveis foi possível: iniciar o *handover*, quer seja directamente através do UMIP, quer seja através do IEEE 802.21; iniciar o tráfego automaticamente através do CN e analisar vários tipos de tráfego para a obtenção das métricas.

Após a obtenção de todos os dados pretendidos procedeu-se à sua análise, podendo identificar todas as vantagens referentes à utilização das implementações/modificações efectuadas bem como à interacção entre o UMIP e o IEEE 802.21, as quais permitem a redução de tempos e de pacotes perdidos durante o processo de *handover*. Relativamente à optimização de rota foi identificada a necessidade da implementação desta para que se possa tornar todo este processo mais eficiente.

Todo este estudo permite demonstrar a verdadeira necessidade de interacção entre a implementação do protocolo de mobilidade e a implementação do protocolo de optimização de mobilidade para que se possa garantir uma mobilidade mais eficiente e optimizada aos utilizadores. Como prova disto temos a diferença de tempos, tais como o *Handover Delay, Handover Execution Delay* e o número de pacotes perdidos, comparativamente entre o caso de não se utilizar a interacção de ambos os protocolos e o caso de esta interacção ser permitida e utilizada.

6.2. Trabalho Futuro

Como trabalho futuro poderá ser feita uma análise a um maior número de tecnologias, de forma a identificar possíveis limitações e características das mesmas. Uma das tecnologias a integrar é o LTE.

Outro aspecto a ter em consideração é o facto de se puder utilizar outro tipo de protocolo de mobilidade, como o PMIPv6, FastMIPv6 ou DSMIP para que seja possível tornar todo este processo o mais independente possível do utilizador, eliminar o número de pacotes perdidos ou mesmo permitir a interacção de ambos os protocolos de endereçamento (IPv4 e IPv6), respectivamente.

Bibliografia

[1] SOARES, J. Desempenho de Redes de Acesso Heterogéneas com Suporte de Mobilidade. Tese de Mestrado, Universidade de Aveiro, Aveiro. 2009.

[2] BOB O'HARA, AL PETRICK. IEEE 802.11 handbook: a designer's companion. IEEE Standards Association, 2004. 364 p.

[3] WILLIAM STALLINGS. Business Data Communications. Prentice Hall, 2008. 608 p.

[4] 3COM. IEEE 802.11b Wireless LANs. Technical Paper. 2003

[5] IEEE 802.11, IEEE Standard for Information technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std. 802.21, Junho de 2007.

[6] RÉS, B. Soluções Tecnológicas e Impacto da Mobilidade Numa Rede WiMAX. Tese de Mestrado, Universidade de Aveiro, Aveiro. 2008.

[7] LOUTFI NUAYMI. WiMAX: technology for broadband wireless access. John Wiley and Sons, 2007. 283p.

[8] SYED AHSON. WiMAX: applications. CRC Press, 2007. 248 p.

[9] IEEE 802.16 WG, IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE std. 802.16-2004, Outubro de 2004.

[10] IEEE 802.16 WG, Amendment to IEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Physical and Medium Access Control Layer for Combined Fixed and Mobile Operation in Licensed Bands, IEEE Std. 802.16e-2005, Dezembro de 2005.

[11] JOSE PUTHENKULUM. MIBs location 802.16g Reference Model. Vancouver,BC. IEEE C802.16g-05/063. 2005.

[12] MATOS, R. Suporte de Mobilidade em Redes WiMAX. Tese de Mestrado, Universidade de Aveiro, Aveiro. 2008.

[13] SEOK-YEE TANG, et al. WiMAX Security and Quality of Service: An End-to-End Perspective. . John Wiley and Sons, 2010. 424 p.

[14] BRUCE ALAN FETTE, et al. RF & wireless technologies. Newnes, 2008. 827 p.

[15] RAMJEE PRASAD, MARINA RUGGIERI. Technology trends in wireless communications. Artech House, 2003. 310 p.

[16] KASERA. 2.5G Mobile Networks. Tata McGraw-Hill, 2008. 257 p.

[17] REGIS J. BATES. GPRS: general packet radio service. McGraw-Hill Professional, 2002. 280 p.

[18] HEIKKI KAARANEN. UMTS networks: architecture, mobility, and services. John Wiley and Sons, 2005. 406 p.

[19] BERNHARD WALKE, PETER SEIDENBERG,MARC PETER ALTHOFF. UMTS: the fundamentals. John Wiley and Sons, 2003. 312 p.

[20] PABLO TAPIA et al. HSPA Performance and Evolution: A Practical Perspective. John Wiley and Sons, 2009. 284 p.

[21] JIE ZHANG, GUILLAUME LA DE ROCHE, GUILLAUME DE LA ROCHE. Femtocells: Technologies and Deployment. John Wiley and Sons, 2010. 328 p.

[22] 3G AMERICAS. EDGE, HSPA and LTE BROADBAND INNOVATION. Setembro de 2008

[23] MORAY RUMNEY. LTE and the Evolution to 4G Wireless: Design and Measurement Challenges. John Wiley and Sons, 2009. 448 p.

[24] CHARLES PERKINS. “IP mobility Support for IPv4”, IETF RFC 3344, Agosto de 2002

[25] DAVID JOHNSON, et al. “Mobility Support in IPv6”, IETF RFC 3775, Junho de 2004.

[26] CHARLES PERKINS, et al. “Fast Handovers for Mobile IPv6”, IETF RFC, Julho de 2005

[27] GUNDAVELLI, et al. “Proxy Mobile IPv6”, IETF RFC 5213, Agosto de 2008

[28] HESHAM SOLIMAN. “Mobile IPv6 Support for Dual Stack Hosts and Routers”, IETF RFC 5555, Junho de 2009

[29] IEEE 802.21, IEEE Standard for Local and Metropolitan Area Networks. Part 21: Media Independent Handover Services, IEEE Std. 802.21, Janeiro de 2008.

[30] MELO, M. Performance of WiMAX networks with mobility. Tese de Mestrado, Universidade de Aveiro, Aveiro. 2008.

[31] DAVID TUNG CHONG WONG et al. Wireless Broadband Networks. John Wiley and Sons, 2009. 508 p.

[32] SHINGO ATA, CHOONG SEON HONG. Managing next generation networks and services: 10th Asia-Pacific Network. Springer, 2007. 619 p.

[33] JORDI PALET MARTÍNEZ. Enabling efficient and operational mobility in large heterogeneous IP networks. Enable, 2008. 280 p.

[34] IEEE 802.21/d14, "draft standard for local and metropolitan area networks: Media independent handover services". Setembro de 2008

[35] MASAFUMI ARAMOTO et al*. http://umip.linux-ipv6.org/.* Acedido em 20 de Dezembro de 2009.

[36] THOMAS NARTEN, et al. “*Neighbor Discovery for IP version 6”*, IETF RFC 4861, Setembro de 2007.

[37] RAJEEV S. KOODLI, CHARLES E. PERKINS. Mobile inter-networking with IPv6: concepts, principles, and practices. Wiley-Interscience, 2007. 365 p.

[38] NEVES, P.; SOARES, J.; SARGENTO, S. Media Independent Handovers: LAN, MAN and WAN Scenarios. Globecom Workshops, 2009 IEEE

[39] W. RICHARD STEVENS, BILL FENER, ANDREW M. RUDOFF. UNIX Network Programming: The Sockets Networking API. Addinson-Wesley, 2004. 991 p.