

Nivia Cruz Quental

CPMIPv6: Uma Extensão do PMIPv6 para Mobilidade IP Interdomínio

Brasil

2015

Nivia Cruz Quental

CPMIPv6: Uma Extensão do PMIPv6 para Mobilidade IP Interdomínio

Proposta de Tese apresentada ao Programa de Pós-Graduação do Centro de Informática da UFPE como requisito parcial para obtenção do grau de Doutor em Ciência da Computação.

Universidade Federal de Pernambuco – UFPE

Centro de Informática

Programa de Pós-Graduação

Orientador: Paulo André da Silva Gonçalves

Brasil

2015

Esta tese é dedicada à minha família e todos aqueles que enfrentam dificuldades para desenvolver pesquisa relevante.

Agradecimentos

Agradeço a Deus, cuja presença sinto nos momentos de maior incerteza, mas também no amor à minha volta e no êxtase da descoberta.

Agradeço aos meus pais Roberto e Ozita Quental; meus irmãos Roberto e Jamilly Quental; meus primos, tios, cunhados e avós, pela companhia constante e encorajamento durante toda a minha trajetória.

Agradeço ao meu orientador Paulo Gonçalves, pelo curto, porém precioso tempo dedicado à me tornar uma pesquisadora melhor.

Agradeço aos meus grandes amigos Érica Teixeira e Fernando Aires pelos conselhos e exemplo de ética e competência em suas áreas de atuação.

Agradeço aos parceiros e amigos do projeto CIn/Samsung, pelas oportunidades de aprendizado técnico e compartilhamento de experiências e pela amizade.

Agradeço aos amigos que fiz durante minha formação no CEFET-PE (atual IFPE) e na Escola Politécnica de Pernambuco, por todos os momentos de companheirismo e aprendizado.

*Toda geração tem uma chance para mudar o mundo
Pobre da nação que não ouve seus meninos e meninas
Pois a melodia mais doce é aquela que ainda não ouvimos
(I'll Go Crazy If I Don't Go Crazy Tonight - U2)*

Resumo

A evolução das telecomunicações trouxe a possibilidade de comunicação entre dispositivos móveis a longas distâncias. Avanços em pesquisas tanto na camada enlace quanto na camada de rede procuram promover a continuidade de sessões de voz entre redes heterogêneas. Na camada enlace, observa-se a definição de entidades específicas para a inter-comunicação entre diferentes tecnologias de acesso ou a utilização do padrão IEEE 802.21 como camada auxiliar nesse processo. Na camada de rede, as soluções de IP móvel são inerentemente independentes da tecnologia de enlace.

Especificamente, os estudos de mobilidade IP têm como principal desafio aliar interoperabilidade com eficiência e a possibilidade de expandir o gerenciamento entre diversos domínios. O protocolo PMIPv6 reduziu o *overhead* de comunicação conhecido do Mobile IP tornando locais as operações de gerenciamento de mobilidade, em detrimento da comunicação interdomínio. Assim, os padrões atuais de mobilidade IP derivados do PMIPv6 não oferecem suporte à mobilidade interdomínio. Este é um problema relevante e atual, uma vez que cenários veiculares com aplicativos de *live-streaming* transitando entre diferentes domínios ao longo do percurso são cada vez mais frequentes.

A presente proposta de tese apresenta o *ClusteredPMIPv6* (CPMIPv6) como uma extensão interdomínio ao PMIPv6. Seu caráter distribuído com mínimo de acréscimo de mensagens de sinalização permite que o PMIPv6 seja elevado à escala interdomínio sem perder as características que atestam a sua eficiência. O CPMIPv6 mantém a infraestrutura de rede original, sem introduzir entidades centralizadas, o que permite a convivência com sistemas PMIPv6 legados.

Um levantamento do Estado-da-Arte de soluções interdomínio é feito. Por meio de uma modelagem analítica, o CPMIPv6 é comparado à essas soluções. Observa-se que o CPMIPv6 é capaz de reduzir em 34% o custo de sinalização e a latência e em 50% a perda de pacotes no cenário avaliado. O *goodput* chega a 97% no cenário estudado, comprovando a eficiência da solução proposta.

Palavras-chaves: CPMIPv6. handover. interdomínio.

Abstract

Session continuity in long-distance communication among wireless devices is a reality due to advances in link layer and network layer research. In that scope, handover in heterogeneous networks is one of the most important issues. Link-layer handover solutions relies on specific entities for mobility management or considers the use of IEEE 802.21 standard as an auxiliary layer. Network-layer solutions inherently supports heterogeneous networks handover.

The main challenge in IP mobility research is to associate interoperability and efficiency to the expansion of the mobility management to several domains. PMIPv6 protocol is a Mobile IP extension that reduces communication overhead. It is accomplished through a local mobility management. However, that approach sacrifices interdomain mobility. Hence, standards derived from PMIPv6 does not support to interdomain handover. That is a relevant issue, since live-streaming applications in vehicular scenarios have become a reality.

This thesis proposal presents *Clustered* PMIPv6 (CPMIPv6) as an interdomain extension to PMIPv6. The CPMIPv6 is a distributed solution and adds minimum signaling and no extra tunneling. Those features gives interdomain scale to PMIPv6 and still maintains the PMIPv6 efficiency and its original infrastructure. It means that CPMIPv6 additionally allows interworking PMIPv6 legacy systems.

The State-of-the-Art on interdomain handover is further presented. Through analytic modeling, CPMIPv6 is compared to that solutions. Results show the CPMIPv6 efficiency. In the studied scenario, CPMIP reduces signaling cost and latency up to 34%. Additionally, packet loss is reduced up to 50% and goodput reaches 97% in the scenario studied.

Key-words: CPMIPv6. handover. interdomain.

Lista de ilustrações

Figura 1 – Exemplo de rede de acesso sem fio.	19
Figura 2 – Arquitetura de uma entidade MIH	25
Figura 3 – Comparison between the different implementations for the <code>t_atts()</code> function.	34
Figura 4 – Example of scheduler instance in our discrete-event simulator.	35
Figura 5 – Probabilidade de bloqueio de <i>handover versus</i> número de nós no cenário 1.	36
Figura 6 – Fração de nós bloqueados <i>versus</i> número de nós no cenário 1.	37
Figura 7 – Latência <i>versus</i> número de nós no cenário 1.	38
Figura 8 – Probabilidade de bloqueio de <i>handover versus</i> número de nós no cenário 2.	38
Figura 9 – Fraction of blocked nodes <i>versus</i> the number of MNs in Scenario 2.	39
Figura 10 – Latency <i>versus</i> the number of MNs in Scenario 2.	39
Figura 11 – Arquitetura do Mobile IP.	41
Figura 12 – Fluxo de mensagens do Mobile IP.	42
Figura 13 – Arquitetura do PMIPv6.	43
Figura 14 – Fluxo de mensagens do PMIPv6.	43
Figura 15 – Fluxo de mensagens do FPMIPv6 no modo preditivo.	45
Figura 16 – Fluxo de mensagens do FPMIPv6 no modo reativo.	45
Figura 17 – <i>Handover</i> interdomínio no esquema de Park <i>et al.</i>	50
Figura 18 – <i>Handover</i> interdomínio no esquema I-PMIPv6.	50
Figura 19 – <i>Handover</i> interdomínio no esquema EIMHP.	51
Figura 20 – Handover interdomain in No-Gap scheme.	52
Figura 21 – Domains in CPMIPv6.	54
Figura 22 – Registro no CPMIPv6.	55
Figura 23 – Desregistro no CPMIPv6.	55
Figura 24 – Handover intradomínio no CPMIPv6.	56
Figura 25 – Handover interdomínio no CPMIPv6.	56
Figura 26 – Um domínio com sete subredes.	62
Figura 27 – Topologia e distâncias em saltos.	62
Figura 28 – Custo de sinalização <i>versus</i> β	63
Figura 29 – Custo <i>versus</i> SMR.	64
Figura 30 – Custo <i>versus</i> velocidade.	65
Figura 31 – Latência <i>versus</i> probabilidade de falha no meio sem fio.	65
Figura 32 – Perda de pacotes <i>versus</i> probabilidade de falha no meio sem fio.	66
Figura 33 – <i>Goodput versus</i> SMR.	67
Figura 34 – <i>Goodput versus</i> wireless failure probability.	67

Lista de tabelas

Tabela 1 – Parâmetros dos experimentos	34
Tabela 2 – Armazenamento dos 128 <i>k-buckets</i>	57
Tabela 3 – Mensagens de cada esquema de <i>handover</i> interdomínio	61
Tabela 4 – Evaluation parameters	63

Lista de abreviaturas e siglas

AAA *Authentication, Authorization, and Accounting.*

CDMA *Code Division Multiple Access.*

CHT *Channel Holding Time.*

CoA *Care-of Address.*

CPMIPv6 *Clustered Proxy Mobile IPv6.*

DHT *Distributed Hash Table.*

DS-WCDMA *Direct-Sequence WCDMA.*

EBB *Entry Before Break.*

EDGE *Enhanced Data rates for GSM Evolution.*

FA *Foreign Agent.*

FBSS *Fast Base Station Switch.*

FCS *Fast Cell Selection.*

FDM *Frequency Division Multiplexing.*

FDMA *Frequency Division Multiple Access.*

FMIP *Mobile IPv6 Fast Handovers.*

FPMIPv6 *Fast Handovers for Proxy Mobile IPv6.*

GPRS *General Packet Radio Service.*

GSM *Global System for Mobile Communications.*

GVHO *Group Vertical Handover ou Handover Vertical em Grupo.*

HA *Home Agent.*

HHO *Hard Handover.*

HMIPv6 *Hierarchical Mobile IPv6.*

ICMP *Internet Control Message Protocol.*

IEEE *Institute of Electrical and Electronics Engineers.*

IETF *Internet Engineering Task Force.*

IGMP *Internet Group Management Protocol.*

IINR *Interference to other Interferences-plus-Noise Ratio.*

IMS *IP Multimedia Subsystem.*

IP *Internet Protocol.*

IPv4 *IP, versão 4.*

IPv6 *IP, versão 6.*

LMA *Local Mobility Anchor.*

LR *Localized Routing.*

MAG *Mobile Access Gateway.*

MDHO *Macro-Diversity Handover.*

MICS *Media Independent Command Service.*

MIES *Media Independent Event Service.*

MIHF *Media Independent Handover Function.*

MIIS *Media Independent Information Service.*

MIP *Mobile IP.*

OFDMA *Orthogonal Frequency Division Multiple Access.*

PDU *Packet Data Unit.*

PMIPv6 *Proxy Mobile IPv6.*

QoS *Quality of Service.*

RSS *Relative Signal Strength.*

SAP *Service Access Point.*

SHO *Soft Handover.*

SIP *Session Initiation Protocol.*

SIR *Signal-to-interference ratio.*

SMR *Session-to-Mobility Ratio.*

SOFDMA *Scalable OFDMA.*

TDM *Time Division Multiplexing.*

TPMIPv6 *Transient Binding for Proxy Mobile IPv6.*

UMTS *Universal Mobile Telecommunication System.*

VHO *Vertical Handover ou Handover Vertical.*

VoIP *Voice over IP.*

Sumário

	Introdução	14
1	GERÊNCIA DE MOBILIDADE NA CAMADA ENLACE	18
1.1	Sistemas de Comunicações sem fio	18
1.2	<i>Handover</i>	20
1.2.1	Critérios para Descoberta	21
1.2.2	Critérios de Decisão	22
1.2.3	Mecanismos de Execução	23
1.2.4	Métricas de Avaliação de Desempenho	24
1.3	Media Independent Handover (MIH)	24
1.4	Trabalhos Relacionados	26
1.4.1	Trabalhos relacionados ao <i>handover</i> tradicional	26
1.4.2	Trabalhos relacionados ao VHO	27
1.4.3	Trabalhos relacionados ao GVHO	28
1.5	Uma Estratégia de Tentativas para GVHO	29
1.5.1	Esquema de GVHO de referência	30
1.5.2	Política para tentativas de requisição de GVHO	33
1.5.3	Avaliação de desempenho	34
1.5.4	Resultados para o cenário 1	36
1.5.5	Resultados para o cenário 2	37
2	GERÊNCIA DE MOBILIDADE IP	41
2.1	Mobilidade IP	41
2.1.1	Mobile IP (MIP)	41
2.1.2	Proxy Mobile IPv6 (PMIPv6)	42
2.1.3	Fast Handovers for Proxy Mobile IPv6 (FPMIPv6)	44
2.1.4	Otimizações para a Mobilidade IP	45
2.2	Mobilidade IP Interdomínio	46
2.3	Trabalhos relacionados	47
2.3.1	Trabalhos relacionados ao MIP	47
2.3.2	Trabalhos relacionados ao PMIPv6 e FPMIPv6	48
2.3.3	Trabalhos relacionados à <i>handover</i> interdomínio	49
2.3.3.1	Abordagem sem otimização	49
2.3.3.2	Abordagem baseada no LMA como âncora de sessão	49
2.3.3.3	Abordagem baseada em entidades centrais	50
2.3.3.4	Abordagem baseada em especialização de MAG	51

3	<i>CLUSTERED PMIPv6</i>(CPMIPv6)	53
3.1	Análise crítica do Estado-da-Arte em <i>handover</i> interdomínio	53
3.2	Arquitetura do CPMIPv6	54
3.2.1	Sinalização do CPMIPv6	54
3.2.2	Gerenciamento do <i>cluster</i> do CPMIPv6	56
4	AVALIAÇÃO DE DESEMPENHO E RESULTADOS	58
4.0.3	Modelagem	58
4.0.3.1	Mobilidade	58
4.0.3.2	Métricas	58
4.0.3.3	Modelagem das soluções interdomínio	60
4.0.4	Cenários e parâmetros	60
4.0.5	Resultados	62
	Conclusão	68
	Referências	70
	Glossário	77

Introdução

Um projeto de redes móveis contempla em geral especificações das tecnologias de acesso, planejamento da topologia, distribuição de entidades de rede e protocolos para gerenciamento de mobilidade. No âmbito da mobilidade, o *handover* interdomínio eficiente em redes heterogêneas ainda é uma questão em aberto. No presente capítulo são apresentadas as motivações para a pesquisa nessa área, as hipóteses levantadas, os objetivos e a estrutura da proposta de tese.

Motivação

Handover (ou *handoff*) é o processo que permite a um nó móvel manter o seu fluxo de tráfego mediante a mudança de enlace (802.21, 2008). Esse processo pode ser iniciado pelo próprio nó móvel ou pelo seu ponto de acesso (*Point of Attachment* - PoA). Essa mudança precisa ocorrer de forma transparente ao usuário, sendo o custo de sinalização, a latência e a perda de pacotes fatores críticos de desempenho.

Recentemente, o conceito de *handover* não tem sido mais apenas ligado à continuidade de uma chamada telefônica, mas também à continuidade de sessões de *streaming* e à manutenção de QoS e do acesso à Internet. A variedade de aplicativos disponíveis para *tablets* e *smartphones* inclui aplicativos de teleconferências, compartilhamento de vídeos e monitoramento de dispositivos em tempo real, entre outros. Adicionalmente, o cenário de mobilidade em variadas velocidades com aplicativos em uso tem sido cada vez mais comum. Nesses casos, o *handover* tem papel fundamental no desempenho e bom funcionamento desses aplicativos.

As novas gerações de *tablets* e *smartphones* trazem também ao usuário o suporte a diversas tecnologias sem fio como 3G, WiMAX, Wi-Fi e LTE em um mesmo aparelho. Isso permite extrapolar o conceito de transferência de um canal para outro em uma mesma tecnologia para o *handover* em redes heterogêneas. Nesse novo cenário, a necessidade de se manter a sessão do usuário permanece, encorajando novas pesquisas na área de *handover* vertical (*Vertical Handover* - VHO) (SHEN; ZENG, 2008) (STEVENS-NAVARRO; LIN; WONG, 2008) (CAI; LIU, 2008) (LEE et al., 2009b) (TANIUCHI et al., 2009) (CICCONETTI; GALEASSI; MAMBRINI, 2010) (ANDERSSON; FORTE; SCHULZRINNE, 2010) (LEE; CHO, 2011) (KIM; KIM, 2011) (ZEKRI; JOUABER; ZEGHLACHE, 2012) (JEONG et al., 2012) (QUENTAL; GONÇALVES, 2014a).

O padrão IEEE 802.21 (TANIUCHI et al., 2009), o qual descreve o *handover* in-

dependente de mídia (*Media Independent Handover* - MIH), é um esforço que busca padronizar a troca de mensagens necessárias para a realização de VHO na camada enlace. O principal objetivo é estabelecer um mapeamento de eventos e mensagens de controle garantindo a transparência do *handover* entre diferentes tecnologias. O MIH em sua implementação atual contempla funções de descoberta, *triggers* para execução de *handover* e um conjunto de consultas para obter informações das redes candidatas. Detalhes do processo de decisão e execução de *handover* devem ser providos pelos grupos de interesse que adotarem o padrão.

O *handover* na camada enlace, entretanto, pode não ser suficiente para que se conservem os dados de uma sessão. Caso o nó móvel siga além das fronteiras de sua rede de acesso, é necessário atualizar as tabelas de roteamento, as informações de autenticação e a nova localização do nó móvel. Esse é um cenário bastante comum, quando se considera tecnologias veiculares, em casos de uso que envolvem automóveis, trens e ônibus com pessoas utilizando os seus dispositivos enquanto percorrem longas distâncias.

Para tal, o IETF (*Internet Engineering Task Force*) adicionou o suporte à mobilidade aos protocolos IPv4 e IPv6, com a especificação do *Mobile IP* MIP (JOHNSON; PERKINS; ARKKO, 2004). O MIP permite que o nó conserve seu endereço IP inicial, mesmo que saia da sua área de cobertura de origem (ZEKRI; JOUABER; ZEGHLACHE, 2012). Assim como na camada enlace, o processo de *handover* no nível IP pode resultar em atrasos que prejudicam a experiência do usuário e operações com alto consumo de energia no dispositivo móvel. Para tratar destes problemas, o IETF também tem proposto extensões ao MIP, como o *Mobile IPv6 Fast Handovers* (KODLI, 2009)(FMIP), o *Proxy Mobile IPv6*(PMIPv6) (GUNDAVELLI et al., 2008), e o *Fast Handovers for Proxy Mobile IPv6*(FPMIPv6) (YOKOTA et al., 2011).

No âmbito de mobilidade IP, um desafio atual é o suporte ao *handover* interdomínio (TAGHIZADEH et al., 2012). O MIP permite o deslocamento entre diferentes domínios, contudo, a presença de uma única entidade âncora disponível para gerenciar a mobilidade do nó torna o protocolo pouco escalável. As extensões *Proxy* de MIP possuem a vantagem de hierarquizar o controle de mobilidade, contudo, eliminam o caráter interdomínio do MIP, tendo como premissa a mobilidade em um domínio único.

Diversas propostas para *handover* interdomínio tem sido apresentadas na literatura (PARK E. LEE; NOH; KIM, 2010) (ZHONG et al., 2010) (NEUMANN et al., 2009) (JOE; LEE, 2012). Park *et al.* (PARK E. LEE; NOH; KIM, 2010) propõem um esquema de repasse de mensagens de sinalização do PMIPv6 entre domínios vizinhos passando pelas entidades âncoras de cada domínio. Contudo, a necessidade introdução de um túnel extra e a duplicação de mensagens de sinalização promovem a degradação do desempenho. A proposta de Zhong *et al.* (ZHONG et al., 2010) requer a introdução de uma entidade centralizadora para manter a informação dos nós durante a visita a novos domínios. A

presença da entidade centralizadora reduz a sinalização necessária para o *handover*. Entretanto, isso implica na introdução de um ponto único de falha, ameaçando a robustez do sistema, além de causar uma mudança expressiva na infraestrutura de rede do PMIPv6. Newmann *et al.* (NEUMANN *et al.*, 2009) propõe manter a entidade âncora de origem durante o *handover* interdomínio. Contudo, a dependência de uma entidade centralizadora persiste, uma vez que se faz necessária a existência de uma entidade que controle a localização do nó móvel. Joe e Lee (JOE; LEE, 2012) propõem a especialização de entidades de mobilidade na fronteira entre dois domínios, otimizando a sinalização. Uma vez que essa proposta requer adicionalmente modificação nos roteadores de borda, ela apresenta obstáculos à integração com sistemas legados devido à mudança na infraestrutura de rede, assim como as propostas anteriores.

Desta forma, faz-se necessária a proposta de uma solução para *handover* interdomínio que alie eficiência, tolerância a falhas e compatibilidade com as arquiteturas de rede pré-existentes.

O CPMIPv6

O *Clustered PMIPv6* (CPMIPv6) é uma extensão ao PMIPv6 que busca atingir os requisitos de eficiência, tolerância a falhas e retro-compatibilidade no suporte à *handover* interdomínio. O CPMIPv6 utiliza um conjunto mínimo de mensagens além daquelas utilizadas no PMIPv6 para gerenciamento dos nós além do domínio de origem. Consiste na formação de um *cluster* de entidades-âncora pertencentes a cada domínio, que se comunicam seguindo uma lógica de DHT derivada da tecnologia *Kademlia* (MAYMOUNKOV; MAZIERES, 2002). A natureza escalável do *Kademlia* permite que o CPMIPv6 seja executado em domínios de diversos tamanhos e crie *backups* em caso de falhas. A simplicidade do protocolo requer alterações mínimas na configuração de entidades já existentes em uma rede legada. Assim, o CPMIPv6 é uma solução de *handover* interdomínio eficiente e que atende os requisitos de desempenho de uma aplicação de voz durante essa operação.

Objetivos

O objetivo geral da tese é prover *handover* interdomínio eficiente e robusto em uma arquitetura distribuída respeitando a infraestrutura de sistemas legados. A presente proposta de tese tem o objetivo de apresentar as premissas do CPMIPv6 e os primeiros resultados decorrentes de sua avaliação. Nesse âmbito, os objetivos específicos da proposta de tese são apresentados a seguir:

- Propor o CPMIPv6 como uma extensão interdomínio ao protocolo PMIPv6;

- Propor um controle distribuído da mobilidade, com modificações mínimas na sinalização do PMIPv6 e sem adição de túneis;
- Garantir a compatibilidade com a infraestrutura legada do PMIPv6;
- Redução de custo, latência, perda de pacotes e melhoria do *goodput* em comparação às demais propostas do Estado-da-Arte.

Organização da Proposta de Defesa

No presente Capítulo foi apresentada a motivação e os objetivos da proposta de tese. No Capítulo 1 é apresentado um panorama das principais tecnologias de acesso de quarta geração, bem como soluções para *handover* vertical na camada enlace. O Capítulo 2 apresenta o Estado-da-Arte das soluções para *handover* na camada IP e os desafios do *handover* interdomínio. O Capítulo 3 apresenta o CPMIPv6 e suas características. O Capítulo 4 descreve a metodologia utilizada e os resultados dos experimentos. Finalmente, são apresentadas em seguida, as conclusões da proposta e os encaminhamentos para o desenvolvimento da tese.

1 Gerência de Mobilidade na Camada Enlace

A evolução dos sistemas de telecomunicações desde ligações cabeadas entre poucos usuários até as complexas redes sem fio trouxe a necessidade de pesquisas por novas técnicas avançadas de *handover*. Neste capítulo, serão apresentadas as técnicas de *handover* utilizadas na camada enlace, bem como as principais questões relacionadas ao VHO e o padrão MIH enquanto tecnologia auxiliar para a realização de *handover* entre diferentes tecnologias.

1.1 Sistemas de Comunicações sem fio

A arquitetura dos sistemas de redes sem fio possuem variações de acordo com o tipo de tecnologia empregada e as aplicações às quais se destinam. Entretanto, pode-se distinguir duas configurações:

- Infraestruturada, onde os dispositivos móveis se comunicam por meio de uma ou mais infraestruturas com papel de ponto de acesso;
- *Ad Hoc*, onde os dispositivos móveis realizam conexões entre si sem auxílio de uma infraestrutura, geralmente em caráter temporário.

As redes metropolitanas sem fio possuem a arquitetura infraestruturada e atualmente suportam uma grande quantidade de usuários simultaneamente graças à divisão da área de cobertura em células, fazendo reuso de frequências. Adicionalmente, mecanismos de multiplexação por tempo, código e frequências ortogonais são empregados, garantindo altas taxas de transferência. Para manter essa estrutura em funcionamento, a arquitetura das atuais redes móveis de forma geral inclui:

- Nós móveis, clientes do sistema;
- PoAs , para controle dos nós móveis a seu alcance;
- Rede de acesso sem fio que conecta PoAs e nós móveis;
- Entidades de gerência de mobilidade e de PoAs;
- Entidades de acesso à rede externa (Internet ou outros serviços).

A Figura 1 apresenta um exemplo de rede metropolitana sem fio.

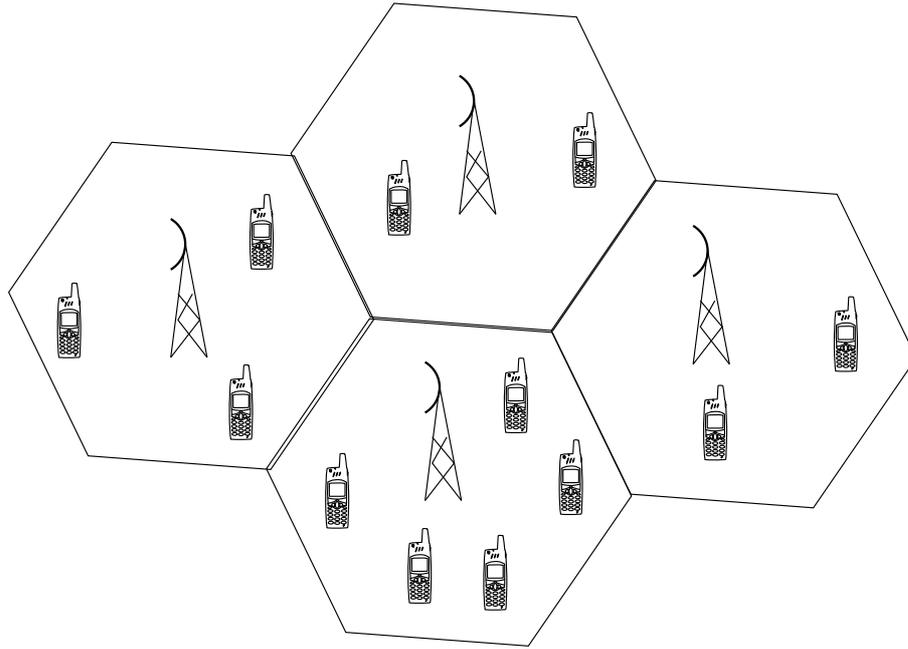


Figura 1 – Exemplo de rede de acesso sem fio.

De acordo com (NOBREGA, 2011), as gerações mais antigas de sistemas celulares foram projetadas para o tráfego de voz. Os sistemas 1G eram analógicos e usavam o modo de acesso FDMA; os sistemas 2G evoluíram para suportar transporte de dados utilizando o padrão GSM, sendo esta uma combinação dos esquemas TDM e FDM de multiplexação; a compatibilidade com as redes IP foi obtida nas gerações 2,5G (com os padrões EDGE e GPRS) e 3G, que introduziu a tecnologia UMTS com o modo de acesso DS-WCDMA, permitindo aumentar as taxas de transferência. A geração 4G propõe o padrão LTE, que oferece suporte a múltiplas interfaces e utiliza o modo de acesso OFDMA. O 4G funciona de maneira semelhante à rede IEEE 802.16.

Segundo (FIGUEIREDO; PEREIRA, 2008), os diferenciais das tecnologias de quarta geração são:

- Infraestrutura mais simples em comparação com os sistemas 3G baseados em CDMA;
- Rede totalmente IP;
- Tolerância à distorções causadas por multipercurso;
- Uso dinâmico do espectro com seleção de canais e aumento da largura espectral sob demanda por meio do método de acesso SOFDMA;
- Mecanismos de criptografia;
- Implementação de QoS.

1.2 Handover

O principal objetivo do *handover* é manter a continuidade de um serviço ao mesmo tempo em que efetua mudanças de rede decorrentes de movimentação do usuário de maneira transparente. A crescente popularização de dispositivos com interfaces para diferentes tecnologias permite expandir essa continuidade em redes heterogêneas, caracterizando o *Vertical Handover* ou Handover Vertical (VHO). Na maioria das tecnologias sem fio, o *handover* ocorre quando a potência recebida pelo nó móvel decai abaixo de um limiar ou quando o mesmo se distancia excessivamente de seu PoA de origem. No caso de VHO, os critérios podem envolver outras características das diferentes tecnologias disponíveis. Dependendo da implementação, o *handover* pode ser requisitado pelo nó móvel, ou pelo seu PoA, dependendo da implementação da tecnologia. De acordo com (ZEKRI; JOUABER; ZEGHLACHE, 2012), o processo de *handover* se divide em três etapas:

- *Descoberta* - Momento em que se faz a descoberta de serviços e a coleta de informações do estado da rede. Nessa etapa também se utiliza um critério específico para detectar a necessidade de *handover*, como potência, taxa de transmissão, carga sobre um PoA, nível de bateria, entre outros.
- *Decisão* - Durante essa etapa, as redes disponíveis são avaliadas com base nos dados coletados na etapa anterior e um algoritmo de decisão escolhe o PoA-alvo.
- *Execução* - Nessa etapa, mensagens de controle são trocadas entre nó móvel, PoA-alvo e PoA de origem para realizar a mudança de enlace. A execução deve causar o mínimo de interrupção possível na comunicação, de modo a parecer imperceptível ao usuário. Essa etapa é fortemente dependente das tecnologias de acesso envolvidas.

Por outro lado, em Kim *et al.* (KIM et al., 2010) consideram quatro fases para a realização do *handover*:

- *Iniciação* - Correspondente às etapas detecção e decisão;
- *Preparação* - Referente à troca de mensagens entre PoA de origem e PoA-alvo para reserva de recursos necessária para a mudança de enlace;
- *Execução*;
- *Finalização* - Liberação de recursos do PoA anterior.

Ambas as classificações são amplamente adotadas na literatura, com pequenas ressalvas quanto à finalização de uma etapa e o início de outra (LEE; CHO, 2011),

(LAMPROPOULOS; SALKINTZIS; PASSAS, 2008), (SILVA et al., 2012), (CICCONETTI; GALEASSI; MAMBRINI, 2010).

1.2.1 Critérios para Descoberta

Em qualquer esquema de *handover*, considera-se que o ambiente sem fio é constantemente monitorado, seja pela rede ou pelo nó móvel. Mudanças expressivas nas condições desse ambiente podem disparar requisições de *handover*. Os critérios a seguir são os mais tradicionalmente empregados na fase de descoberta (ZEKRI; JOUABER; ZEGHLACHE, 2012) (POLLHI, 1996):

- *Relative Signal Strength* (RSS) - Detecta o PoA com sinal mais potente. Costuma causar *handovers* desnecessários quando o PoA de origem ainda possui sinal adequado;
- RSS com limiar - O *handover* é iniciado apenas quando o RSS do PoA de origem assume um valor abaixo de um limiar predeterminado e existe um candidato com RSS maior. Em áreas de sobreposição, essa informação pode não ser suficiente para determinar qual dos PoAs possui melhor qualidade de sinal;
- RSS com histerese - Apenas determina que uma rede possui melhores condições que outra quando a diferença entre os RSSs ultrapassa um valor predeterminado. Essa técnica evita o efeito *ping-pong*, onde o nó constantemente realiza *handover* saindo e retornando ao PoA de origem devido à flutuação do RSS.
- RSS com limiar e histerese - Uma combinação dos dois critérios anteriores;
- Técnicas de previsão - Procura prever valores futuros de RSS.

Risco de segurança, largura de banda disponível e carga sobre PoAs são geralmente encontrados em propostas para VHO (ZEKRI; JOUABER; ZEGHLACHE, 2012). Esses critérios levam em consideração a conversão entre tecnologias e o balanceamento de carga na rede. Alguns critérios de descoberta incluem avaliação não apenas do PoA, mas também da qualidade do enlace. Uma métrica conhecida é o *Signal-to-Interference Ratio* (SIR), que define o grau de interferência co-canal, um dos maiores causadores da degradação de desempenho. Outra importante métrica para avaliar o enlace é o *Bit Error Rate* (BER), que determina a confiabilidade de um canal para aplicações que requerem baixa tolerância a perdas.

Padrões de redes metropolitanas sem fio comumente deixam a critério dos fabricantes de dispositivos e dos consórcios dos quais participam definir a métrica utilizada para descoberta do *handover*.

1.2.2 Critérios de Decisão

Além dos mecanismos de descoberta, é possível que seja necessário escolher um PoA entre uma lista de candidatos. Em esquemas mais simples, a etapa de descoberta é suficiente para a escolha do PoA-alvo. No caso do VHO, porém, a fase de decisão é mais influente no desempenho, pois utiliza esquemas mais sofisticados, que recebem como entrada as informações coletadas na etapa anterior. Os critérios podem ser os mais diversos, como a largura de banda disponível nas redes candidatas, QoS esperada, consumo de bateria, entre outros. O tipo de tráfego (voz ou dados) utilizado no momento é um fator determinante na adoção desses critérios.

As principais abordagens de decisão de *handover* adotadas na literatura envolvem:

- *Uso de uma entidade centralizadora* (NIYATO; HOSSAIN, 2009) (NING et al., 2013) - A gerência do *handover* é responsabilidade de uma *relay station*, retirando a complexidade dos nós móveis, além de diminuir o grau de incerteza e garantir um desempenho melhor que a abordagem descentralizada. Um ponto negativo é a pouca tolerância a falhas;
- *Algoritmos distribuídos* (LEI; HUI; ZHENG, 2010) - Utiliza técnicas conhecidas de paralelismo e sincronização. São geralmente de fácil compreensão, porém limitados quanto à adaptabilidade a novos cenários;
- *Atrasos aleatórios* (CAI; LIU, 2008) - Estações móveis optam por tentar o *handover* após um intervalo de tempo aleatório, evitando que tentativas simultâneas de *handover* ocorram. Trata-se de um subtipo de algoritmo distribuído muito utilizado em pesquisas da área;
- *Aprendizado por reforço* (NIYATO; HOSSAIN, 2009) - O emprego de técnicas de Inteligência Artificial (IA) permite que os nós aprendam mais sobre a rede à medida que realizam tentativas de *handover*. Esta abordagem não requer interação com outros nós, porém pode gerar problemas de desempenho;
- *Teoria de jogos* (CAI; LIU, 2008) (NIYATO; HOSSAIN, 2009) - Mapeia os cenários de *handover* em jogos cooperativos ou não-cooperativos, onde os nós são jogadores interessados em obter o seu *payoff*. O *payoff* pode ser uma maior largura de banda, um gasto menor de energia ou maior segurança. O equilíbrio de Nash é a situação desejada, onde todos os nós não possuem mais estratégias para obter um melhor *payoff*, garantindo o equilíbrio. A principal vantagem é o mapeamento quase perfeito de um cenário de GVHO em modelos competitivos da Teoria de Jogos. Por outro lado, nem sempre é possível a consideração de parâmetros adicionais no modelo;
- *Derivação de problemas de otimização* (LEE; CHO, 2011) - A decisão é modelada com equações matemáticas acompanhadas de uma condição pré-determinada. A par-

tir daí, o problema é solucionado para encontrar o valor ideal para as variáveis dessas equações. Requerendo uma modelagem mais complexa, a derivação para problemas de otimização é mais flexível que a abordagem de Teoria de Jogos.

A fase de decisão é ainda mais importante nas pesquisas de *Handover* Vertical em Grupo (*Group Vertical Handover* - GVHO), um caso particular de VHO onde vários nós realizam *handover* simultaneamente. Quando não são consideradas as consequências advindas da escolha de uma rede em favor de outra ou quando se restringe a decisão de *handover* à preferência individual, os resultados podem ser desastrosos do ponto de vista de desempenho. Decisões equivocadas podem levar várias estações móveis a optar pela mesma rede ou por uma rede que não seja adequada às suas necessidades, causando uma alocação de recursos ineficiente, além de prejudicar o desempenho dos demais usuários.

1.2.3 Mecanismos de Execução

Para execução de *handover*, a implementação do *Hard Handover* (HHO) é obrigatória em todas as tecnologias. Nesse caso, o nó móvel apenas entra em contato com seu PoA-alvo uma vez que se desconecta do seu PoA de origem. Durante essa fração de tempo em que o nó móvel se encontra sem comunicação com nenhum PoA, pacotes podem ser perdidos. Desta forma, mecanismos opcionais de *Soft Handover* (SHO) (KIM et al., 2010) (FIGUEIREDO; PEREIRA, 2008) tem sido implementados nas recentes tecnologias de redes móveis para evitar essa ruptura súbita de comunicação, com:

- *Seamless Handover* - Procedimento que consiste em permitir que o nó móvel troque informações com um PoA candidato antes de escolhê-lo como alvo. Caso seja escolhido, o tempo de interrupção de comunicação é reduzido;
- EBB (*Entry Before Break*) - A interrupção da comunicação com o PoA de origem ocorre apenas após o fim da execução do *handover* para o PoA-alvo;
- *Handover* Multiportadora - Quando suportado pela tecnologia de acesso, o nó móvel mantém comunicação com PoA de origem e PoA-alvo em portadoras diferentes, permitindo conexões simultâneas;
- FBSS (*Fast Base Station Switch*) ou FCS (*Fast Cell Seleccion*) - Neste esquema, o nó mantém uma lista de PoAs denominada *Active Set* e periodicamente seleciona uma delas como âncora, para trocar mensagens de controle. desta forma, a troca de PoA ocorre de maneira simplificada, sem a necessidade de mensagens explícitas;
- MDHO (*Macro-Diversity Handover*)- Se diferencia do anterior por permitir que o nó se comunique com os PoAs do *Active Set*.

1.2.4 Métricas de Avaliação de Desempenho

De acordo com (POLLHI, 1996), as métricas comumente utilizadas para avaliar o desempenho de um esquema de *handover* são:

- Probabilidade de bloqueio de chamada - probabilidade de se impedir a realização de uma nova chamada;
- Probabilidade de bloqueio de *handover* - probabilidade de uma requisição de *handover* ser recusada pela rede;
- Probabilidade de *handover* - probabilidade de um *handover* ser requisitado antes do fim de uma sessão;
- Probabilidade de perda de chamada - probabilidade de uma sessão se encerrar devido à falha no *handover*;
- Probabilidade de *handover* desnecessário - probabilidade de um esquema incentivar o *handover* quando o *link* atual ainda é adequado;
- Taxa de *handover* - Número de *handovers* realizados em uma unidade de tempo ou por chamada. Pode ajudar a estimar a probabilidade de *handover*;
- Duração da interrupção - Tempo em que o nó móvel não se comunica com nenhum PoA durante o *handover*;
- Número de pacotes perdidos - Quantidade de *Packet Data Unit* (PDU) não entregues ao destino devido à interrupção causada pelo *handover*;
- Custo do *handover* - Quantidade de mensagens de controle enviadas e recebidas para realizar o *handover*;
- *Goodput* - Métrica que relaciona a quantidade de tráfego útil e o tráfego total em uma sessão;
- Latência de *handover* - Tempo decorrido desde a iniciação até a conclusão do *handover*.

1.3 Media Independent Handover (MIH)

O padrão IEEE 802.21 (TANIUCHI et al., 2009) descreve o *handover* independente de mídia (*Media Independent Handover* - MIH), o qual pode auxiliar na determinação de critérios para descoberta e decisão de *handover*. O MIH é uma camada de abstração comum entre tecnologias de enlace que permite que redes heterogêneas possam trocar informações e realizar o *handover*. O MIH é um padrão relativamente recente e

o seu emprego ainda enfrenta desafios relacionados ao mapeamento de primitivas dependentes da tecnologia, bem como questões de segurança, incorporação em esquemas de *handover* legados, gerenciamento de energia, e armazenamento de dados das redes para posterior envio.

O MIH requer que cada tecnologia de acesso provenha sua implementação do padrão e a correspondência entre mensagens MIH e primitivas da rede. Os principais elementos do MIH são:

- *MIH Function* (MIHF) - Módulo que detecta mudanças e controla o estado do enlace e provê informações de vizinhança;
- *Service Access Points* (SAPs) - Módulo que define interfaces dependentes e independentes de mídia;
- *MIH Users* - Quaisquer entidades da rede que utilizem ou consultem os serviços de MIH. Os usuários do MIH geralmente são os nós móveis, PoAs e eventuais entidades que provêm informações de outras redes.

A Figura 2 apresenta a arquitetura de uma entidade . A sua MIHF é usada para na comunicação com a MIHF de outras entidades, reportando eventos da tecnologia de enlace ou enviando/recebendo comandos por meio das primitivas dependentes de mídia. O mapeamento entre essas primitivas e mensagens MIH é feito por meio dos SAPs.

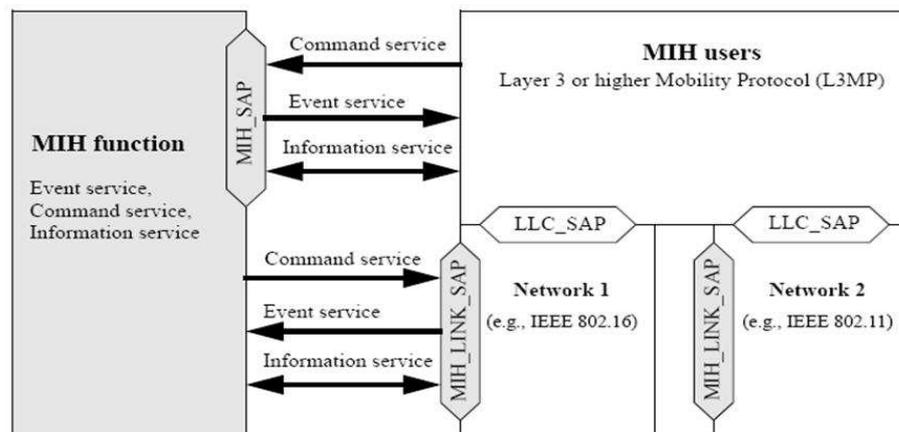


Figura 2 – Arquitetura de uma entidade MIH

O MIHF divide-se em três serviços: o *Media Independent Event Service* (MIES), que detecta mudanças na camada enlace e dispara gatilhos para camadas superiores; o *Media Independent Command Service* (MICS), que controla propriedades do enlace e o *Media Independent Information Service* (MIIS), que provê informações de rede para ser usado em esquemas de decisão. Um cenário de *handover* com MIH pode ter como premissa a existência do MIIS para auxiliar os nós móveis a obter informações de vizinhança, evitando que ele utilize seus próprios recursos de busca, economizando energia.

O MIH tem sido utilizado amplamente em pesquisas relacionadas a descoberta e decisão de *handover* (LEE; CHO, 2011) (BAE; CHUNG; SO, 2011) (KHAN; ANDRESEN, 2012) (LIANG; CHANG; CHEN, 2011) (SILVA et al., 2012).

1.4 Trabalhos Relacionados

Nesta seção, são apresentados os trabalhos relacionados ao *handover* tradicional, ao VHO e ao GVHO na camada enlace.

1.4.1 Trabalhos relacionados ao *handover* tradicional

Kim *et al.* apresentam o Estado da Arte dos esquemas de *handover* com destaque às tecnologias IEEE 802.16m e 3GPP LTE-Advanced, além de apresentar as novas propostas que vem sendo analisadas por estes consórcios (KIM et al., 2010). De acordo com os autores, as referidas tecnologias precisam considerar o trânsito entre zonas legadas e zonas com a nova tecnologia e negociação entre estações-base para garantir a integridade de dados.

No contexto de algoritmos de decisão Choi (CHOI, 2010) propõe uma nova métrica para selecionar estações-base para *handover*: o *Interference to other Interferences-plus-Noise Ratio* (IINR). Neste trabalho o foco está em melhorar o desempenho em termos de *throughput*. O artigo traz a questão da interferência entre células durante o *handover* e aponta os esquemas baseados em cooperação como uma boa solução para evitar este problema. Por outro lado, a cooperação deve ser projetada com cautela, uma vez que a seleção do dispositivo móvel que fará o *handover* poderá influenciar no desempenho geral da rede, já que células adjacentes participam deste processo. O artigo propõe um esquema de decisão para os métodos *Soft Handover* e o *Fast Cell Selection*. Neste esquema, o dispositivo móvel só realiza o *handover* se houver ganho de *throughput*. Para tal, utiliza a métrica proposta IINR. Os autores observaram por meio de simulação que houve melhoria do *throughput* nos cenários estudados.

O *handover* rápido em redes sem fio *multicast* é o tema do trabalho de Koh *et al.* (KOH; GOHAR, 2010). Os autores argumentam que o esquema atualmente utilizado realiza transmissões de dados desnecessárias originadas por operações de *leave* e *join* do protocolo IGMP, aumentando o atraso. Neste trabalho é proposta a implantação de *Multicast Handover Agents* (MHAs) nas estações-base, realizando uma otimização destas operações. Experimentos com simulação numérica mostraram que o atraso se reduziu nos cenários avaliados.

A preocupação com a economia de energia é destaque no artigo de Hunukumbure *et al.* (HUNUKUMBURE; AGARWAL; VADGAMA, 2011), onde é proposta a arquitetura de *Twin State Network*. Esta arquitetura consiste em manter estações-base que são

habilitadas ou desabilitadas de acordo com a demanda dos usuários em dado momento, fazendo com que se economize energia em períodos que não são de pico. Adicionalmente, mecanismos de *handover* são propostos de acordo com a arquitetura proposta tendo em vista a tecnologia LTE.

No trabalho de Park *et al.* (PARK *et al.*, 2009) propõe-se economizar energia por meio de gerência de mobilidade sensível a contexto. A proposta foi implementada para o IEEE 802.11 de maneira que o período de *scanning* e o número de canais escaneados variavam de acordo com o tipo de aplicação e condições da rede. De acordo com resultados de simulação, esta otimização reduziu a latência de rede, trazendo como consequência a economia de energia na operação de *handover*.

Chowdhury *et al.* propõem um esquema de gerenciamento de recursos utilizando uma política de alocação dinâmica de banda em redes femtocelulares no cenário veicular (CHOWDHURY; CHAE; JANG, 2012). O esquema utiliza a proximidade de novos nós e o QoS necessário como informação para alocação de banda apenas quando necessário. Os resultados de simulação apontam uma redução na probabilidade de perda de chamadas em comparação a esquemas sem o critérios de QoS e de prioridade.

Jeong *et al.* (JEONG *et al.*, 2012) propõem um esquema de *handover* específico para o padrão IEEE 802.16e. Ele consiste em reduzir o número de pacotes necessários para realização de *handover* por meio de uma leitura de canal baseada em grupo. Os nós móveis formam grupos, cada qual com uma agenda para o *handover* de cada nó. Os resultados obtidos por simulação e por modelos de Markov mostram que o esquema reduz a probabilidade de bloqueio de *handover*.

Fu *et al.* (FU *et al.*, 2012) apresentam um esquema de autenticação baseado em grupo para redes . Neste esquema, o PoA envia mensagens de segurança para o grupo de nós se algum membro deste grupo requisitar o *handover*. O objetivo principal é reduzir a latência do *handover* ao mesmo tempo que preserva a privacidade. As métricas avaliadas são a latência, o custo de comunicação e o custo computacional. Os resultados mostram que as duas primeiras métricas são reduzidas, entretanto, a última sofre aumento.

1.4.2 Trabalhos relacionados ao VHO

Zekri *et al.* (ZEKRI; JOUABER; ZEGHLACHE, 2012) apresentam um amplo levantamento de soluções para VHO destacando os principais desafios técnicos. O trabalho ainda apresenta os padrões de rede metropolitanas e seus processos de gerenciamento de mobilidade.

Park *et al.* propõem a integração entre as tecnologias WiMAX e CDMA2000 (PARK; YU; IHM, 2007). A proposta consiste em introduzir mensagens da camada enlace com técnicas de *cross-layering* e o estabelecimento de túneis na camada IP. As simulações

são realizadas com a ferramenta OPNET. As métricas avaliadas foram a latência ao longo do tempo e variando com a velocidade dos nós e a taxa de perda de pacotes ao longo do tempo. De acordo com os autores, essas métricas são reduzidas com o uso do esquema proposto em comparação com um esquema fracamente acoplado.

Shen *et al.* (SHEN; ZENG, 2008) propõem um critério de decisão de VHO baseado em uma função de custo. Os autores consideram largura de banda, carga do tráfego e RSS. Os resultados de simulação mostram que o critério proposto afeta diversos parâmetros do sistema, que precisam ser cuidadosamente analisados.

Stevens-Navarro *et al.* (STEVENS-NAVARRO; LIN; WONG, 2008) utilizam um processo de decisão Markoviano com o objetivo de maximizar a recompensa por enlace em aplicativos de voz e dados. Os resultados da simulação mostram que o algoritmo proposto possui melhor desempenho que algoritmos baseados em modelos aditivos com pesos.

O uso de informações de contexto de rede ao se realizar o *handover* é também tema do trabalho de Gondi *et al.* (GONDI; AGOULMINE, 2010). Estas informações incluem localização, largura de banda necessária, status da bateria, interfaces de rede disponíveis e chaves para autenticação entre outras. Neste trabalho é dada atenção à segurança durante o *handover* em redes heterogêneas.

Kim *et al.* (KIM et al., 2011) propõem uma camada enlace comum às tecnologias 3G, WiMAX e WiBRO. Adicionalmente, são apresentados três esquemas de decisão baseados na largura de banda e custo empregando técnicas de redes neurais. As simulações medem *throughput*, custo e taxa de sucesso do *handover*. Os resultados apontam que o esquema proposto apresenta melhores resultados nessas métricas que esquemas baseados em RSS.

1.4.3 Trabalhos relacionados ao GVHO

O uso de uma *relay station* como entidade centralizadora é proposta por Shan *et al.* (SHAN et al., 2008). A *relay station* coordena o GVHO de usuários dentro de um trem levando-se em conta a localização e a direção na qual os nós seguem. São avaliadas a probabilidade de bloqueio do *handover* e a de perda de chamada em função do número de chamadas por minuto. Os resultados são comparados a um esquema sem a inteligência na *relay station* e o trabalho conclui que há uma redução significativa nessas métricas com a adoção do esquema.

Ning *et al.* (NING et al., 2013) propõem a introdução de uma entidade de rede denominada *Radio Resource Management Center* (RRMC). Essa entidade é responsável por coletar dados de nós e redes candidatas. Assim, o RRMC decide qual grupo de nós podem realizar *handover* para uma determinada rede. O processo de decisão é baseado em *Fuzzy Clustering*, técnica utilizada para agrupar nós com características similares. Os

resultados de simulação mostram que a proposta reduz a probabilidade de bloqueio em comparação a um outro esquema descentralizado (LEE; CHO, 2011).

Cai e Liu (CAI; LIU, 2008) apresentam três algoritmos descentralizados de GVHO: o primeiro é baseado em equilíbrio de Nash, onde a lógica de tentativas reside na estratégia de cada jogador; o segundo se baseia em atrasos aleatórios com variação em um intervalo constante ao se fazer requisições de *handover*; o terceiro é uma versão modificada do anterior considerando a latência do *handover* como base do cálculo. As avaliações de desempenho mostram resultados semelhantes entre as abordagens em relação à latência.

Um modelo baseado em jogos evolucionários é proposto no trabalho de Niyato e Hossain (NIYATO; HOSSAIN, 2009). São consideradas duas abordagens: a primeira com o uso de uma entidade central para fornecer informações de vizinhança; a segunda é uma abordagem descentralizada que utiliza aprendizado por reforço, permitindo que os nós infiram o estado da rede para escolha de PoAs. Na segunda abordagem, a estratégia de tentativas de *handover* é gerenciada pela experiência adquirida pelo próprio nó. A porcentagem de nós que escolhem o mesmo PoA foi a métrica escolhida. Conclui-se que cada abordagem possui vantagens dependendo do cenário onde é empregada.

Lei *et al.* (LEI; HUI; ZHENG, 2010) comparam três esquemas para resolver o problema de GVHO: o primeiro procura dividir as requisições simultâneas por meio de atrasos aleatórios; no segundo esquema, os nós selecionam os PoAs de acordo com uma probabilidade pré-definida; no terceiro, a rede coleta informações do estado da rede e gerencia o *handover*. As métricas avaliadas foram a latência, a taxa de perda de pacotes e a taxa de rejeição. Os resultados mostram que a terceira abordagem obteve os melhores resultados na maioria dos cenários avaliados.

No trabalho de Lee e Cho (LEE; CHO, 2011), o foco é a proposta de um esquema de GVHO baseado na solução de um problema de otimização com o objetivo de minimizar a latência limitando a probabilidade de bloqueio de *handover*. As métricas avaliadas foram a latência e a probabilidade de bloqueio em função do número de nós. Os resultados apresentam uma redução da latência com relação a um esquema tido como convencional.

1.5 Uma Estratégia de Tentativas para GVHO

Um fator determinante ao desempenho do GVHO, além do esquema de decisão, é a estratégia de tentativas adotada. Uma vez tomada a decisão, o nó ou seu PoA de origem podem determinar irá requisitar o *handover* imediatamente ou se essa requisição deve ser adiada para evitar o bloqueio de *handover*, dada as condições da rede. Assim, a estratégia de tentativas de *handover* tem influência direta no desempenho do esquema adotado.

Entre as pesquisas na literatura de GVHO, destaca-se o trabalho de Lee e Cho

(LEE; CHO, 2011) , por não requerer a presença de uma entidade centralizadora para coordenar o GVHO, sendo assim mais tolerante a falhas. A solução também provê balanceamento de carga e a convivência com dispositivos que não suportem o esquema. Entretanto, a estratégia de tentativas de *handover* adotada é baseada em atraso constante, o que prejudica o desempenho quando se aumenta o número de nós envolvidos. Para se obter melhores resultados de desempenho, a estratégia de tentativas deve se utilizar das informações providas pelo próprio esquema e pela rede-alvo.

Assim, propõe-se nesta seção uma estratégia de tentativas de *handover* a ser integrada ao esquema proposto em por Lee e Cho, com o objetivo de reduzir a latência do *handover* (QUENTAL; GONÇALVES, 2013) (QUENTAL; GONÇALVES, 2014a) (QUENTAL; GONÇALVES, 2014b). A solução consiste em adiar o *handover* em um tempo determinado por um algoritmo de *backoff* exponencial no caso do nó optar por não requisitar o *handover* imediatamente. O algoritmo usou como parâmetro informações do próprio esquema, como o número de tentativas já realizadas e a tecnologia da rede pretendida.

A proposta permite distribuir as requisições em *slots* de tempo distintos de modo a reduzir o número total de tentativas de *handover*. Os resultados mostram a redução da latência e a suavização da sua curva de crescimento, consequências da integração da estratégia de tentativas ao esquema de Lee e Cho. nas próximas subseções são detalhados o esquema de Lee e Cho tomados como referência, a proposta para melhoria de desempenho e uma avaliação de desempenho comparando as abordagens.

1.5.1 Esquema de GVHO de referência

O esquema de Lee e Cho (LEE; CHO, 2011) propõe a otimização da latência de *handover* L , tendo como premissa a limitação da probabilidade de bloqueio de *handover*:

Minimizar L

Sujeito a $P_{HoBlock}(t) \leq P_{HoBlockThreshold}$,

onde $P_{HoBlock}(t)$ é a probabilidade de bloqueio de *handover* em um instante de tempo t e $P_{HoBlockThreshold}$ é o máximo valor possível aceitável para $P_{HoBlock}(t)$.

A latência do *handover* é calculada da seguinte forma:

$$L = N_{HO} \cdot \Delta t, \quad (1.1)$$

onde N_{HO} é o número total de tentativas até que o nó faça a requisição de *handover*; Δt é o intervalo entre tentativas consecutivas. Os autores também consideram que a duração da fase de execução de *handover* equivale a *handover*. Caso o nó decida requisitar o *handover* na primeira tentativa, considera-se que a latência total é Δt

A Equação (1.2) apresenta o cálculo de $P_{HoBlock}(t)$. O Valor de $P_{HoBlock}(t)$ depende do número de redes candidatas, largura de banda disponível, e do número de nós participantes do GVHO. Lee e Cho consideram que esses parâmetros são obtidos por meio de consultas a serviços e comunicação *ad hoc*.

$$P_{HoBlock}(t) = \sum_{k=1}^K \sum_{i=C_k(t)}^{M-1} \frac{(i+1-C_k(t)) \cdot (M-1)!}{(i+1)! \cdot (M-1-i)!} \times \left((P_{sel}^k)^{i+1} \cdot (1-P_{sel}^k)^{M-1-i} \right), \quad (1.2)$$

Onde:

- M representa o número de nós participantes do GVHO.
- K representa o número de redes candidatas com áreas de cobertura sobrepostas.
- $C_k(t)$ é a largura de banda disponível no instante de tempo t para uma rede k . O modelo considera que a largura de banda disponível é representada por um valor inteiro. Cada nó requer uma unidade no *handover*.
- P_{sel}^k é a probabilidade de se selecionar a rede k .

Para a solução do problema de otimização, os autores propõem a aplicação da condição de *Karush-Kuhn-Tucker* (KKT) à Equação (1.2) a fim de determinar o valor de P_{sel}^k . Contudo, o valor de P_{sel}^k pode ser obtido de forma heurística, utilizando a Equação (1.3), simplificando esse processo.

$$P_{sel}^k(t) = C_k(t) / \sum_{k=1}^K C_k(t). \quad (1.3)$$

Assim, é possível encontrar o valor de $M_{optimal}(t)$ que garanta a condição do problema de otimização. Esse valor pode ser inicializado com 1, sendo incrementado de 1 em 1 enquanto $P_{HoBlock}(t)$ permanecer abaixo do limite de $P_{HoBlockThreshold}$. Esse procedimento é descrito no Algoritmo 1.

Algorithm 1: Find $M_{optimal}$ value

```

 $M_{optimal} = 0$  ;
repeat
  |  $p = \text{Equation (1.2)}$  ;
  |  $M_{optimal} = M_{optimal} + 1$  ;
until  $p \leq P_{HoBlockThreshold}$ ;

```

A probabilidade $P_{HO}(t)$ com a qual o nó pode requisitar o *handover* é dada por:

$$P_{HO}(t) = M_{optimal}(t) / M. \quad (1.4)$$

Se o nó opta por não requisitar o *handover* imediatamente, uma nova tentativa será realizada após o intervalo de tempo constante Δ_t . O nó requer o número de tentativas necessário para garantir a condição da probabilidade de bloqueio não ultrapassar $P_{HoBlockThreshold}$.

O Algoritmo 2 apresenta um resumo deste processo.

Algorithm 2: Reference GVHO scheme

```

L = 0;
c_atts = 1;
Mtotal = number of GVHO participants;
Mremaining = Mtotal;
while Mremaining > 0 do
  find Moptimal in function of (1.2);
  calculate PHO;
  if decision(PHO) then
    choose networkk depending on Pselk;
    NHO = c_atts;
    break ;
  else
    L += t_atts(c_atts);
    c_atts++;
  end
  Mremaining = Mremaining - Moptimal
end
L += LHOexec;

```

Onde:

- M_{total} é o número total de nós no GVHO.
- $M_{remaining}$ é o contador de nós que ainda não realizaram *handover*.
- `decision()` é a função que retorna `true` com probabilidade $P_{HO}(t)$.
- L_{HOexec} é a duração da etapa de execução do *handover*. É igual a Δt .
- `t_atts()` é a função que calcula o período de tempo entre tentativas consecutivas. Os autores consideram que essa função sempre retorna Δt .
- `c_atts` é o contador de tentativas. Quando a função `decision()` retorna `true` na primeira tentativa, a latência total do *handover* é L_{HOexec} .

A função `t_atts()` caracteriza a política de tentativas de requisição de *handover*. No caso da proposta de Lee e Cho, ela retorna um valor constante .

1.5.2 Política para tentativas de requisição de GVHO

Apesar de apresentar um esquema promissor de GVHO, o trabalho de Lee e Cho carece de uma política adequada para tentativas de requisição de *handover*. Sendo baseada em atraso constante, ela causa um impacto negativo no desempenho à medida em que se aumenta o número de nós envolvidos.

Assim, nesta seção, propõe-se modificar a função $t_atts()$ do Algoritmo 2 em uma implementação de *backoff* exponencial (KWAK; SONG; MILLER, 2005). A implementação usa o contador c_atts como parâmetro e a duração de um *slot* de tempo de referência. A proposta trata de associar a técnica de *random delay* à solução do problema de otimização. Os algoritmos de *backoff* exponencial possuem a particularidade de manter a probabilidade de colisão e a probabilidade de transmissão estáveis à medida que se aumenta o número de nós que compartilham o meio. Esta política de tentativas de requisição de *handover*, apesar de ser proposto para melhorar o desempenho da solução de Lee e Cho, é genérica o suficiente para ser empregada em qualquer outro esquema de GVHO. A Equação (1.5) apresenta uma versão alternativa para $t_atts()$ empregando o *backoff* exponencial:

$$t_atts(c_atts) = \begin{cases} random[0..2^{c_atts} - 1] \cdot timeSlot , \\ \quad \text{if } c_atts \leq LimBackFactor \\ random[0..2^{LimBackFactor} - 1] \cdot timeSlot , \\ \quad \text{caso contrário} \end{cases} \quad (1.5)$$

onde *random* é uma função que escolhe um número uniformemente distribuído sobre um intervalo; *LimBackFactor* é o número de tentativas que limita o tamanho do intervalo para a função *random*; e *timeSlot* é o *slot* de tempo da camada enlace tido como referência, que depende da tecnologia da rede alvo. Essa informação é obtida via serviço .

A latência do *handover* depende diretamente do número de tentativas, que variam de acordo com o retorno da função $decision()$. O *backoff* exponencial permite que os nós tenham a chance de adiar suas tentativas de requisição de *handover* em um tempo menor que Δt , ou até mesmo requisitá-lo imediatamente. Quando um nó adia a sua requisição de *handover*, outros nós têm a chance de fazê-la, reduzindo a concorrência nas próximas tentativas. A consequência é a execução mais antecipada do *handover* para a maioria dos nós, reduzindo a latência média.

A Figura 3 apresenta o comportamento da função $t_atts()$ em função do número de tentativas. É importante observar que com a política proposta, o valor é sempre menor que a abordagem de Lee e Cho.

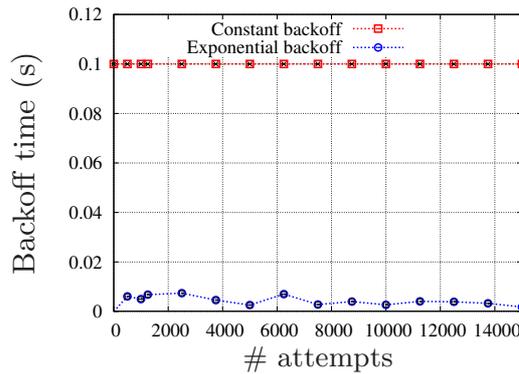


Figura 3. Comparison between the different implementations for the $t_atts()$ function.

Parâmetro	Valor
Δt	0,1 s
$P_{HoBlockThreshold}$	0,01 , 0,02 e 0,05
$timeSlot$	$9 \cdot 10^{-6} s$
$FatorLimBack$	10
valor médio do CHT	60 s
número de PoAs candidatos	5

Tabela 1 – Parâmetros dos experimentos

1.5.3 Avaliação de desempenho

As métricas avaliadas foram latência, probabilidade de bloqueio de *handover* e a fração de nós bloqueados. Essas métricas são avaliadas em função do crescimento do número de nós realizando o GVHO, cujos valores variam de 20 a 100.

A maioria dos parâmetros utilizados nos experimentos possuem os mesmos valores do trabalho de Lee e Cho (LEE; CHO, 2011) e estão listados na Tabela 1. Os valores de limiares para probabilidade de bloqueio 0,01 e 0,02 são baseados em valores típicos (NADA, 2009) (KARRAY, 2010) (CHEKURI et al., 2000) e o valor 0,05 foi acrescentado de modo a avaliar o comportamento do *handover* mediante um critério menos rigoroso. O valor de $timeSlot$ é baseado no *slot* de tempo SIFS do padrão IEEE 802.11. Considera-se que os nós estão migrando de uma rede com tecnologia arbitrária para uma rede IEEE 802.11. O valor de $FatorLimBack$ é baseado em experimentos preliminares.

Nos experimentos é incluído o tempo de permanência em um canal (*Channel Holding Time* - CHT). O CHT é o intervalo de tempo em que um nó ocupa um canal em uma célula devido à uma nova sessão ou *handover* durante uma sessão em andamento. A modelagem do CHT depende em geral do tempo de manutenção de uma chamada, das dimensões da célula, do tempo de permanência na célula, da estratégia de alocação de recursos e da arquitetura da rede (ZHANG; SOONG, 2004). Entretanto, estudos mostram que o CHT pode ser aproximado a uma variável aleatória com distribuição exponencial

(KHEDHER; VALOIS; TABBANE, 2003) (ZHANG; SOONG, 2004). O valor médio do CHT considerado nos experimentos está disponível na Tabela 1.

A caracterização de redes heterogêneas, assim como no trabalho de Lee e Cho, é dada pelos diferentes valores de largura de banda disponíveis. Esta caracterização foi mantida para permitir compatibilidade com o modelo apresentado por esses autores (LEE; CHO, 2011). Considera-se que durante a simulação, os nós realizam tentativas de requisição baseados na política de *backoff* exponencial; uma vez requisitado o *handover*, os nós permanecem consumindo uma unidade de banda por um período de tempo definido pela variável aleatória com distribuição exponencial que define o CHT. Assim, são considerados os seguintes cenários:

Scenario 1 - Todos os PoAs possuem 20 unidades de banda.

Scenario 2 - Dois PoAs têm 15, dois PoAs têm 17, e um PoA tem 20 unidades de banda, respectivamente.

O esquema de Lee e Cho foi implementado com e sem o acréscimo da solução proposta em um simulador de eventos discretos escrito em C++ exclusivamente para este experimento. A Figura 4 ilustra como o escalonador do simulador opera enquanto se encontra em certo estado. No estado apresentado, o *nó 3* acabou de tomar sua decisão. Há uma fila de eventos a serem executados na ordem do tempo agendado. Inicialmente, há n eventos de nós tentando requisitar o *handover* simultaneamente, no instante $t = t_0$. Então, cada evento é retirado da fila e processado de acordo com o Algoritmo 2. No caso da Figura 4, o *nó 3* optou por adiar a requisição para o instante t_3 , enfileirando mais uma tentativa. À esta altura, o *nó 1* já teve o seu evento processado (em $t = t_0$) e sua decisão de adiar a requisição para o instante t_1 o fez enfileirar a nova tentativa. Na Figura 4 também é apresentado um evento para o *nó 2*, que no instante t_2 optou por executar o *handover*, sem mais adiamentos. Desta forma, o paralelismo dos eventos é simulado, uma vez que a alocação de banda se dá em no evento de execução, posterior ao processamento da decisão. Assim, em um instante t a rede está no mesmo estado para todos os nós, refletindo a simultaneidade das operações.

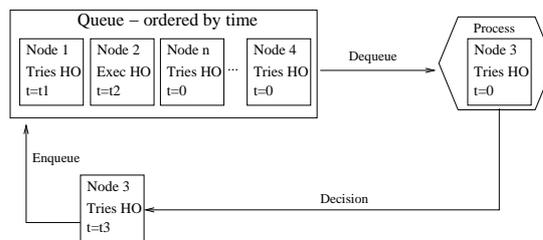


Figura 4. Example of scheduler instance in our discrete-event simulator.

A implementação do esquema de Lee e Cho foi validado pelos seus próprios autores. Os valores plotados nos gráficos possuem 99% de nível de confiança. Os intervalos de

confiança são imperceptíveis nas Figuras 5-9. O foco da avaliação não é o esquema de decisão em si, e sim o impacto do emprego da política de tentativas proposta.

1.5.4 Resultados para o cenário 1

A Figura 5 apresenta os resultados para probabilidade de bloqueio de *handover* no cenário 1. A probabilidade aumenta até que o número de nós alcance 55 para o limiar 0,01, 60 para o limiar 0,02 e 70 para o limiar 0,05. A partir desse ponto, as curvas se estabilizam, pois a probabilidade atinge o limiar definido pelo problema de otimização. Nesse momento, o valor de $M_{optimal}(t)$ não pode mais aumentar, levando os nós restantes a adiar a requisição do *handover*. A consequência da estabilização da curva da probabilidade de bloqueio é o aumento da latência. As curvas com e sem a política proposta são semelhantes uma vez que as condições do problema de otimização são as mesmas. É importante também observar que a política de tentativas proposta não causou danos à esta métrica, mesmo que o intervalo de tentativas seja menor que o esquema de referência.

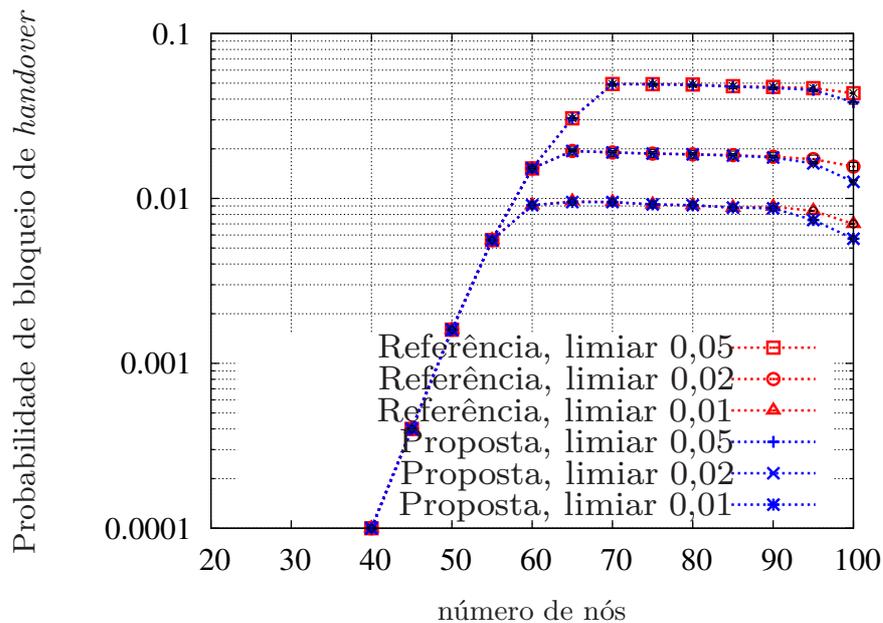


Figura 5. Probabilidade de bloqueio de *handover* versus número de nós no cenário 1.

A Figura 6 mostra os resultados para a fração de nós bloqueados no cenário 1. É possível observar que ao se aproximar de 100 nós, o número de nós bloqueados no esquema de referência é maior que o valor encontrado no esquema com a política proposta. Isso se reflete no gráfico da probabilidade de bloqueio na Figura 5. Para todos os limiares, a probabilidade de bloqueio é um pouco menor quando o número de nós está entre 95 e 100. Isso ocorre devido à natureza aleatória das tentativas, que evita a colisão entre as requisições.

A Figura 7 apresenta os resultados para a latência no cenário 1. No esquema de referência, observa-se que a latência começa a aumentar a partir de 55 nós para o limiar

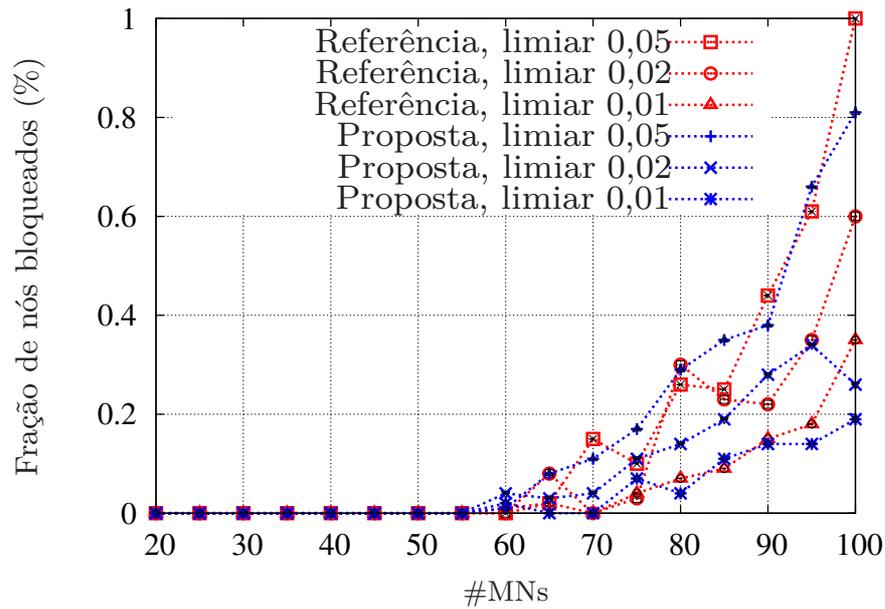


Figura 6. Fração de nós bloqueados *versus* número de nós no cenário 1.

0,01. Para o limiar 0,02, a latência começa a aumentar a partir de 60 nós. NO caso do limiar 0,05, o crescimento da latência se dá a partir de 70 nós. Este crescimento se deve à estabilização da probabilidade de bloqueio, que torna o esquema mais conservador e faz com que os nós adiem por mais tempo a requisição de *handover*. Quanto menor o limiar, mais conservador o esquema se torna. Isto se aplica a ambos os esquemas, com e sem a política proposta. No entanto, observamos que a curva do esquema com a política proposta é mais suave, devido à otimização na lógica de tentativas. Para o limiar 0,05, a proposta reduz a latência em 11% para 80 nó e em 38% para 100 nós. Para o limiar 0,02, a latência se reduz em 18% para 80 nós e em 50% para 100 nós. Finalmente, para o limiar 0,01, ocorre uma redução de 22,5% para 80 nós e de 58% para 100 nós.

A redução da latência ocorre devido à política proposta, que flexibiliza e reduz o intervalo entre tentativas. O uso de *backoff* exponencial permite que os nós tentem o *handover* novamente mais cedo e em instantes diferentes de tempo.

1.5.5 Resultados para o cenário 2

A Figura 8 apresentam os resultados para o cenário 2. Ela apresenta similaridades com a Figura 5, porém, as curvas se estabilizam mais cedo: a partir de 50 nós para os limiares 0,01 e 0,02 e a partir de 55 nós para o limiar 0,05. Uma vez que a largura de banda total disponível neste cenário é menor, a disputa por recursos é maior, fazendo com que a probabilidade de bloqueio aumente mais rapidamente com o aumento do número de nós. Da mesma forma que no cenário anterior, porém, uma vez atingido o limiar, a probabilidade de bloqueio se estabiliza. Entretanto, observa-se que a mesma sofre uma redução a partir de 85 nós. Esse fenômeno pode ser compreendido por meio da Figura 9,

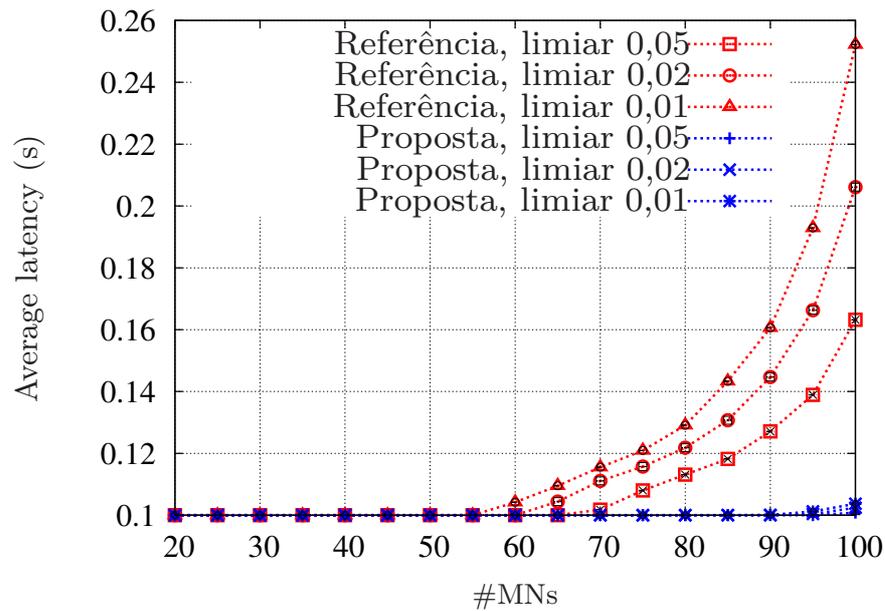


Figura 7. Latência *versus* número de nós no cenário 1.

que apresenta a fração de nós bloqueados.

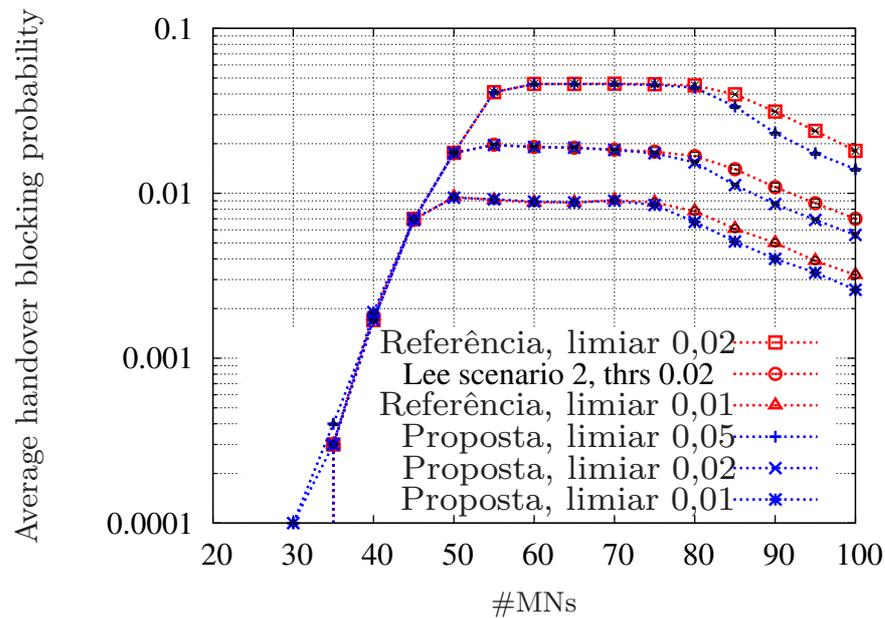


Figura 8. Probabilidade de bloqueio de *handover* *versus* número de nós no cenário 2.

O crescimento expressivo do número de nós bloqueados na Figura 9 faz com que alguns nós desistam definitivamente do *handover* devido ao bloqueio da requisição. Assim, para os nós restantes, a probabilidade de bloqueio diminui. Esse fenômeno também ocorre no caso do esquema com a política proposta, porém, o número de nós bloqueados é menor. Isso ocorre porque a randomização das tentativas torna a requisição de *handover* um processo menos arriscado. Este comportamento é observado para todos os limiares.

A Figura 10 mostra os resultados para a latência no cenário 2. Assim como no

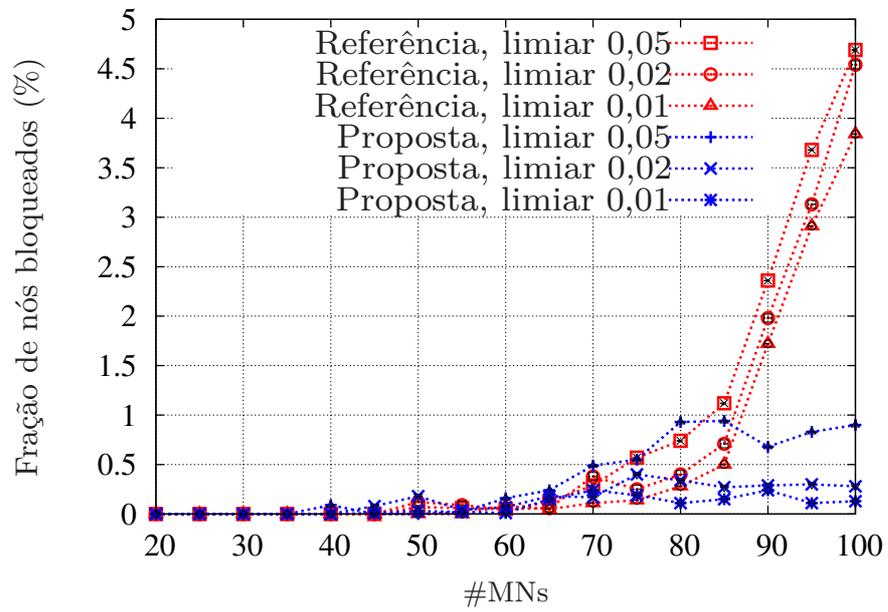


Figura 9. Fraction of blocked nodes *versus* the number of MNs in Scenario 2.

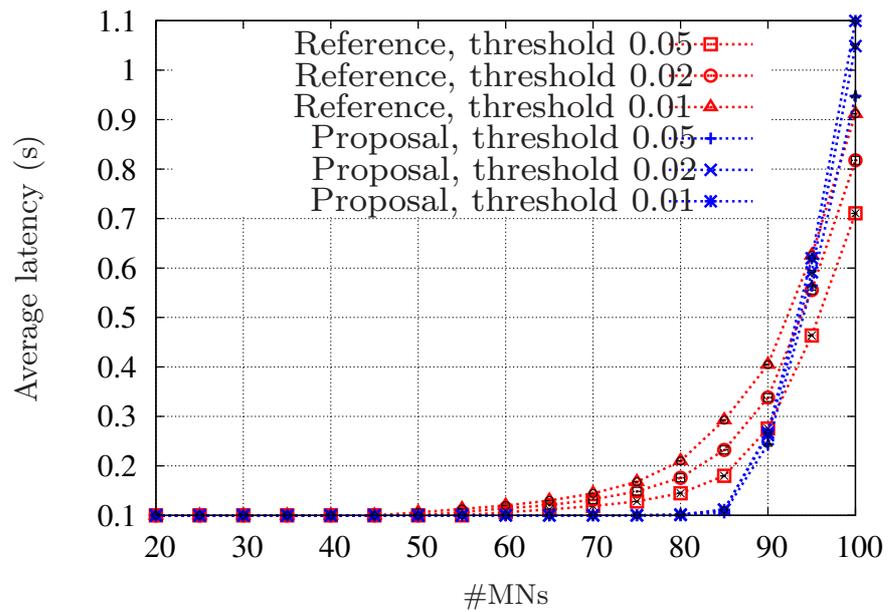


Figura 10. Latency *versus* the number of MNs in Scenario 2.

cenário 1, as curvas com os limiares 0,01 e 0,02 apresentam valores maiores para a latência que a curva com o limiar 0,05. No esquema de referência, a latência começa a aumentar a partir de 60 nós para o limiar 0,01, a partir de 65 nós para o limiar 0,02 e a partir de 70 nós no limiar 0,05. Espera-se valores maiores na latência neste cenário, uma vez que a largura de banda total disponível é menor que no cenário 1. A Figura 10 também apresenta as diferenças entre as latências com e sem a política proposta. Para o limiar 0,05, a latência tem uma redução de 30% para 80 nós. Para o limiar 0,02, a redução é de 42% para 80 nós e de 51,5% para o limiar de 0,05. Adicionalmente nota-se que para 95 nós, a latência do esquema com a política proposta é maior que no esquema sem a proposta. Ao se atingir 100 nós, a latência é maior em 25%, 22%, and 17% nos limiares 0,05, 0,02, e 0,01, respectivamente. Isso se deve a quantidade menor de nós bloqueados no esquema com a política proposta, que pode ser vista na Figura 9. Os nós restantes, mais numerosos com a política proposta, acabam por realizar mais adiamentos e conseqüentemente sofrem uma latência maior.

2 Gerência de Mobilidade IP

O surgimento de protocolos multimídia como VoIP na década de 90 popularizaram ainda mais os aplicativos *online*. Anos mais tarde, as tecnologias veiculares permitiriam transmissão em *streaming* por meio de equipamentos embarcados em automóveis. Após realizar o *handover* na camada enlace, faz-se necessário atualizar informações de roteamento, endereçamento e autenticação. O *handover* entre redes no nível IP tornou-se assim uma questão de vital importância nas pesquisas de Gerência de Mobilidade. Este tipo de *handover* é inerentemente vertical, pois independe das tecnologias da camada enlace. Neste capítulo são apresentadas as principais tecnologias de camada IP e os desafios relacionados ao *handover* entre diferentes domínios.

2.1 Mobilidade IP

Nesta seção são apresentadas as principais tecnologias padronizadas pelo IETF em mobilidade IP.

2.1.1 Mobile IP (MIP)

Sendo o padrão de mobilidade IP mais conhecido do IETF, o Mobile IP (MIP) (JOHNSON; PERKINS; ARKKO, 2004) propõe que um nó móvel mantenha o seu endereço IP original enquanto se move além de sua rede original, denominada *Home Network*, coordenada por um *Home Agent* (HA). O MIP possui padronizações para o IPv4 e IPv6.

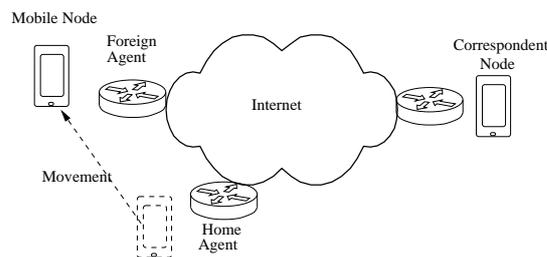


Figura 11. Arquitetura do Mobile IP.

A Figura 11 apresenta a arquitetura do MIP. Ao chegar em uma rede estrangeira, o nó móvel recebe um novo endereço IP de um agente estrangeiro (*Foreign Agent* - FA) para que esse nó seja alcançável dentro dessa rede. Assim, o nó precisa informar seu HA sobre seu endereço na rede estrangeira, conhecido por *Care-of Address* (CoA). O HA mantém uma tabela que associa o endereço original e o CoA denominada *binding table*. Isso permite que o nó correspondente, aquele com o qual o nó móvel se comunica, mantenha a comunicação via HA, que reencaminha a mensagem ao FA, que finalmente a entrega

ao nó móvel. O nó móvel assim sempre será conhecido por seu endereço original, que é traduzido em CoA pelo HA. A Figura 12 apresenta esse fluxo de mensagens de controle do MIP. As mensagens BU e BA referem-se à atualização da tabela do HA (mensagens de *Binding Update* e *Binding Acknowledgment*, respectivamente).

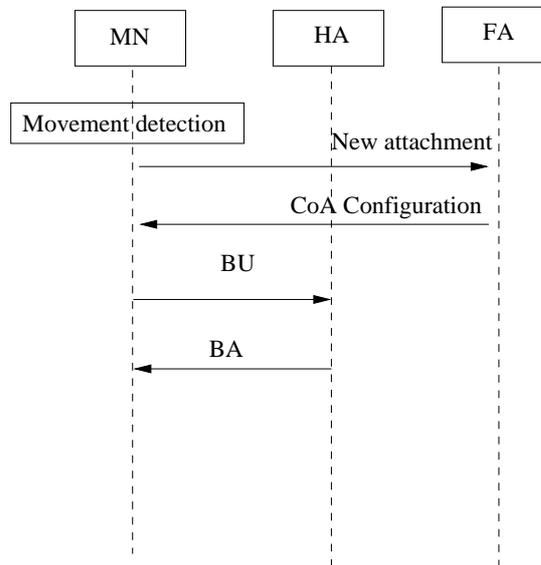


Figura 12. Fluxo de mensagens do Mobile IP.

A extensão *Mobile IPv6 Fast Handovers* (FMIP) (KODLI, 2009) tem o objetivo de reduzir a latência do *handover* antecipando a configuração de endereços com a detecção de movimentos do nó.

A extensão *Hierarchical Mobile IPv6* (SOLIMAN et al., 2008) procura diferenciar mobilidade local e global. Essa diferenciação evita *overhead* na mobilidade local propondo uma entidade denominada *Mobility Anchor Point*. Uma vez que a sinalização do nó é feita com essa nova entidade, a latência pode ser reduzida.

2.1.2 Proxy Mobile IPv6 (PMIPv6)

O MIP requer que o dispositivo móvel possua a implementação do protocolo no seu sistema operacional, o que leva a um consumo adicional de energia. Para reduzir o impacto da mobilidade no consumo de energia do nó móvel, o IETF propôs o *Proxy Mobile IPv6* (PMIPv6) (GUNDAVELLI et al., 2008). O PMIPv6 tem como objetivo tirar a responsabilidade do nó móvel de operações como a atualização de endereço, reduzindo o consumo de energia e sendo assim um protocolo mais adaptável a dispositivos legados. O PMIPv6 introduz duas novas entidades de rede: o *Mobile Access Gateway* (MAG) e o *Local Mobility Anchor* (LMA). Deste modo, a responsabilidade da gerência de mobilidade é passada a essas duas entidades. A Figura 13 ilustra essa arquitetura. O MAG torna-se responsável por enviar atualizações de endereço e manter o controle da localização do nó

móvel, evitando a troca de mensagens pelo dispositivo sem fio. O LMA possui função semelhante à do HA e gerencia todos os MAGs de sua região.

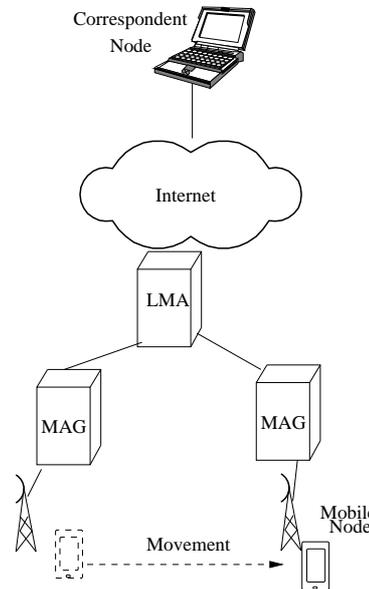


Figura 13. Arquitetura do PMIPv6.

A Figura 14 apresenta o fluxo de mensagens para o PMIPv6. Ao se mover de uma rede para outra, o nó móvel requisita uma nova rota ao novo MAG (NMAG) pela mensagem *Rtr Sol.* do protocolo ICMP. Em seguida, a NMAG solicita ao LMA que atualize suas informações por meio da mensagem *Proxy Binding Update (PBU)*, recebendo um reconhecimento pela mensagem *Proxy Binding Acknowledgment (PBA)*.

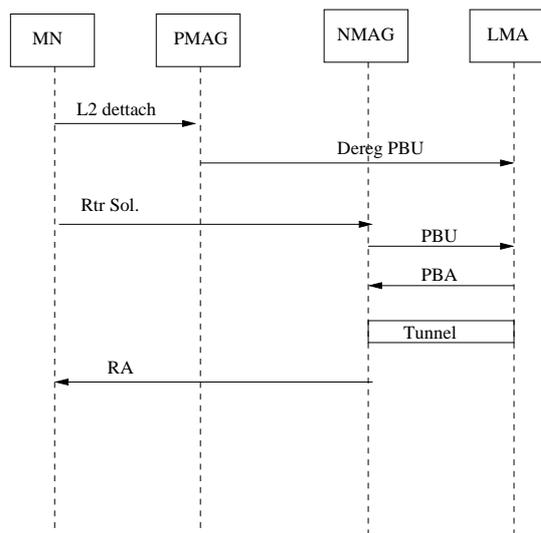


Figura 14. Fluxo de mensagens do PMIPv6.

Os padrões WiMAX e LTE possuem as entidades *Access Service Network Gateway* (ASN-GW) e *Serving Gateway* (S-GW), respectivamente, que são responsáveis por gerenciar a mobilidade dos nós na rede de acesso. Em uma implementação de PMIPv6, essas entidades assumiriam o papel de MAG. Eventualmente poderiam acumular a função do

LMA ou opcionalmente utilizar as entidades *Packet Data Network Gateway* (P-GW) do LTE e alguma entidade da *Connectivity Service Network* (CSN) do WiMAX. Este caso seria mais indicado para que a arquitetura suporte a mobilidade interdomínio.

A extensão *Transient Binding for Proxy Mobile IPv6* (TPMIPv6) (LIEBSCH; MUHANNA; BLUME, 2011) é uma otimização do PMIPv6 para *handover* entre MAG no caso *multihoming*. É acrescentada uma mensagem de TPBU para atualizar a LMA sobre mudança de interface antes que a interface anterior seja desconectada, antecipando a sinalização.

2.1.3 Fast Handovers for Proxy Mobile IPv6 (FPMIPv6)

A extensão *Fast Handovers for Proxy Mobile IPv6* (FPMIPv6) (YOKOTA et al., 2011) adiciona um esquema de *buffering* e criação de um túnel entre o MAG anterior (PMAG) e o NMAG enquanto as mensagens de controle do *handover* ainda estão sendo trocadas. Essa extensão permite reduzir o número de pacotes perdidos durante o processo.

O FPMIPv6 pode funcionar em dois modos: preditivo e reativo. No modo preditivo, ilustrado na Figura 15, o PMAG configura um túnel para o NMAG por meio das mensagens HI (*Handover Indication*) e HACK (*Handover Acknowledgment*) assim que detecta que o enlace está prestes a ser desfeito pelo nó. Após se associar à rede, a NMAG troca mensagens com o LMA da mesma forma que no PMIPv6. Para descobrir o endereço da NMAG correta, o PMAG recebe do nó móvel o endereço do PoA-alvo, que o mapeia para o NMAG correspondente. Opcionalmente, o NAG pode enviar e receber novamente as mensagens de HI e HACK para informar quando está pronta para receber as mensagens do túnel. Durante o *handover* o NMAG acumula as mensagens em um *buffer* para repassar ao nó assim que a conexão entre os dois for estabelecida. É importante observar que no modo preditivo, a rede de acesso ou o nó devem estar preparados para fornecer ao PMAG a informação do PoA-alvo.

No modo reativo do FPMIPv6 o estabelecimento do túnel entre PMAG e NMAG ocorre após o nó se conectar ao enlace da nova rede. Nesse caso, a NMAG é que inicia a comunicação com a PMAG para a configuração do túnel, enviando a mensagem de HI para receber a mensagem de HACK como resposta. Assim como no modo preditivo, o restante da comunicação é semelhante ao que ocorre no PMIPv6. O modo reativo tem a vantagem de não requerer que a rede de acesso envie informações específicas da rede-alvo, uma vez que o contato com a NMAG é feito após o *handover* no novo enlace.

De acordo com Chung *et al.* (CHUNG et al., 2013), o FPMIPv6 apresenta limitações em sua concepção. Por exemplo, o FPMIPv6 considera como premissa que todos os MAGs possuam um mapeamento dos PoAs para o MAG correspondente. Nem sempre essa condição é possível, especialmente no caso de *handover* entre redes heterogêneas ou

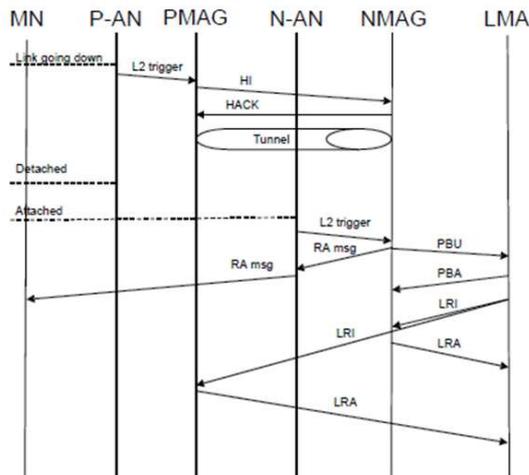


Figura 15. Fluxo de mensagens do FPMIPv6 no modo preditivo.

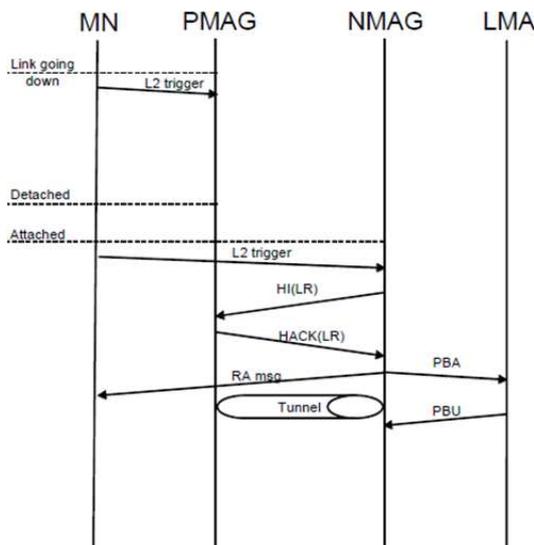


Figura 16. Fluxo de mensagens do FPMIPv6 no modo reativo.

handover interdomínio. Um outro problema apontado por Chung *et al.* é a possibilidade de sobrecarga nas entidades envolvidas no túnel, caso vários *handovers* ocorram simultaneamente na mesma região. As MAGs geralmente são entidades com uma capacidade de processamento inferior à de uma LMA, de modo que faz-se necessário estabelecer parâmetros mínimos de processamento e largura de banda para essas entidades. De acordo com a RFC 5949 (YOKOTA *et al.*, 2011), o FPMIPv6 é capaz de reduzir a perda de pacotes em relação ao PMIPv6, porém, o seu *overhead* de sinalização, gera um aumento na latência.

2.1.4 Otimizações para a Mobilidade IP

Em geral, os protocolos de mobilidade IP tratam do *handover* após a execução deste na camada enlace. Porém, a abordagem de *cross-layering* pode ser desejável dependendo do esquema proposto. Essa implementação pode ser realizada com o auxílio de

eventos e comandos MIH. A otimização do MIP utilizando MIH é objeto de diversas pesquisas, que envolvem inclusive o uso de protocolos de camadas superiores, como o *Session Initiation Protocol* (SIP) (ANGOMA et al., 2011) (BANERJEE; DAS; ACHARYA, 2005) (MUNASINGHE; JAMALIPOUR, 2009). Uma outra forma de otimização observada na literatura é o emprego de *Localized Routing* no PMIPv6 de modo a facilitar a manutenção de rotas otimizadas após o *handover* (??).

2.2 Mobilidade IP Interdomínio

De acordo com a RFC 5213 (GUNDAVELLI et al., 2008), um domínio PMIPv6 inclui LMAs e MAGs entre os quais associações de segurança podem ser configuradas e há autorização para envio de mensagens PBU em nome dos nós. Já Taghizadeh *et al.* (TAGHIZADEH et al., 2012) consideram que um domínio é a representação lógica de uma rede de acesso sem fio. Em ambas as definições, o domínio está relacionado à uma área onde uma mesma operadora controla a confiabilidade e autenticação das entidades de rede.

Diferentemente do MIP, no PMIPv6 e em suas extensões, os LMAs não possuem conhecimento global da rede, tampouco de domínios externos, como um HA teria. O HA consegue acessar domínios além do seu graças à comunicação com o nó móvel, que se encarrega de informar sobre atualização do CoA. Como essa comunicação é eliminada no PMIPv6, não é possível rastrear o nó móvel quando este deixa o domínio.

Entretanto, os cenários veiculares, cada vez mais frequentes em situações realísticas, tornam provável e até mesmo necessária a sinalização de *handover* entre redes de domínios diferentes (JOE; LEE, 2012) (BAIK et al., 2009) (ZHONG et al., 2010) (CHUNG et al., 2013) (ZHOU et al., 2010).

Taghizadeh *et al.* (TAGHIZADEH et al., 2012) classificam as soluções de mobilidade IP quanto à comunicação entre domínios:

- **Domínio único** - Um único domínio envolve toda a rede. Não se considera a existência de outros domínios além dessa rede. Um cenário de domínio único pode ser implementado com o protocolo PMIPv6, uma vez que a autenticação se limita ao MAG correspondente, que é uma entidade local.
- **Multidomínio hierárquico** - Cada rede de acesso é gerenciada por um esquema de mobilidade localizado, como o PMIPv6, sendo a comunicação entre estas redes gerenciadas por um esquema global de mobilidade IP, como o MIP.
- **Multidomínio de pares** - O *handover* em cada rede é gerenciado por um esquema de mobilidade IP local e o *handover* entre redes é realizado pela comunicação entre

esses esquemas sem hierarquia entre eles.

Um dos fatores mais importantes na pesquisa de *handover* interdomínio é a escalabilidade. Se o MIP possui problemas de *overhead* de sinalização, o PMIPv6 fragmenta a rede, pois isola os nós em um domínio local. Desta forma, faz-se necessária uma extensão ao PMIPv6 que o torne escalável do ponto de vista interdomínio conservando sua simplicidade e mantendo as vantagens com relação ao não envolvimento do nó móvel nas operações de gerenciamento. O maior interesse da presente tese se encontra nas soluções que se enquadram no tipo *Multidomínio de pares*, uma vez que é a alternativa mais escalável.

2.3 Trabalhos relacionados

Nesta seção são apresentadas as propostas para otimização dos protocolos de mobilidade MIP, PMIPv6 e FPMIPv6, bem como o Estado-da-Arte em *handover* interdomínio.

2.3.1 Trabalhos relacionados ao MIP

Yeh *et al.* (YEH; CHEN; AGRAWAL, 2009) propõem o FINCH (*Fast Intra-Network and Cross-layer Handover*), um mecanismo complementar ao Mobile IPv4 para gerenciamento de mobilidade intradomínio para WiMAX. O objetivo principal do FINCH é reduzir a latência de *handover*. Utilizando técnicas de *cross-layering*, os autores destacam que o FINCH permite que se utilize caminhos mais curtos na comunicação, reduzindo o tempo de *handover*. A idéia consiste em usar o FINCH para gerenciar o *handover* intradomínio e usar o MIP no caso interdomínio, onde o HA seria responsável pelo gerenciamento de mobilidade. O desempenho de FINCH é comparado com os mecanismos MIP, FMIP, HMIP, Cellular IP e HAWAII por meio de simulação numérica. As métricas avaliadas foram latência, perda de pacotes, custo de atualização da localização e custo total. De acordo com os autores, o FINCH apresentou a segunda menor latência e perda de pacotes, sendo apenas maior que no FMIP. O FINCH possui melhor desempenho no custo de atualização da localização e no custo total apenas se for empregada a sua versão com paginação (P-FINCH).

Kim *et al.* (KIM; SHIN; SHIN, 2008) apresentam uma proposta para o HMIPv6. Os autores propõem executar o *handover* no nível IP e na camada enlace simultaneamente, de modo a reduzir a latência geral do *handover*. Os resultados mostram a redução dessa métrica e da perda de pacotes em um cenário intradomínio em comparação com o HMIPv6.

Angoma *et al.* (ANGOMA *et al.*, 2011) propõem uma arquitetura de integração entre WLAN, 3G e WiMAX. Para tal, três camadas middleware são integradas ao MIPv4: *Driver Management Component layer*, *Discovery and Monitoring Component layer* e *Se-*

lection and Handover Execution Component layer. A interligação com a camada enlace é feita com um serviço do . A avaliação consiste na criação de um *testbed* comparando-se a latência do *handover* no sistema sobre WLAN, 3G e WiMAX. Os autores concluem que o sistema proposto executado sobre 3G é o mais lento.

Munasinghe e Jamalipour (MUNASINGHE; JAMALIPOUR, 2009) propõem uma arquitetura de integração WiMAX com 3GPP com continuidade de sessão. A integração nesse caso é feita entre o MIPv4 e protocolos de camadas superiores. Os autores criam uma arquitetura que utiliza o *IP Multimedia Subsystem* (IMS) como controlador de sessões, que por sua vez, utiliza o protocolo SIP. Avaliações foram realizadas com modelagem analítica e simulação com a ferramenta OPNET (OPNET, 2015). As métricas avaliadas foram latência, taxa de perda de pacotes, *jitter* e custo de sinalização x número de *handovers*. As comparações foram realizadas entre SIP puro e a solução proposta, que mostrou melhor desempenho nas quatro métricas.

2.3.2 Trabalhos relacionados ao PMIPv6 e FPMIPv6

Banerjee, Das e Acharya (BANERJEE; DAS; ACHARYA, 2005) propõem associar MIH, PMIPv6 e SIP para garantir continuidade de sessão durante VHO. O MIH é usado para reportar eventos da camada enlace, enquanto o PMIPv6 tem o papel de atualizar endereços IP. O SIP é utilizado para reiniciar sessões sempre que necessário. A arquitetura foi avaliada por meio de um *testbed*. Os resultados mostram eliminação da perda de pacotes e controle do *jitter*. A latência não foi avaliada.

O trabalho de Kim e Kim (KIM; KIM, 2011) aborda a questão do *throughput* do TCP durante o *handover* no FPMIPv6. A solução inclui MIH para negociação de QoS, pré-registro e pré-autenticação. As simulações foram realizadas com OPNET e os resultados mostram que a proposta reduz o *throughput* do TCP em comparação com o FPMIPv6 puro.

Chung *et al.* (CHUNG et al., 2013) propõem uma abordagem de consulta por proxy CoA sob demanda para tratar do problema do acesso ao endereço proxy-CoA quando se muda de uma PMAG para uma NMAG de outra rede. No FPMIPv6 tradicional, o LMA consegue contactar o NMAG, mas não possui o proxy-CoA antes do *handover* se o NMAG for de outra rede. Assim, os autores propõem a criação das mensagens HPAR e HPAP para obtenção desse endereço pela LMA e das mensagens FPBU e FPBA para bufferizar e estabelecer ou liberar conexões do LMA com o MAG. Os testes foram realizados com simulação própria e observou-se que a proposta reduz a latência e a probabilidade de se ultrapassar o limite da mesma. Uma desvantagem dessa solução é a transferência da responsabilidade de localização do proxy-CoA do NMAG para o LMA, gerando um gargalo na rede com as novas mensagens.

Rasem, Makaya e St-Hilaire propõem o suporte a roteamento baseado em localização (*Localized Routing* - LR) no FPMIPv6 para o modo preditivo (RASEM; MAKAYA; ST-HILAIRE, 2012) e reativo (RASEM; ST-HILAIRE; MAKAYA, 2012). Isso permite recuperar uma rota ótima previamente estabelecida entre nó móvel e seu correspondente após o *handover*. Com o uso de LR dados não precisam passar pelo LMA, nem pelo MAG, melhorando o desempenho da aplicação. Para tal, as mensagens LRI e LRA usadas para iniciar e reconhecer o *Localized Routing* são embutidas nas mensagens de HI e HACK do FPMIPv6. A avaliação é feita com simulador próprio e foram medidas a latência e a taxa de perda de pacote. Observa-se uma redução significativa na latência e a manutenção da taxa de perda de pacotes.

Zhou *et al.* (ZHOU et al., 2010) comparam o desempenho entre PMIPv6, FPMIPv6 e TPMIPv6. A avaliação foi realizada por meio do simulador NS-2 (NS-2, 2015). De acordo com o cenário e parâmetros adotados, conclui-se que o FPMIPv6 tem a maior latência e a menor perda de pacotes UDP. Conclui-se também que o TPMIPv6 tem a menor latência porém, tem a maior perda se o nó passar mais de 1 s em zona de interseção.

2.3.3 Trabalhos relacionados à *handover* interdomínio

Nesta subseção são apresentadas diversas abordagens para se obter *handover* interdomínio, classificadas pela metodologia da solução.

2.3.3.1 Abordagem sem otimização

Park *et al.* (PARK E. LEE; NOH; KIM, 2010) propõem uma extensão ao PMIPv6 para prover *handover* interdomínio sem qualquer tipo de otimização ou entidades adicionais, acrescentando repasse das mensagens já conhecidas do padrão à entidades de domínios vizinhos. É uma solução de *multidomínio de pares*.

A Figura 17 apresenta o fluxo de sinalização. O nó é responsável pela requisição de autenticação. Cada domínio possui o seu próprio serviço de autenticação, autorização e auditoria (*Authentication, Authorization, and Accounting* - AAA). Deve haver um túnel extra entre a LMA anterior e a LMA nova além do túnel já existente entre LMA e NMAG. Avaliações foram realizadas com o simulador QualNET (QUALNET, 2015) medindo a perda de pacotes e a latência em comparação com o esquema que usa PMIPv6/MIP hierarquicamente. Os autores concluem que a proposta é mais adequada em cenários de *handover* frequente. Uma solução semelhante é apresentada em (ZHOU et al., 2010).

2.3.3.2 Abordagem baseada no LMA como âncora de sessão

Newmann *et al.* (NEUMANN et al., 2009) propõem o I-PMIP, uma extensão ao PMIPv6 com suporte a *handover* interdomínio que mantém o mesmo LMA até o fim da

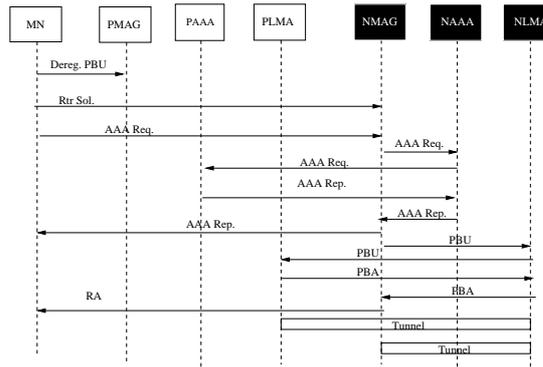


Figura 17. *Handover* interdomínio no esquema de Park *et al.*

sessão. Para tal, parte-se da premissa de que as LMAs de domínios vizinhos são fisicamente próximas e que conhecem seus endereços. Trata-se de uma solução de *multidomínio de pares*. A LMA de origem mantida como âncora do *handover* é denominada *Session Mobility Anchor* (SMA). O I-PMIP prevê uma entidade adicional chamada *Virtual Mobility Anchor* (VMA), responsável por manter a informação do domínio onde o nó se encontra. A Figura 18 apresenta as mensagens de sinalização do I-PMIP. O SMA repassa os dados ao futuro LMA no novo domínio, que cria um túnel para a nova MAG. O VMA é atualizado cada vez que o nó se move para outro domínio. A avaliação de desempenho é apenas teórica, comparando-se a fórmula da latência no MIP, HMIP e H-PMIP. No cenário estudado, o I-PMIP apresentou latência inferior aos demais esquemas.

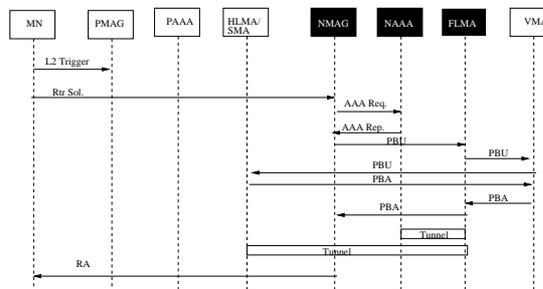


Figura 18. *Handover* interdomínio no esquema I-PMIPv6.

2.3.3.3 Abordagem baseada em entidades centrais

Zhong *et al.* (ZHONG et al., 2010) propõem o *Enabling Inter PMIPv6 Domain Handover* (EIPMH). O EIPMH introduz uma entidade central denominada *Traffic Distributor* (TD), que redireciona dados para o LMA enquanto o nó estiver além do seu domínio original. Os TDs são configurados estaticamente e possuem conhecimento de outros TDs, seus prefixos IP e mapeamento para os LMAs. O TD assume a responsabilidade do LMA de atribuir prefixos IP ao nó móvel além de agir como *gateway* para a rede externa. Esta é uma abordagem de *multidomínio hierárquica*.

A Figura 19 apresenta o fluxo de mensagens de controle para essa proposta. Assim que o nó se registra na NAG, a sua LMA correspondente faz uma consulta a LMA de ori-

gem por meio da mensagem `PBU_Forwarding`. Essa consulta busca informações adicionais do nó e do TD responsável pela comunicação com a Internet. O TD cria um túnel com o novo LMA. Também é criado um túnel entre LMAs além do túnel já existente entre o novo LMA e NMAG.

A avaliação de desempenho é realizada por meio do simulador NS-2 (NS-2, 2015) comparando o EIPMH com o I-PMIP. As métricas avaliadas são latência e *throughput* e os resultados mostram melhor desempenho no EIPMH. Entretanto, a avaliação não considera o *overhead* extra causado pelo túnel entre o TD e a LMA, tampouco à consulta com a mensagem `PBU_Forwarding` e a troca de uma MAG para outra.

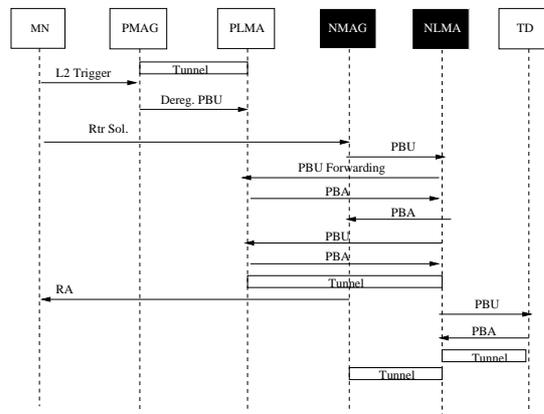


Figura 19. *Handover* interdomínio no esquema EIMHP.

2.3.3.4 Abordagem baseada em especialização de MAG

Joe e Lee (JOE; LEE, 2012) apresentam uma abordagem para *handover* interdomínio baseada em uma arquitetura que distingue dois tipos de MAG: *Boundary* e *Overlapping* MAG (BMAG e OMAG, respectivamente). Assim como em alguns casos anteriores, é uma solução de *multidomínio de pares*. O BMAG é associada a apenas uma LMA enquanto o OMAG se associa a mais de uma LMA, de domínios diferentes. Espera-se que tanto o BMAG quanto o OMAG estejam em áreas de sobreposição entre dois domínios. Os autores partem da premissa de que há apenas uma entidade de autenticação para todos os domínios. A presença de um *gateway* garante a manutenção do endereço IP.

Os autores propõem duas soluções: reativa e *no-gap*. Na solução reativa, um caminho é criado entre o nó correspondente e as LMAs antiga e nova. A nova LMA é descoberta por meio de localização geográfica pela BMAG. Os autores não especificam como a consulta é realizada. A solução também prevê que a funcionalidade da BMAG é replicada em roteadores de borda. Nessa solução, faz-se necessária a criação de um túnel entre o *gateway* e o novo LMA, entre os LMAs e entre o novo LMA e o NMAG.

Na solução *no-gap*, o OMAG cria dois caminhos simultâneos assim que o nó entra em sua área de cobertura. Assim, o nó recebe informação redundante de ambas LMAs.

A Figura 20 apresenta o fluxo de chamadas de sinalização para a solução *no-gap*. Além das mensagens PMIPv6, as mensagens FBD e FBDA são trocadas entre o novo LMA e o *gateway* para confirmar e obter informação adicional sobre o nó. Adicionalmente a nova LMA faz a autenticação do nó. É também necessário criar um túnel entre o *gateway* e o novo LMA e entre o LMA e o OMAG.

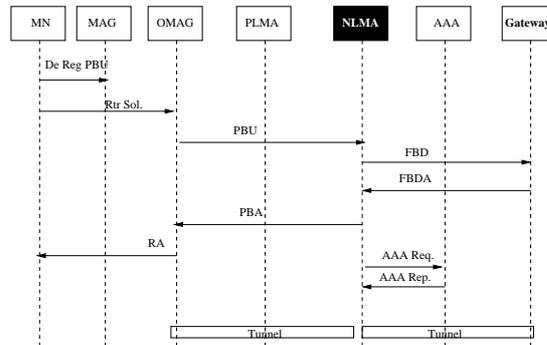


Figura 20. Handover interdomain in No-Gap scheme.

A avaliação de desempenho compara as duas soluções propostas com o MIPv6, FPMIPv6 e EIPMH. A métrica avaliada foi a latência. De acordo com o cenário estudado, os autores concluem que ambas as soluções propostas possuem melhor desempenho sendo *no-gap* a mais eficiente. Entretanto, a avaliação desconsiderou o *overhead* de busca e da criação de túneis adicionais. Uma proposta semelhante ao *no-gap* foi feita por Lee et al. (LEE et al., 2009a).

3 *Clustered PMIPv6*(CPMIPv6)

Este capítulo propõe o *Clustered PMIPv6*(CPMIPv6), uma extensão interdomínio ao PMIPv6 eficiente, distribuído, tolerante a falhas e que conserva as vantagens do PMIPv6 de gerenciamento localizado de mobilidade.

3.1 Análise crítica do Estado-da-Arte em *handover* interdomínio

Os estudos do Estado-da-Arte mostram que uma solução em *handover* interdomínio requer, além da baixa latência, uma perda de pacotes tolerável e uma arquitetura robusta. Assim, algumas soluções optam pela presença de uma entidade global de modo a reduzir o *overhead*. Outras soluções chamam atenção para a questão da simplificação da autenticação. Algumas soluções buscam atribuir novas funções à entidades existentes.

A abordagem de Park *et al.* (PARK E. LEE; NOH; KIM, 2010) propõe o repasse de mensagens PMIPv6 considerando que os LMAs e entidades de autenticação de domínios diferentes possam se comunicar. Assim, é esperado um *overhead* de sinalização dobrado devido à esse repasse. Também é esperado um *overhead* adicional de encapsulamento de cabeçalhos devido ao túnel extra criado entre os LMAs. Uma consequência direta é o aumento da latência.

O I-PMIP (NEUMANN *et al.*, 2009) utiliza o LMA de origem como âncora durante o *handover*, estando associado ao nó ao menos até o fim da sessão em andamento. Entretanto, faz-se necessário a existência de uma entidade para armazenar a localização atual do nó, introduzindo um gargalo e ponto único de falha na arquitetura.

O EIPMH (ZHONG *et al.*, 2010) introduz uma entidade distribuidora de tráfego para gerenciar a transição entre LMAs. A proposta prevê a possível existência de várias dessas entidades, cada uma responsável por uma área de cobertura. Observa-se que o problema de *handover* interdomínio é apenas adiado para o nível dos distribuidores de tráfego, tornando a solução incompleta.

A abordagem *no-gap*, que consiste em especializar o MAG localizado em regiões de sobreposição (JOE; LEE, 2012) requer uma mudança estrutural em roteadores de borda em sistemas legados. Adicionalmente, o nó recebe mensagens redundantes do mesmo MAG vindas de diferentes LMAs a partir do mesmo *gateway*.

Assim, conclui-se que o principal desafio relacionado ao *handover* interdomínio é conciliar as vantagens e evitar as desvantagens dessas propostas em uma arquitetura distribuída, respeitando a compatibilidade com o padrão PMIPv6.

3.2 Arquitetura do CPMIPv6

O CPMIPv6 procura organizar os LMAs de cada domínio em uma estrutura de *Distributed Hash Table* (DHT) denominada *cluster*. A Figura 21 apresenta a arquitetura do CPMIPv6 com a disposição dos LMAs em *cluster*. O gerenciamento do *cluster* é baseado em *Kademlia* (MAYMOUNKOV; MAZIERES, 2002), uma DHT tolerante a falhas com performance logarítmica. *Kademlia* armazena pares <chave, valor> em nós cujos IDs estiverem mais próximos à chave usando a métrica *XOR*.

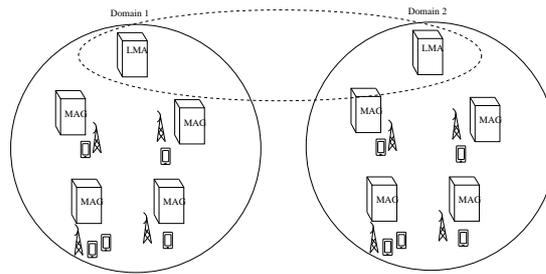


Figura 21. Domains in CPMIPv6.

A arquitetura do CPMIPv6 permite que MAGs de domínios diferentes se localizem por meio de seus LMAs, previamente conectados ao *cluster*. O *cluster* é configurado estaticamente, dependendo de acordos entre as operadoras de banda-larga. Cada LMA possui informação de todas as MAGs conectadas às LMAs da vizinhança, graças às operações de armazenamento do *cluster* durante o registro inicial do nó na rede. A configuração estática permite que domínios possam confiar um no outro, tornando desnecessária a repetição de procedimentos de autenticação ao se mudar de domínio. Desta forma, os serviços de autenticação legados podem permanecer inalterados, como no PMIPv6.

O CPMIPv6 possui a vantagem de prover mobilidade interdomínio distribuído com mudanças pontuais no fluxo de mensagens de controle do PMIPv6. Assim, o CPMIPv6 considera as premissas a seguir:

- Os MAGs são fisicamente alcançáveis a partir de um LMA de um domínio vizinho;
- Os LMAs funcionam como *gateways* para a Internet;
- Cada serviço de AAA está localizado na mesma rede que o LMA no domínio correspondente;
- Os MAGs não realizam *buffering* adicional em comparação ao que já é feito no PMIPv6.

3.2.1 Sinalização do CPMIPv6

A Figura 22 ilustra o fluxo de mensagens de sinalização no momento do registro de um nó na rede. O nó envia a mensagem ICMP *RtrSol* solicitando ao MAG mais próximo

uma rota de acesso à rede externa. O MAG primeiramente autentica o nó com o serviço de AAA de seu domínio. Uma vez que o nó é autenticado, o MAG envia uma mensagem de PBU ao seu LMA. Até esse momento, o fluxo de registro é idêntico ao do PMIPv6. A partir de então, o LMA envia o comando **STORE** derivado do *Kademlia* para armazenar essa associação no *cluster*. Essa operação é exclusiva do CPMIPv6. Assim, os LMAs em domínios vizinhos podem ter acesso ao mapeamento do nó ao seu MAG. A execução do comando **STORE** é assíncrona e não requer aguardar a resposta do *cluster* para o envio da mensagem de PBA para o MAG. O nó é registrado e o MAG pode finalmente anunciar a sua rota por meio da mensagem ICPM RA para o nó.

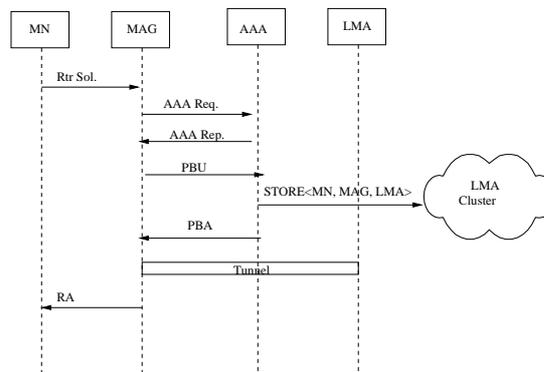


Figura 22. Registro no CPMIPv6.

A Figura 23 apresenta o processo de desregistro. O processo é inicialmente idêntico ao que ocorre no PMIPv6. Após detectar o evento de desligamento, o MAG envia a mensagem PBU ao LMA para o desregistro. O LMA aguarda um intervalo de tempo fixo denominado `INITIAL_BINDACK_TIMEOUT` (JOHNSON; PERKINS; ARKKO, 2004) para remover de fato a associação entre nó e MAG. A seguir, o LMA precisa enviar a mensagem **DELETE** ao *cluster*. A mensagem não possui primitiva do *Kademlia* corresponde, tendo sido criada exclusivamente para o CPMIPv6. Essa operação, assim como **STORE**, é assíncrona e independe da sinalização trocada entre LMA e MAG. Assim, o LMA pode enviar a mensagem PBA para o MAG e finalizar o processo de desregistro.

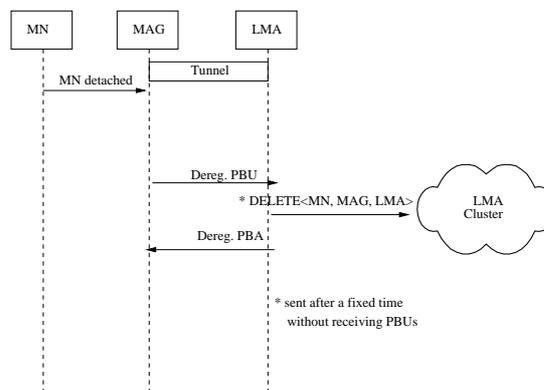


Figura 23. Desregistro no CPMIPv6.

A Figura 24 apresenta o fluxo de sinalização para o *handover* intradomínio. O fluxo é similar àquele proposto pelo padrão PMIPv6, com a adição da mensagem STORE para atualizar o *cluster* após a associação com o novo MAG.

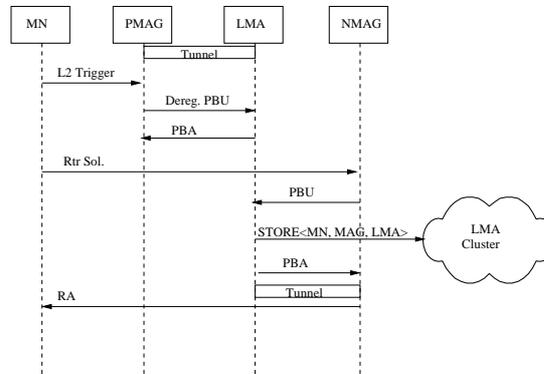


Figura 24. Handover intradomínio no CPMIPv6.

A Figura 25 apresenta a sinalização para o *handover* interdomínio. O nó envia a mensagem PBU para o PMAG para realizar o desregistro. O PLMA aguarda durante o intervalo INITIAL_BINDACK_TIMEOUT para realizar a remoção definitiva do registro. Quando o nó entra no novo domínio e se comunica com o NMAG, ele envia a mensagem PBU para o novo LMA (NLMA). O NLMA encontra em seu registro a antiga associação do nó com a PMAG e o PLMA e o identifica como nó estrangeiro. Assim, o NLMA envia a mensagem PBU para o PLMA informando que o nó está em um novo domínio. Assim, o PLMA desiste de remover o registro e o atualiza. Uma premissa do CPMIPv6 é de que essas mensagens são trocadas em um intervalo inferior a INITIAL_BINDACK_TIMEOUT. Finalmente, o PLMA atualiza o *cluster* com a nova associação.

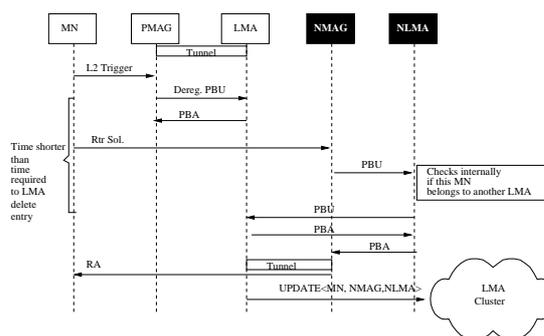


Figura 25. Handover interdomínio no CPMIPv6.

3.2.2 Gerenciamento do *cluster* do CPMIPv6

O *cluster* do CPMIPv6 é uma DHT de LMAs que preserva todas as propriedades *Kademlia*. O *cluster* armazena pares <chave, valor> em cada LMA, onde:

- A chave é o IP do nó;

Nós com distância $1(2^0)$ a $2(2^1)$	Lista de k LMAs
...	...
Nós com distância $1(2^i)$ a $2(2^{i+1})$	Lista de k LMAs
Nós com distância $1(2^{127})$ a $2(2^{128})$	Lista de k LMAs

Tabela 2 – Armazenamento dos 128 k -buckets

- O valor é uma tupla de $\langle \text{IP}_{\text{nó}}, \text{IP}_{\text{MAG}}, \text{IP}_{\text{LMA}} \rangle$;
- O `nodeID`, ou seja, o identificador do LMA no *cluster*, é o IP do LMA ;
- As chaves e os `nodeIDs` estão tem 128 bits de tamanho, assim como todo endereço IPv6, ao invés dos 160 bits padrão do *Kademlia*.

As tuplas $\langle \text{IP}_{\text{nó}}, \text{IP}_{\text{MAG}}, \text{IP}_{\text{LMA}} \rangle$ são armazenadas nos LMAs cujo IP estiver mais próximo do nó em questão, de acordo com a métrica *XOR*. As similaridades nos prefixos IP levam a menores distâncias na métrica *XOR*. As similaridades nos prefixos IP levam a menores distâncias na métrica *XOR*. Assim, o critério de proximidade não é necessariamente geográfico. Entretanto, uma vez que o domínio é identificado pelo seu prefixo de IP, os prefixos mais próximos tendem a ser domínios pertencentes à mesma companhia, assim, sendo mais provável a existência de uma rota ótima entre eles.

Cada LMA no *cluster* precisa ter um armazenamento de k -buckets, onde k é um parâmetro que depende do número médio de domínios que um nó pode cruzar durante uma sessão de comunicação. Cada *bucket* armazena os identificadores dos k LMAs cuja distância para si é n , onde n varia de 1 a 128. A Tabela 2 apresenta um exemplo do armazenamento dos k -buckets.

As primitivas de *Kademlia* PING, STORE, FIND_NODE, FIND_VALUE e o procedimento de busca funcionam da mesma forma prevista por esta DHT. O procedimento de entrada de um LMA no *cluster* é feito durante a configuração inicial da infraestrutura da rede, seguindo o acordos entre as operadoras de telecomunicações envolvidas.

O CPMIPv6 introduz novas primitivas UPDATE e DELETE para atualizar e remover as tuplas, respectivamente. Essas primitivas, que seguem a mesma lógica do comando STORE, não pertencem à implementação original do *Kademlia*. A configuração estática inicial do *cluster* permite que o CPMIPv6 implemente essas primitivas de forma consistente, uma vez que os LMAs considerados vizinhos sempre serão os mesmos.

4 Avaliação de Desempenho e Resultados

4.0.3 Modelagem

A modelagem é baseada em um conjunto de métricas, equações e modelos de mobilidade utilizados por trabalhos do Estado-da-Arte (TAGHIZADEH et al., 2012) (MCNAIR; AKYILDIZ; BENDER, 2001) (MAKAYA; PIERRE, 2008).

4.0.3.1 Mobilidade

Para as avaliações, considera-se o modelo de mobilidade *Fluid-Flow* (SALEHAN et al., 2008). O *Fluid-Flow* é empregado na simulação de padrões de mobilidade veiculares, tendo como parâmetros a velocidade média (v) e as áreas de cobertura do domínio (A_D) e da subrede (A_M). A direção do movimento é uniformemente distribuída em um intervalo de 0 a 2π . Neste modelo, a taxa de cruzamento de um domínio (μ_D) é equivalente à taxa de *handover* interdomínio. A taxa de *handover* intradomínio é a diferença entre a taxa de cruzamento de uma subrede (μ_M) e (μ_D). As equações a seguir ilustram as taxas de *handover* interdomínio e intradomínio.

$$\mu_M = \frac{vL_M}{\pi A_M} \quad (4.1)$$

$$Ng = \mu_D = \frac{vL_D}{\pi A_D} \quad (4.2)$$

$$Nl = \mu_M - \mu_D \quad (4.3)$$

O parâmetro *Session-to-Mobility Ratio* (SMR) descreve a mobilidade dos nós, relacionando a taxa de chegada de sessões com a taxa de cruzamento de subrede. Caso o SMR se aproxime de zero, a mobilidade é considerada alta. Quanto maior o valor do SMR, mais estática é a característica dos nós:

$$SMR = \frac{\lambda_S}{\mu_M} \quad (4.4)$$

4.0.3.2 Métricas

As métricas avaliadas são: custo de sinalização, latência, perda de pacotes e *goodput*.

No modelo utilizado neste capítulo, o custo de sinalização é o número de mensagens de sinalização durante o *handover*, incluindo-se a distância em saltos entre as entidades envolvidas ($H(x - y)$), o meio de transmissão e o custo de processamento. Para cada mensagem trocada entre duas entidades x e y , a equação do custo de sinalização (C_{x-y}) é:

$$C_{x-y} = \alpha(H(x - y)) + \beta + PC_y, \text{ where} \quad (4.5)$$

$$PC_y = \varsigma \log N_{MN}^y \quad (4.6)$$

Os parâmetros α e β representam os coeficientes de unidades de custo de transmissão em mensagens/salto nos meios cabeado e sem fio, respectivamente. Caso nenhuma das entidades envolvidas seja móvel, β tem valor zero. O custo de processamento (PC_y) é medido com base no número de registros de nós armazenados e uma constante normalizadora equivalente à alocação de banda (ς). Caso a mensagem de sinalização não implique busca em repositório, PC_y pode ser considerado zero. O custo total de sinalização é a soma dos custos de todas as mensagens de sinalização necessárias para o *handover*.

A latência é medida como a duração da operação de *handover*. Trata-se da soma das latências de cada mensagem de sinalização trocadas por duas entidades x e y (T_{x-y}). A equação da latência para cada mensagem é dada por:

$$T_{x-y} = \frac{1+q}{1-q} \left(\frac{M_{size}}{B_{wl}} + L_{wl} \right) + H_{x-y} \left(\frac{M_{size}}{B_w} + L_w + T_q \right) \quad (4.7)$$

A primeira parte da soma é o *overhead* do meio sem fio e é desconsiderada caso a mensagem não envolva entidades móveis. O parâmetro q é a probabilidade de falha no enlace. O parâmetro M_{size} é o tamanho médio de uma mensagem e B_{wl} e B_w são as larguras de banda com fio e sem fio, respectivamente. Os parâmetros L_{wl} e L_w são os atrasos de propagação no meio com fio e sem fio. Finalmente, T_q é o atraso médio de fila em cada roteador.

A perda média de pacotes é o número médio de pacotes que deixam de ser enviados/recebidos durante o *handover*. É, portanto, o produto entre a latência de *handover* e a taxa de chegada de pacotes (λ_p):

$$PL = T\lambda_p \quad (4.8)$$

O *goodput* neste modelo relaciona o tráfego útil de dados com o tráfego total durante uma sessão (TOT):

$$Goodput = \frac{TOT - (P_{size} \times PL + TOT \times PD)}{TOT}, \text{ onde} \quad (4.9)$$

$$TOT = SMR \times S \times \lambda_p \times P_{size} \quad (4.10)$$

$$PD = \frac{40 \times H_{tunnel}}{(40 + P_{size}) \times H_{MN-CN}} \quad (4.11)$$

O *goodput* depende diretamente da perda de pacotes e do *overhead* da entrega de pacotes (PD). O PD é o custo do encapsulamento de cabeçalhos IP em túneis ao longo do caminho entre o nó móvel e seu correspondente. Os parâmetros para se determinar o PD são o tamanho do pacote IP (P_{size}) e o tamanho do túnel em saltos (H_{tunnel}).

4.0.3.3 Modelagem das soluções interdomínio

A Tabela 3 resume o fluxo de mensagens de sinalização trocadas para cada esquema de *handover* interdomínio discutido na Seção 2.3.3. As mensagens em *itálico* não são trocadas durante o *handover* intradomínio. As mensagens assíncronas do CPMIPv6, como STORE não são consideradas na avaliação, uma vez que são enviadas de forma independente do andamento do *handover*.

4.0.4 Cenários e parâmetros

No presente experimento, considera-se o modelo hexagonal de célula, sendo cada célula uma subrede do domínio. Cada subrede é coordenada por um MAG. Considera-se também que o domínio é gerenciado por apenas um LMA. No experimento, um domínio é formado por sete subredes, em um arranjo como o apresentado na Figura 26. Cada subrede possui uma área de aproximadamente 1.87 Km², ou com 5Km de perímetro (ALEKSICA et al., 2013). A densidade de concentração dos nós é de 200 nós/Km² (TAGHIZADEH et al., 2012).

A Figura 27 mostra a topologia de referência usada nos experimentos, incluindo entidades de todas as propostas, inclusive CPMIPv6. A distância em saltos entre as entidades é baseada no modelo de Makaya e Pierre (MAKAYA; PIERRE, 2008).

Na rede sem fio, considera-se o padrão IEEE 802.11g, com largura de banda nominal de 54Mbps. Na rede cabeada, a largura de banda é de 100Mbps. O aplicativo *Skype* é tomado como referência para parâmetros de sessão. O tamanho do pacote de dados é de 250 bytes e o tamanho das mensagens de sinalização são de 80 bytes (CHU et al., 2005). A duração média de uma sessão é de 13 minutos uma vez que o baixo custo de chamadas pelo *Skype* faz com que as chamadas tenham duração maior que aquelas iniciadas por operadoras de telecomunicações (GUHA; DASWANI; JAIN, 2006).

O custo total é medido em função do SMR, da velocidade dos nós e do parâmetro *beta* (β). A latência e a perda de pacotes são medidas em função da probabilidade de

Esquema	Mensagens de Handover
CPMIPv6	DeReg (PMAG→LMA) PBU (NMAG↔NLMA) <i>PBU (NLMA↔LMA)</i> StoreAsync(NLMA→Cluster) AddConf (MN↔NMAG)
No-Gap	DeReg (MAG1→LMA) PBU (OMAG↔NnLMA) <i>FBD(nLMA↔NGW)</i> PoInc (nLMA↔NPS) AddConf (MN↔NNMAG)
I-PMIP	DeReg (PMAG→HLMA) PoInc(NMAG↔PS) PBU (NMAG↔FLMA) AddConf (MN↔NMAG) <i>PBU (FLMA↔VMA)</i> <i>PBU (VMA↔HLMA)</i>
EIPMH	DeReg (PMAG→LMA) QueryMN(NFLMA↔PFLMA) PBU (NMAG↔NFLMA) PBU (NFLMA↔PFLMA) <i>PBU (NFLMA↔TD)</i> AddConf (MN↔NMAG)
Sem otimização	DeReg (MAG→LMAh) <i>PoInc(MN↔NMAGv)</i> PoInc(MAGv↔NAAAv) <i>PoInc(AAAv↔NAAAh)</i> PBU (MAGv↔NLMAv) <i>PBU (LMAv↔NLMAh)</i> AddConf (MN↔NMAGv)

Tabela 3 – Mensagens de cada esquema de *handover* interdomínio

falha no enlace. O *goodput* é medido em função do SMR e da probabilidade de falha no enlace.

O custo e a latência total da execução de um *handover* são calculados como uma soma ponderada dos componentes intradomínio e interdomínio:

$$cost = \frac{local\ cost \times Nl + global\ cost \times Ng}{Nl + Ng} \quad (4.12)$$

$$latency = \frac{local\ latency \times Nl + global\ latency \times Ng}{Nl + Ng} \quad (4.13)$$

Ao se avaliar o custo em função da velocidade e *beta*, o mesmo é calculado com

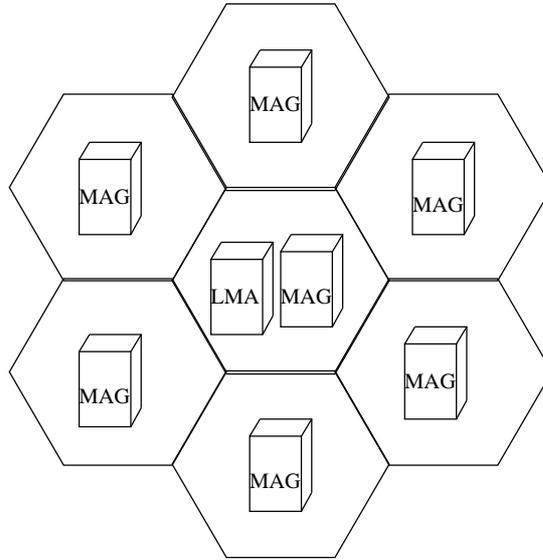


Figura 26. Um domínio com sete subredes.

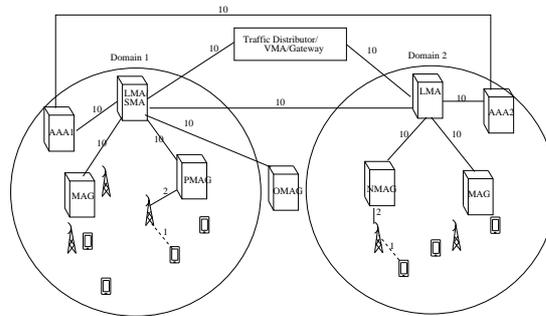


Figura 27. Topologia e distâncias em saltos.

base no número médio de *handovers* realizados em uma sessão VoIP:

$$cost\ in\ session = global\ cost \times Ng \times session\ duration \quad (4.14)$$

A Tabela 4 apresenta outros parâmetros baseados no trabalho de Taghizadeh *et al.* (TAGHIZADEH *et al.*, 2012) e Chu *et al.* (CHU *et al.*, 2005). O parâmetro k de Kademia usado no CPMIPv6 é 10. Esse valor baseia-se em um cenário onde os nós se deslocam a uma velocidade média de 15 m/s (60 Km/h) e, assim, podem cruzar em torno de 10 domínios.

4.0.5 Resultados

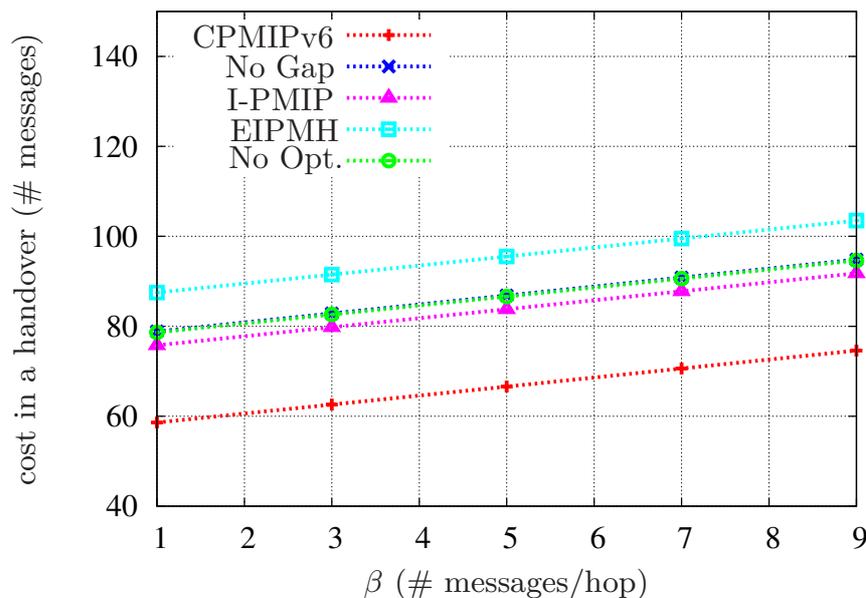
Nesta seção, são apresentados gráficos das métricas de custo de sinalização, latência e *goodput* comparando-se o CPMIPv6 com os esquemas No Gap, I-PMIP, EIPMH, e o esquema sem otimização.

A Figura 28 apresenta os resultados do custo médio de um *handover* em função do fator β . Quanto maior o fator β , mais custoso é o meio sem fio. É possível observar

Parâmetro	Valor padrão	Intervalo
Velocidade	15 m/s	5 - 40 m/s
Prob. falha no enlace sem fio	0.5	0 - 0.8
α	1 mensagens/salto	-
β	10 mensagens/salto	1 - 10
ς	0.01	-
Tempo de fila	5 ms	-
Tempo de permanência na subrede	300 s	-
Atraso de propagação no meio com fio	0.72 μ s	-
Atraso de propagação no meio sem fio	10 ms	-
Taxa de chegada de pacotes	13 pacotes/s (30kbps)	-
Taxa de chegada de sessões	0.001 sessões/s	-

Tabela 4 – Evaluation parameters

que o EIPMH tem o maior custo, uma vez que requer mais interação entre as entidades globais, que são mais distantes entre si. O aumento de β se reflete diretamente no custo, aumentando-o para todos os esquemas. Contudo, o CPMIPv6 tem o custo mais baixo devido ao menor número de mensagens trocadas. A presença de um *cluster* que mantenha informações de domínio proativamente no CPMIPv6 simplifica a comunicação no momento do *handover* e faz com que menos interações sejam necessárias. Os esquemas I-PMIP, No Gap e sem otimização possuem custos similares. No pior caso, o CPMIPv6 possui um custo 26% menor que o EIPMH.

Figura 28. Custo de sinalização *versus* β .

A Figura 29 apresenta a influência do SMR no custo durante uma sessão. O custo tende a se reduzir com o aumento do SMR, pois um alto SMR indica baixa mobilidade.

O esquema sem otimização apresenta o pior desempenho e o CPMIPv6 apresenta o custo mais baixo, uma vez que requer menos mensagens. O número de mensagens tem um papel importante neste cenário pois com baixos valores de SMR, o número de *handovers* durante uma mesma sessão é maior, aumentando o custo de sinalização. Na situação de mais alta mobilidade, o CPMIPv6 apresenta uma redução do custo de até 34%.

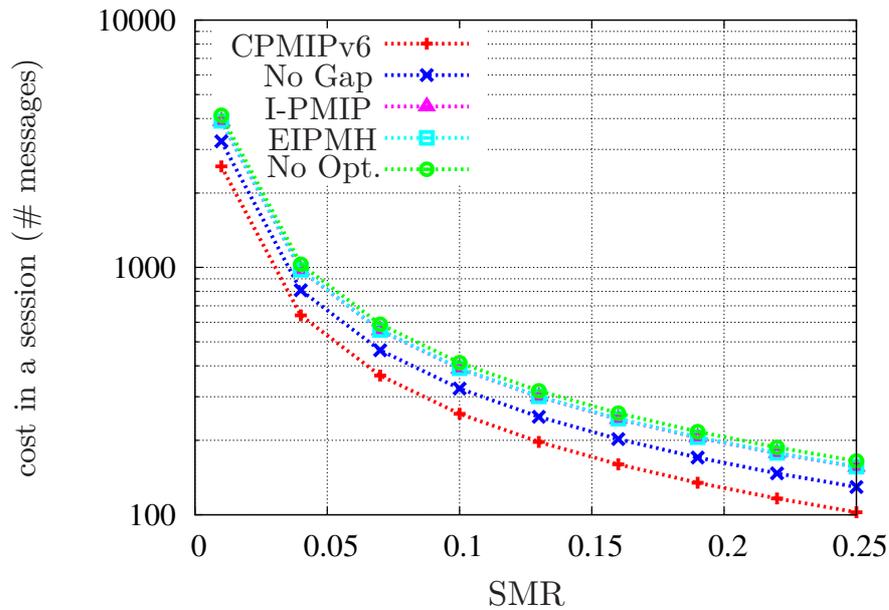


Figura 29. Custo versus SMR.

A Figura 30 mostra o custo de uma sessão em função da velocidade média dos nós. Altas velocidades levam a uma mobilidade mais intensa e, assim, a um número maior de *handovers*. Mai uma vez, o CPMIPv6 apresenta o custo mais baixo, seguido pelo No-Gap. Os esquemas I-PMIP e EIPMH possuem resultados similares e o esquema sem otimização possui o custo mais alto. No caso onde a velocidade é de 40 m/s, o CPMIPv6 possui custo até 34% menor que a abordagem sem otimização.

A Figura 31 apresenta a latência média de *handover* quando se varia a probabilidade de falha de enlace sem fio. Essa probabilidade representa a confiabilidade do meio sem fio e pode degradar o desempenho devido a retransmissões. O EIPMH tem a maior latência, influenciada pela maior quantidade de mensagens trocadas até a probabilidade de 0.65. A partir desse ponto o esquema sem otimização mostra uma latência maior. O No-Gap apresenta resultados ligeiramente melhores que no I-PMIP. É importante observar que o CPMIPv6 apresenta a menor latência, sendo até 30% menor no pior caso. Quando a probabilidade de falha é 0.8, o CPMIPv6 mostra latência de 400 ms, um valor ainda tolerável de acordo com as especificações da ITU (ITU, 2003). Esse melhor desempenho se deve à eliminação de interações desnecessárias no nível da *core network* e na WLAN.

A Figura 32 apresenta o número de pacotes perdidos em função da probabilidade de falha no meio sem fio. A perda de pacotes está diretamente relacionada à latência

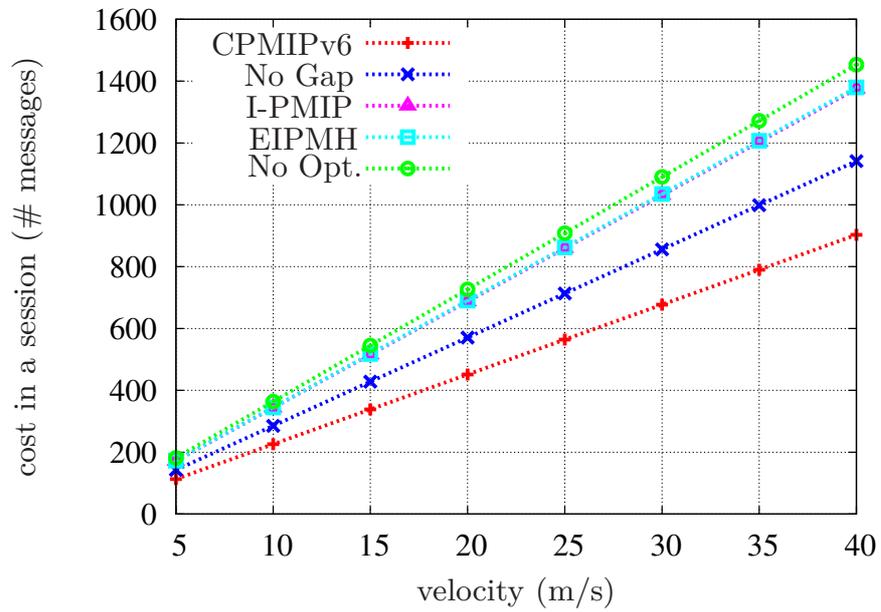


Figura 30. Custo *versus* velocidade.

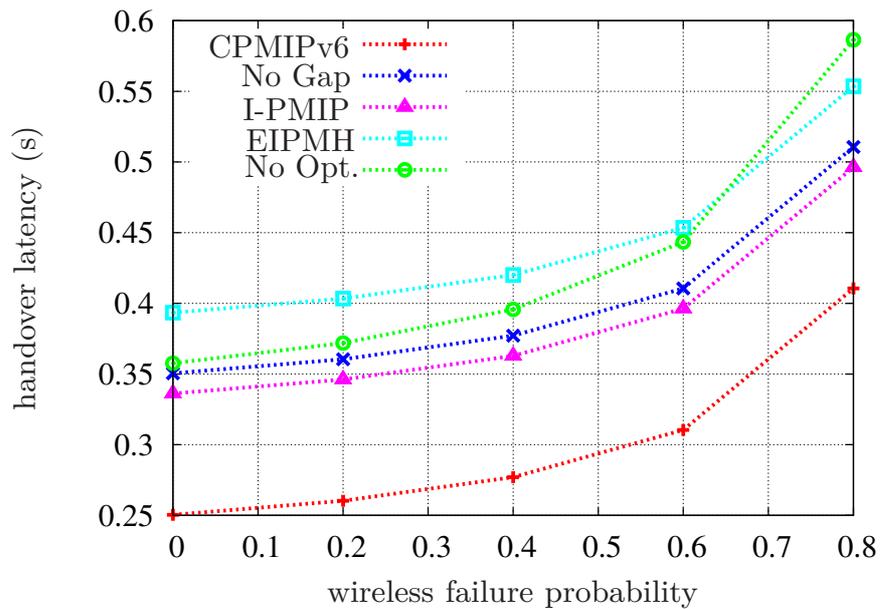


Figura 31. Latência *versus* probabilidade de falha no meio sem fio.

do *handover*. Assim, o CPMIPv6 tem a menor perda em comparação com as demais propostas, chegando a reduzir a perda em 50% com relação à abordagem sem otimização.

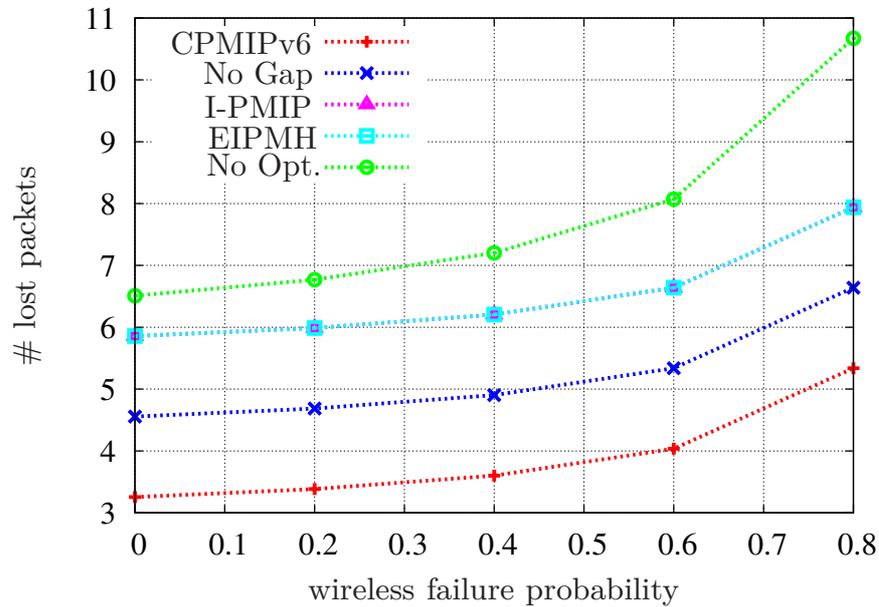


Figura 32. Perda de pacotes *versus* probabilidade de falha no meio sem fio.

A Figura 33 apresenta o *goodput versus* SMR. O *goodput* tende a ser mais estável enquanto o SMR cresce e a mobilidade é reduzida. Já a Figura 34 apresenta o *goodput versus* a probabilidade de falha no enlace sem fio. A probabilidade reduz o *goodput* para todos os esquemas avaliados por causa da maior perda de pacotes. O CPMIPv6 mostra o melhor rendimento variando de 93% a 97%. Isto mostra que o CPMIPv6 pode enviar mais tráfego útil durante a sessão que os demais esquemas. O CPMIPv6 mantém a mesma quantidade de túneis do PMIPv6, evitando o *overhead* de entrega de pacotes de dados devido ao encapsulamento de cabeçalhos IP. O EIPMH apresenta o pior *goodput* pois requer a criação de dois túneis extras além dos túneis do PMIPv6 preexistentes.

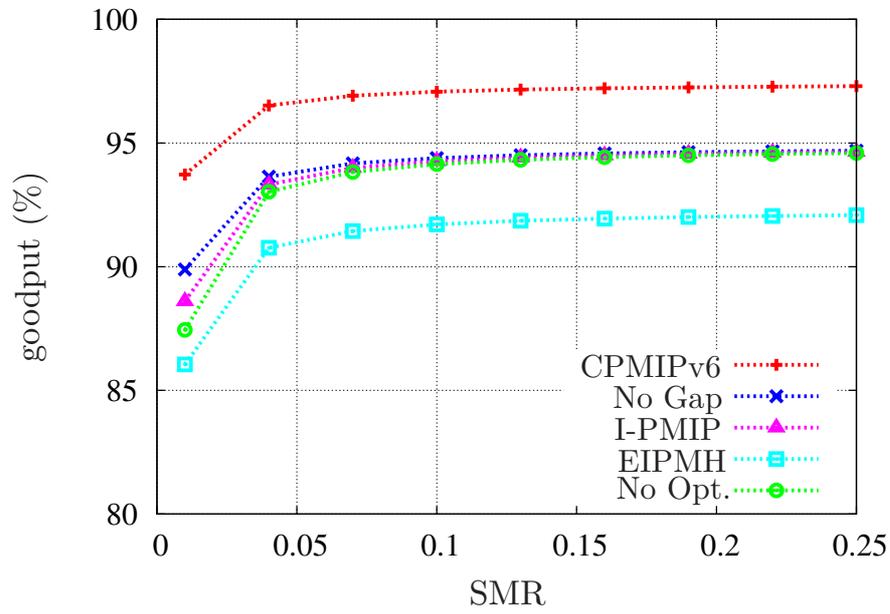


Figura 33. Goodput versus SMR.

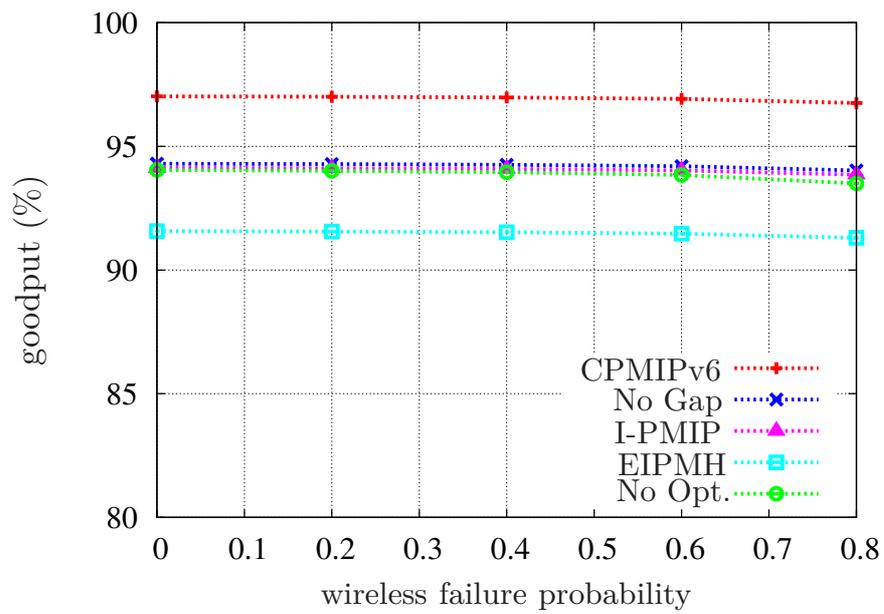


Figura 34. Goodput versus wireless failure probability.

Conclusões e Trabalhos futuros

O presente trabalho apresentou o Estado-da-Arte de *handover* tanto na camada enlace quanto na camada de rede, enfatizando as soluções para interação entre redes de diferentes tecnologias e domínios.

O CPMIPv6 foi proposto enquanto extensão interdomínio do PMIPv6 com *overhead* adicional mínimo de forma distribuída e eficiente. O CPMIPv6 permitiu aliar a simplicidade do PMIPv6 com a robustez de uma DHT como Kademia, garantindo a sua extensão a vários domínios. A extensão proposta foi comparada a diversas abordagens do Estado-da-Arte e os resultados mostraram que, para o cenário estudado:

- Obteve-se menor custo de sinalização, com redução de até 34%;
- A latência pôde ser reduzida em até 34%;
- A perda de pacotes apresentou uma queda de até 50%;
- O *goodput* alcançou um rendimento de até 97%;
- A compatibilidade com a infraestrutura legada do PMIPv6 foi mantida.

Os estudos da proposta de tese resultaram até o momento nas seguintes publicações em conferências e periódicos:

- QUENTAL, N.; GONÇALVES, P. Uma Estratégia de Tentativas de Handover Vertical em Grupo. In: Proc. do 31o. Simpósio Brasileiro de redes de Computadores e Sistemas Distribuídos. Brasília: [s.n.], 2013. p. 411–424.
- QUENTAL, N. C.; GONÇALVES, P. A. S. A Policy for Group Vertical Handover Attempts. In: Proc. of the 13th International Conference on Networks. Nice: [s.n.], 2014. p. 154–159.
- QUENTAL, N. C.; GONÇALVES, P. A. S. Policy for Group Handover Attempts over Heterogeneous Networks. The International Journal on Advances in Networks and Services, v. 7, n. 34, p. 183–193, 2014.
- Submissão de artigo ao *journal* “Wireless Communication and Mobile Computing” (Wiley and Sons).

Para o desenvolvimento futuro da tese, recomenda-se estender o CPMIPv6 para oferecer suporte ao FPMIPv6. Adicionalmente, pode-se considerar aplicação de técnicas

de *Localized Routing* de modo a otimizar ainda mais o desempenho em cenários de alta mobilidade.

Referências

- ITU. *Transport Systems Generic Requirements (TSGR): Common Requirements. GR-499, Issue 2*, Telecordia Report 2009. Citado na pagina 34.
- 802.21. *IEEE Standard for Local and metropolitan area networks - Part 21: Media Independent Handover Services*, IEEE Standard 802.21, 2008. Citado na pagina 14.
- ALEKSICA, S. et al. Energy Efficiency of Femtocell Deployment in Combined Wireless/Optical Access Networks. *Computer Networks*, v. 57, n. 5, p. 1217–1233, 2013. Citado na pagina 60.
- ANDERSSON, K.; FORTE, A.; SCHULZRINNE, H. Enhanced Mobility Support for Roaming Users: Extending the IEEE 802.21 Information Service. In: *Proc. of the 8th International Conference on Wired/Wireless Internet Communications*. Berlin: [s.n.], 2010. p. 52–63. Citado na pagina 14.
- ANGOMA, B. et al. HaVe-2W3G: A vertical handoff solution between WLAN, WiMAX and 3G networks. In: *Proc. of the 7th International Wireless Communications and Mobile Computing Conference*. Istanbul: [s.n.], 2011. p. 101 – 106. Citado 2 vezes nas paginas 46 e 47.
- BAE, S. J.; CHUNG, M. Y.; SO, J. Handover Triggering Mechanism Based on IEEE 802.21 in Heterogeneous Networks with LTE and WLAN. In: *Proc. of the International Conference on Information Networking (ICOIN)*. Barcelona: [s.n.], 2011. p. 399–403. Citado na pagina 26.
- BAIK, J.-W. et al. Inter-Domain Mobility Support Scheme Using Multicast in Proxy Mobile IPv6. In: *Proc. of the 6th IEEE Consumer Communications and Networking Conference*. Las Vegas: [s.n.], 2009. p. 1–2. Citado na pagina 46.
- BANERJEE, N.; DAS, S.; ACHARYA, A. SIP-Based Mobility Architecture for Next Generation Wireless Networks. In: *Proc. of the 3rd IEEE International Conference on Pervasive Computing and Communications*. Kauai Island: [s.n.], 2005. p. 181 – 190. Citado 2 vezes nas paginas 46 e 48.
- CAI, X.; LIU, F. Network Selection for Group Handover in Multi-access Networks. In: *Proc. of the IEEE International Conference on Communications*. Beijing: [s.n.], 2008. p. 2164–2168. Citado 3 vezes nas paginas 14, 22 e 29.
- CHEKURI, C. et al. Blocking Probability Estimates in a Partitioned Sector TDMA System. In: *Proc. of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIAL-M)*. Boston, USA: [s.n.], 2000. p. 28–34. Citado na pagina 34.
- CHOI, H. An optimal handover decision for throughput enhancement. *IEEE Communications Letters*, IEEE, v. 14, n. 9, p. 851–853, 2010. Citado na pagina 26.
- CHOWDHURY, M.; CHAE, S. H.; JANG, Y. M. Group Handover Management in Mobile Femtocellular Network Deployment. In: *Proc. of the 4th International Conference*

- on *Ubiquitous and Future Networks (ICUFN)*. Phuket: [s.n.], 2012. p. 162 – 165. Citado na pagina 27.
- CHU, C. et al. *End-to-End Performance and Reliability Estimation of PacketCable VoIP Services*. 2005. Telcordia Tech. Report. Citado 2 vezes nas paginas 60 e 62.
- CHUNG, J.-M. et al. Enhancements to FPMIPv6 for Improved Seamless Vertical Handover Between LTE and Heterogeneous Access Networks. *IEEE Wireless Communications*, v. 20, n. 3, p. 112 – 119, 2013. Citado 3 vezes nas paginas 44, 46 e 48.
- CICCONETTI, C.; GALEASSI, F.; MAMBRINI, R. Network-assisted Handover for Heterogeneous Wireless Networks. In: *Proc. of the IEEE GLOBECOM Workshops*. Miami: [s.n.], 2010. p. 1–5. Citado 2 vezes nas paginas 14 e 21.
- FIGUEIREDO, F.; PEREIRA, L. Tecnologia WiMAX: Uma visão geral. *Cadernos CPqD Tecnologia*, v. 4, n. 2, p. 7–26, 2008. Citado 2 vezes nas paginas 19 e 23.
- FU, A. et al. A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks. *IEEE Communications Letters*, v. 16, n. 11, p. 1744–1747, 2012. Citado na pagina 27.
- GONDI, V.; AGOULMINE, N. Low Latency Handover and Roaming Using Security Context Transfer for Heterogeneous Wireless and Cellular Networks. In: *Proc. of the IEEE Asia-Pacific Services Computing Conference (APSCC)*. Hangzhou, China: [s.n.], 2010. p. 548–554. Citado na pagina 28.
- GUHA, S.; DASWANI, N.; JAIN, R. *An Experimental Study of the Skype Peer-to-Peer VoIP System*. 2006. Microsoft Research. Disponível em: <<http://research.microsoft.com/en-us/um/people/saikat/paper-iptps06-guha-skype.html>>. Citado na pagina 60.
- GUNDAVELLI, S. et al. *Proxy Mobile IPv6*. IETF, 2008. RFC 5213. (Request for Comments, 1). Disponível em: <<http://tools.ietf.org/html/rfc5213>>. Citado 3 vezes nas paginas 15, 42 e 46.
- HUNUKUMBURE, M.; AGARWAL, R.; VADGAMA, S. Handover Mechanisms for Planned Cell Outage in Twin State Green Wireless Networks. In: *Proc. of the IEEE 73rd Vehicular Technology Conference (VTC Spring)*. Budapest: [s.n.], 2011. p. 1–5. Citado na pagina 26.
- ITU. *International Telephone Connections and Circuits - General Recommendations on the Transmission Quality for an Entire International Telephone Connection*. 2003. ITU-T Recommendation G.114. Citado na pagina 64.
- JEONG, H. et al. An Efficient Group-Based Channel Scanning Scheme for Handover with IEEE 802.16e. In: *Proc. of the 26th IEEE International Conference on Advanced Information Networking and Applications Workshops*. Fukuoka: [s.n.], 2012. p. 639–644. Citado 2 vezes nas paginas 14 e 27.
- JOE, I.; LEE, H. An efficient inter-domain handover scheme with minimized latency for PMIPv6. In: *Proc. of the International Conference on Computing, Networking and Communications*. Maui: [s.n.], 2012. p. 332 – 336. Citado 5 vezes nas paginas 15, 16, 46, 51 e 53.

JOHNSON, D.; PERKINS, C.; ARKKO, J. *Mobility Support in IPv6*. IETF, 2004. RFC 3775. (Request for Comments, 1). Disponível em: <<http://tools.ietf.org/html/rfc3775>>. Citado 3 vezes nas paginas 15, 41 e 55.

KARRAY, M. K. Evaluation of the Blocking Probability and the Throughput in the Uplink of Wireless Cellular Networks. In: *Proc. of the International Conference on Communications and Networking (ComNet)*. Tozeur, Tunisia: [s.n.], 2010. p. 1–8. Citado na pagina 34.

KHAN, M. Q.; ANDRESEN, S. H. PoA Selection in 802.11 Networks Using Media Independent Information Server (MIIS). In: *Proc. of the 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. Fukuoka, Japan: [s.n.], 2012. p. 454–459. Citado na pagina 26.

KHEDHER, H.; VALOIS, F.; TABBANE, S. Channel Holding Time Characterization in Real GSM Network. In: *Proc. of the 14th International Symposium on Personal, Indoor and Mobile Radio Communication (PIMRC)*. Beijing: [s.n.], 2003. p. 46–49. Citado na pagina 35.

KIM, D.; SHIN, H.; SHIN, D. A network-based handover scheme for hierarchical mobile IPv6 over IEEE 802.16 e. In: *Proc. of the 10th International Conference on Advanced Communication Technology, 2008. ICACT 2008*. Pyeongchang, Korea: [s.n.], 2008. v. 1, p. 468–472. Citado na pagina 47.

KIM, I.; KIM, Y. Performance Evaluation and Improvement of TCP Throughput over PFMIPv6 with MIH. In: *Proc. of the 12th IFIP/IEEE International Symposium on Integrated Network Management*. Dublin: [s.n.], 2011. p. 997–1004. Citado 2 vezes nas paginas 14 e 48.

KIM, R. Y. et al. Advanced Handover Schemes in IMT-Advanced Systems. *IEEE Communications Magazine*, IEEE, v. 48, n. 8, p. 78–85, 2010. Citado 3 vezes nas paginas 20, 23 e 26.

KIM, T.-S. et al. Cell selection and trigger point decision for next generation heterogeneous wireless networking environment: Algorithm & evaluation. In: *Proc. of the 5th International Conference on New Trends in Information Science and Service Science (NISS)*. Macao: [s.n.], 2011. p. 247–254. Citado na pagina 28.

KOH, S.; GOHAR, M. Multicast Handover Agents for Fast Handover in Wireless Multicast Networks. *IEEE Communications Letters*, IEEE, v. 14, n. 7, p. 676–678, 2010. Citado na pagina 26.

KOODLI, E. R. *Mobile IPv6 Fast Handovers*. IETF, 2009. RFC 5568. (Request for Comments, 1). Disponível em: <<http://tools.ietf.org/html/rfc5568>>. Citado 2 vezes nas paginas 15 e 42.

KWAK, B.; SONG, N.; MILLER, L. Performance Analysis of Exponential Backoff. *IEEE/ACM Transactions on Networking*, v. 13, n. 2, p. 343–355, 2005. Citado na pagina 33.

LAMPROPOULOS, G.; SALKINTZIS, A. K.; PASSAS, N. Media-Independent Handover for Seamless Service Provision in Heterogeneous Networks. *IEEE Communications Magazine*, IEEE, v. 46, n. 1, p. 64–71, 2008. Citado na pagina 21.

- LEE, K.-W. et al. Inter-Domain Handover Scheme Using an Intermediate Mobile Access Gateway for Seamless Service in Vehicular Networks. *International Journal of Communication Systems*, v. 23, n. 9–10, p. 1127–1144, 2009. Citado na pagina 52.
- LEE, S. et al. Vertical Handoff Decision Algorithms for Providing Optimized Performance in Heterogeneous Wireless Networks. *IEEE Transactions on Vehicular Technology*, v. 58, n. 2, p. 865–881, 2009. Citado na pagina 14.
- LEE, W.; CHO, D. Enhanced Group Handover Scheme in Multi-Access Networks. *IEEE Transactions on Vehicular Technology*, v. 60, n. 5, p. 2389–2395, 2011. Citado 8 vezes nas paginas 14, 20, 22, 26, 29, 30, 34 e 35.
- LEI, S.; HUI, T.; ZHENG, H. Group Vertical Handover in Heterogeneous Radio Access Networks. In: *Proc. of the 72nd IEEE Vehicular Technology Conference Fall*. Ottawa: [s.n.], 2010. p. 1–5. Citado 2 vezes nas paginas 22 e 29.
- LIANG, Y.-H.; CHANG, B.-J.; CHEN, C.-T. Media Independent Handover-based Competitive On-Line CAC for Seamless Mobile Wireless Networks. *Journal Wireless Personal Networks*, 2011. Citado na pagina 26.
- LIEBSCH, M.; MUHANNA, A.; BLUME, O. *Transient Binding for Proxy Mobile IPv6*. IETF, 2011. RFC 6058. (Request for Comments, 1). Disponível em: <<http://tools.ietf.org/html/rfc6058>>. Citado na pagina 44.
- MAKAYA, C.; PIERRE, S. An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols. *IEEE Transactions on Wireless Communications*, v. 7, n. 3, p. 7, 2008. Citado 2 vezes nas paginas 58 e 60.
- MAYMOUNKOV, P.; MAZIÈRES, D. Kademia: A Peer-to-Peer Information System Based on the XOR Metric. In: *Proc. of the First International Workshop on Peer-to-Peer Systems*. [S.l.: s.n.], 2002. p. 53–65. Citado 2 vezes nas paginas 16 e 54.
- MCNAIR, J.; AKYILDIZ, I.; BENDER, M. D. Handoffs for Real-Time Traffic in Mobile IP Version 6 Networks. In: *Proc. of the First Global Telecommunications Conference*. San Antonio: [s.n.], 2001. p. 3463–3467. Citado na pagina 58.
- MUNASINGHE, K.; JAMALIPOUR, A. Interworked WiMAX-3G cellular data networks: An architecture for mobility management and performance evaluation. *IEEE Transactions on Wireless Communications*, v. 8, n. 4, p. 1847 – 1853, 2009. Citado 2 vezes nas paginas 46 e 48.
- NEUMANN, N. et al. I-PMIP: An Inter-Domain Mobility Extension for Proxy-Mobile IP. In: *Proc. of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*. Leipzig: [s.n.], 2009. p. 994–999. Citado 4 vezes nas paginas 15, 16, 49 e 53.
- NING, L. et al. Fuzzy Clustering based Group Vertical Handover Decision for Heterogeneous Wireless Networks. In: *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC)*. Changai: [s.n.], 2013. p. 1231–1336. Citado 2 vezes nas paginas 22 e 28.
- NIYATO, D.; HOSSAIN, E. Dynamics of Network Selection in Heterogeneous Wireless Networks: an Evolutionary Game Approach. *IEEE Transactions on Vehicular Technology*, v. 58, n. 4, p. 2008–2017, 2009. Citado 2 vezes nas paginas 22 e 29.

- NOBREGA, O. de O. *Modelo para Transparência de Handover Vertical em Redes de Quarta Geração*. Tese (Doutorado) — Universidade Federal de Pernambuco, 2011. Citado na pagina 19.
- NS-2. *The Network Simulator - ns-2*. 2015. Acessado: 24-02-2015. Disponível em: <http://nslam.isi.edu/nslam/index.php/User_Information>. Citado 2 vezes nas paginas 49 e 51.
- OPNET. *OPNET*. 2015. Acessado: 24-02-2015. Disponível em: <<http://www.riverbed.com/products/performance-management-control/opnet.html>>. Citado na pagina 48.
- PARK E. LEE, F. Y. S.; NOH, S.; KIM, S.-H. Inter-domain Roaming Mechanism Transparent to IPv6-Node among PMIPv6 Networks. In: *Proc. of the Taipei*: [s.n.], 2010. p. 1-5. Citado 3 vezes nas paginas 15, 49 e 53.
- PARK, J. et al. Context-Aware Mobility Management with Energy Efficiency for Multimedia Streaming Service in Wireless LAN. In: *Proc. of the 6th IEEE Consumer Communications and Networking Conference (CCNC)*. Las Vegas: [s.n.], 2009. p. 1-6. Citado na pagina 27.
- PARK, S.; YU, J.; IHM, J. A Performance Evaluation of Vertical Handoff Scheme between Mobile-WiMax and Cellular Networks. In: *Proc. of 16th International Conference on Computer Communications and Networks (ICCCN)*. Honolulu: [s.n.], 2007. p. 894 - 899. Citado na pagina 27.
- POLLHI, G. P. Trends in Handover Design. *IEEE Communications Magazine*, 1996. Citado 2 vezes nas paginas 21 e 24.
- QUALNET. *QualNet - Scalable Network Technologies*. 2015. Acessado: 19-02-2015. Disponível em: <<http://web.scalable-networks.com/content/qualnet>>. Citado na pagina 49.
- QUENTAL, N. C.; GONÇALVES, P. A. S. Uma Estratégia de Tentativas de Handover Vertical em Grupo. In: *Proc. do 31o. Simpósio Brasileiro de redes de Computadores e Sistemas Distribuídos*. Brasília: [s.n.], 2013. p. 411-424. Citado na pagina 30.
- QUENTAL, N. C.; GONÇALVES, P. A. S. A Policy for Group Vertical Handover Attempts. In: *Proc. of the 13th International Conference on Networks*. Nice: [s.n.], 2014. p. 154-159. Citado 2 vezes nas paginas 14 e 30.
- QUENTAL, N. C.; GONÇALVES, P. A. S. Policy for Group Handover Attempts over Heterogeneous Networks. *The International Journal on Advances in Networks and Services*, v. 7, n. 34, p. 183-193, 2014. Citado na pagina 30.
- RASEM, A.; MAKAYA, C.; ST-HILAIRE, M. O-PMIPv6: Efficient Handover with Route Optimization in Proxy Mobile IPv6 Domain. In: *Proc. of the IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications*. Barcelona: [s.n.], 2012. p. 47-54. Citado na pagina 49.
- RASEM, A.; ST-HILAIRE, M.; MAKAYA, C. A Comparative Analysis of Predictive and Reactive Mode of Optimized PMIPv6. In: *Proc. of the 8th International Wireless Communications and Mobile Computing Conference*. Limassol: [s.n.], 2012. p. 722-727. Citado na pagina 49.

- SALEHAN, A. et al. A Comparison of Various Routing Protocols in Mobile Ad-Hoc Networks (MANETs) with the Use of Fluid Flow Simulation Method. In: *Proc. of the 4th International Conference on Wireless and Mobile Communications*. Athens: [s.n.], 2008. p. 260–267. Citado na página 58.
- SHAN, L. et al. Predictive Group Handover Scheme with Channel Borrowing for Mobile Relay Systems. In: *Proc. of the International Wireless Communications and Mobile Computing Conference*. Crete Island: [s.n.], 2008. p. 153–158. Citado na página 28.
- SHEN, W.; ZENG, Q. Cost-function-based network selection strategy in integrated wireless and mobile networks. *IEEE Transactions on Vehicular Technology*, v. 57, n. 6, p. 3778–3788, 2008. Citado 2 vezes nas páginas 14 e 28.
- SILVA, R. et al. Heterogeneous Mobility in Next Generation Devices: An Android-Based Case Study. *Mobile Multimedia Communications*, Springer, v. 77, p. 316–330, 2012. Citado 2 vezes nas páginas 21 e 26.
- SOLIMAN, H. et al. *Hierarchical Mobile IPv6 (HMIPv6) Mobility Management*. IETF, 2008. RFC 5380. (Request for Comments, 1). Disponível em: <<http://tools.ietf.org/html/rfc5380>>. Citado na página 42.
- STEVENS-NAVARRO, E.; LIN, Y.; WONG, V. An MDP-Based Vertical Handoff Decision Algorithm for Heterogeneous Wireless Networks. *IEEE Transactions on Vehicular Technology*, v. 57, n. 2, p. 1243–1254, 2008. Citado 2 vezes nas páginas 14 e 28.
- TAGHIZADEH, A. et al. A performance Evaluation Framework for Network-Based IP Mobility Solutions. *International Journal of Innovative, Computing, Information and Control*, v. 8, n. 10, p. 7263–7288, 2012. Citado 5 vezes nas páginas 15, 46, 58, 60 e 62.
- TANIUCHI, K. et al. IEEE 802.21: Media Independent Handover: Features, Applicability, and Realization. *IEEE Communications Magazine*, v. 47, n. 1, p. 112–120, 2009. Citado 2 vezes nas páginas 14 e 24.
- YEH, J.; CHEN, J.; AGRAWAL, P. Fast intra-network and cross-layer handover (finch) for wimax and mobile internet. *IEEE Transactions on Mobile Computing, IEEE*, v. 8, n. 4, p. 558–574, 2009. Citado na página 47.
- YOKOTA, H. et al. *Fast Handovers for Proxy Mobile IPv6*. IETF, 2011. RFC 5949. (Request for Comments, 1). Disponível em: <<http://tools.ietf.org/html/rfc5949>>. Citado 3 vezes nas páginas 15, 44 e 45.
- ZEKRI, M.; JOUABER, B.; ZEGHLACHE, D. A Review on Mobility Management and Vertical Handover Solutions over Heterogeneous Wireless Networks. *Computer Communications*, v. 35, n. 17, p. 2055–2068, 2012. Citado 5 vezes nas páginas 14, 15, 20, 21 e 27.
- ZHANG, Y.; SOONG, B.-H. Channel Holding Time in Hierarchical Cellular Systems. *IEEE Communications Letters*, v. 8, n. 10, p. 614–616, 2004. Citado 2 vezes nas páginas 34 e 35.
- ZHONG, F. et al. Enabling Inter-PMIPv6-Domain Handover with Traffic Distributors. In: *Proc. of the 7th IEEE Consumer Communications and Networking Conference*. Las Vegas: [s.n.], 2010. p. 1–5. Citado 4 vezes nas páginas 15, 46, 50 e 53.

ZHOU, D. et al. Evaluation of Fast PMIPv6 and Transient Binding PMIPv6 in Vertical Handover Environment. In: *Proc. of the IEEE International Conference on Communications*. Cape Town: [s.n.], 2010. p. 1550–3607. Citado 2 vezes nas paginas 46 e 49.

Glossário

Kademlia É uma Tabela Hash Distribuída para redes P2P descentralizadas que especifica a estrutura da rede e troca de informações por meio de buscas baseadas na métrica XOR..

XOR Operação lógica de OU exclusivo..

cross-layering Técnica que consiste em permitir que entidades de uma camada da pilha de protocolos obtenham dados ou executem comandos em outra camada..

multihoming Situação em que um dispositivo está conectado à mais de uma rede simultaneamente. Pode-se considerar *multihoming* em caso de haver apenas uma interface com múltiplos endereços ou múltiplas interfaces com um único endereço..

throughput Quantidade de dados transferidos de um lugar a outro, ou a quantidade de dados processados em um determinado espaço de tempo..

LTE *Long-Term Evolution*, sistema definido pela *Third Generation Partnership Project*(3GPP) como pertencente à quarta geração de redes móveis.

MIH *Media Independent Handover*, ou handover independente de mídia, correspondente ao padrão IEEE 802.21.

PoA *Point of Attachment*, ou ponto de acesso; entidade situada em uma das extremidades de um enlace.

PoA candidato PoA candidato a ser escolhido para *handover*.

PoA de origem PoA ao qual o nó móvel está inicialmente associado.

PoA-alvo PoA ao qual o nó móvel estará associado ao fim do *handover*.

Wi-Fi *Wireless Fidelity*, sistema definido pela *Wi-Fi Alliance* que garante a compatibilidade entre dispositivos que adotam o padrão IEEE 802.11.

WiMAX *Worldwide Interoperability Microwave Access*, sistema definido pelo WiMAX Forum, que garante a compatibilidade entre dispositivos que adotam o padrão IEEE 802.16.