Uma análise das implementações de protocolos IPv6 puros e híbridos para provimento de mobilidade em IPv6

César A. H. Loureiro, Liane M. R. Tarouco, Lisandro Z. Granville, Leandro M. Bertholdo

Programa de Pós-Graduação em Computação – Instituto de Informática – Universidade Federal do Rio Grande do Sul, 91.501-970 – Porto Alegre – RS – Brasil

cahloureiro@inf.ufrgs.br, liane@penta.ufrgs.br, granville@inf.ufrgs.br, berthold@penta.ufrgs.br

Resumo. *O uso crescente de dispositivos móveis sem fio, associado ao esgotamento de endereços IPv4, nos levou a pensar que a mobilidade em redes IP será feita apenas utilizando o protocolo IPv6. No entanto, a diversidade de protocolos de mobilidade, pode ser interpretada como um indício de que as soluções de mobilidade utilizando IPv6 não estão maduras o suficiente para serem implantadas em larga escala. Neste artigo vamos analisar, testar e avaliar algumas implementações usadas no provimento de mobilidade em IPv6, analisando o desempenho, dificuldade de implantação e estabilidade destas implementações.*

Abstract. *The growing use of mobile wireless devices, associated with the depletion of IPv4 addresses, led us to think that mobility in IP networks will be done just by using the protocol IPv6. However, the diversity of mobile protocols in existence can be interpreted like a symptom that mobility´s solution using IPv6 are not mature enough to deploy on a large scale. In this paper we will review, test and evaluate several implementations used to provide mobility over IPv6, analyzing its performance, level of difficulty to deploy and stability of the solution.*

1. Introdução

A proliferação dos dispositivos móveis sem fio, associado ao esgotamento de endereços IPv4, levou-nos ao pensamento natural que a implementação da mobilidade nas redes IP ocorrerá apenas usando o protocolo IPv6. Este pensamento pode ser sentido no esforço realizado pelas operadoras de telefonia celular, em preparação para o novo padrão "4G", que em um futuro não muito distante, provavelmente terá que lidar com dispositivos *IPv6-only* [Limoncelli; Cerf, 2011] [Morr, 2010]. Além disso, IPv6 e seus protocolos de configuração de endereços (*Neighbor Discovery* e *Stateless Address Configuration)* formam uma base de protocolo apropriada para redes móveis [Perkins, 2002].

Por outro lado, existem vários protocolos propostos para lidar com a mobilidade, como: [Johnson; Perkins; Arkko, 2004] [Koodli, 2009], [Soliman; et al., 2008], [Leung; et al., 2008] [Menth; Klein; Hartmann, 2010] [Moskowitz; et al., 2008] e [Nordmark; Bagnulo, 2009]. Essa diversidade de protocolos pode ser interpretada como um indício que as soluções de mobilidade não estão maduras o suficiente para ser implantadas em redes IP, e que pesquisas ainda são necessárias.

Neste contexto, este trabalho tem por objetivo revisar, testar e avaliar as implementações mais importantes dos protocolos utilizados para prover mobilidade em IPv6, analisando seu desempenho, dificuldade de implantação e estabilidade das implementações.

Este artigo está organizado da seguinte forma: a seção (2) descreve uma classificação e uma visão geral sobre os protocolos de mobilidade avaliados, a seção (3) referencia trabalhos relacionados ao ensejo de nossa pesquisa, a seção (4) demonstra a metodologia utilizada nos experimentos, bem como uma descrição das implementações analisadas. Na seção (5) demonstramos os resultados obtidos e a análise dos mesmos. Finalmente, na seção (6) concluímos o artigo.

2. Protocolos de Mobilidade

Primeiramente, para ganhar uma melhor compreensão de conceitos de protocolos de mobilidade, é necessário obter algum *know-how* sobre a terminologia. A RFC 2002 define algumas entidades referenciadas neste artigo, incluindo: O *Mobile Node* (MN) como um *host* ou dispositivo que migra de uma rede para outra, mantendo a comunicação com um *Correspondent Node* (CN), que se refere ao par com o qual um nó móvel está se comunicando. Quando o nó móvel está trocando de rede, a partir de uma *Home Network* (HN) a uma *Foreign Network* (FN), a comunicação é controlada por um agente de mobilidade, conhecido como *Home Agent* (HA), responsável por receber e encaminhar todos os pacotes enviados entre o nó móvel e o nó correspondente. Esta comunicação, na maioria das vezes, é implementada por túneis IPSec ou *IP-over-IP*.

Existem dois tipos de protocolos de mobilidade classificados por nós, o primeiro chamamos de protocolo IPv6 "puros" e o segundo de protocolos "híbridos".

Os protocolos IPv6 "puros" são classificados dessa maneira porque utilizam apenas os recursos nativos oferecidos pelo IPv6. Entre eles vamos encontrar: *Mobile IPv6*, *Fast Handover for Mobile IPv6*, *Hierarchical Mobile IPv6* e o *Proxy Mobile IPv6*.

A segunda abordagem, que consideramos "híbridos", sugere a separação entre a identificação e a localização de um dispositivo na rede. Aqui encontramos protocolos como o *Locator / ID Separation Protocol*, *Host Identity Protocol* e *Site Multihoming by IPv6 intermediation*.

2.1. Mobile IPv6

O protocolo de mobilidade inicialmente concebido, MIPv6 [Johnson; Perkins; Arkko, 2004], permite o uso de mobilidade sem a necessidade de qualquer agente externo nas redes estrangeiras. Ao migrar para outra rede, o nó móvel (MN) solicita um endereço IPv6 na nova rede e informa ao seu *Home Agent* (HA) sobre o seu novo local. A partir deste momento, um túnel IPv6 é estabelecido entre o *Mobile Node* (MN) e seu *Home*

Agent (HA). Assim, a comunicação entre *Mobile Node* (MN) e *Correspondent Node* (CN) continua a fluir por este túnel.

A Figura 1 detalha todos os passos do processo de troca de rede, chamado de *handover*; no passo (1), o *Mobile Node* (MN) possui um endereço em sua *Home Network* e uma comunicação estabelecida com o *Correspondent Node* (CN). No passo (2), MN inicia o processo de troca de rede, movendo-se a uma *Foreign Network* (FN). Neste momento ele irá receber um novo endereço IPv6 chamado *Care-of Address* (CoA), esta designação é apenas para distinguir seus dois endereços IPv6.

Como o MN mantém seu antigo endereço, deve enviar um pacote para o seu *Home Agent* (HA) por meio da rede estrangeira, registrando o novo endereço (3) através de uma mensagem de *Binding Update*, onde o HA responde com *Binding Acknowledgement*. Neste momento, passo (4), MN atualiza seu endereço com o CN e, dependendo do suporte a mobilidade de CN, pode estabelecer a comunicação através do túnel, como podemos observar no passo (5), ou diretamente com MN, como no passo (6) [Le; Fu; Hogrefe, 2006].

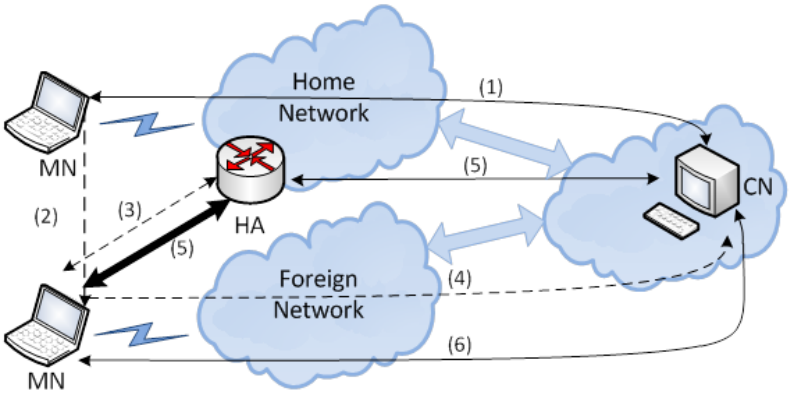

Figura 1. MIPv6 - Arquitetura e operação

2.2. Fast Handover for Mobile IPv6

O *Fast Handover for Mobile IPv6* (FMIPv6) se propõe a minimizar o tempo de configuração do túnel entre MN e HA durante a fase de troca de rede executada no MIPv6. Ele atinge seu objetivo realizando uma conexão com a nova rede, sem perder a conexão com a rede atual. Para realizar isso, o FMIPv6 utiliza informações de nível dois para sinalizar a mudança de uma rede, ou seja, quando um dispositivo móvel reconhece que o sinal do seu *Access Point* (AP) está enfraquecendo e que há um sinal mais elevado de outro AP, ele inicia o processo de conexão para a outra rede usando as novas mensagens introduzida no FMIPv6, mas ainda realizando a sua transmissão através do AP inicial, utilizando para isto duas interfaces de rede.

Neste protocolo, quando o MN realiza a negociação com o novo ponto de acesso (Figura 2), ele envia para o seu *Previous Access Router* (PAR) uma mensagem *Router Solicitation for Proxy Advertisement* (RtSolPr) (1), recebendo em troca uma mensagem *Proxy Router Advertisement* (PrRtAdv) (2), iniciando o processo de obtenção de um

endereço *stateful* ou *stateless*. Este endereço será usado para definir um novo *Care-of Address* (NCoA).

Na posse de seu novo endereço, mas ainda comunicando-se através do seu *Previous Access Router* (PAR), MN envia um *Fast Binding Update* (FBU) (3) para o PAR, solicitando o redirecionamento do tráfego através do *New Access Router* (NAR). Imediatamente PAR envia um *Handover Initiate* (HI) (4) para o NAR, informando os endereços *Previous Care-of Address (PCoA)* e *New Care-of Address* (NCoA) para validá-los.

Em resposta, o PAR envia ao NAR um *Handover Acknowledgment message* (HAck) (5), aceitando o endereço proposto ou indicando o seu novo endereço válido. Após essa negociação, o PAR envia um *Fast Binding Acknowledgment* (FBAck) (6) em retorno a mensagem *Fast Binding Update* (FBU) recebida anteriormente. Neste ponto, o nó móvel envia um *Fast Neighbor Advertisement* (FNA) (7) para o NAR, comunicando a sua presença na nova rede, permitindo que o tráfego transmitido pela rede antiga ao NAR, seja direcionado para o MN (8). Finalmente, o MN informa ao CN seu novo endereço para realizar uma possível otimização de rotas, que permite a comunicação direta, sem a necessidade de trafegar através do PAR (9) [Viinikainen; et al., 2006].

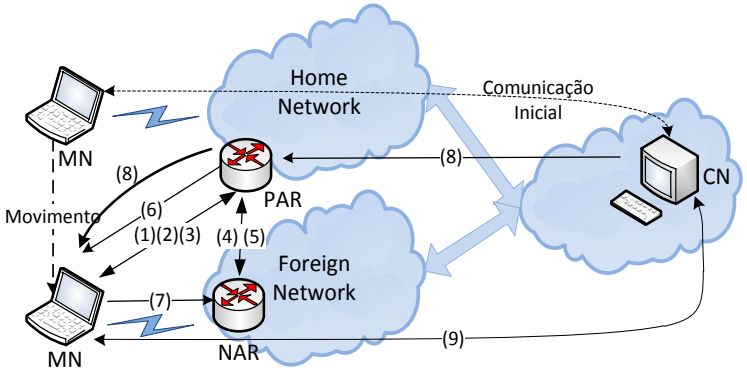

Figura 2. Configuração da conexão no FMIPv6

2.3. Hierarchical MIPv6

O HMIPv6 inclui um novo agente no processo: o *Mobility Anchor Point* (MAP). Este agente é responsável por controlar o domínio de toda a rede móvel, independentemente de quantas redes existem em cada domínio. Com isso, agora possuímos dois tipos de *handovers*: um local, dentro do mesmo domínio de rede e outro considerado externo. Esta segunda abordagem é utilizada cada vez que ocorre mobilidade entre diferentes domínios de rede.

No HMIPv6, MN sempre possui dois endereços de rede: o *Regional Care-of Address* (RCoA) e o *Local Care-of Address* (LCoA). Quando NM se conecta a alguma rede, ele recebe um *Router Advertisement* (RA) contendo os endereços dos MAPs locais. Assim, na mobilidade intradomínio evita-se que o nó móvel precise realizar um *Binding Update* para o *Home Agent*, minimizando o tempo de *handover* [Wang; Li;

Yan, 2009]. Em contraponto, o protocolo aumenta a quantidade de mensagens no *handover* externo, exigindo que o *Mobile Node* execute o processo de *Bind Update* no MAP, no HA e no CN.

Na Figura 3 demonstramos o processo de *handover* entre diferentes domínios. Na etapa (1), MN recebe um *Router Advertisement* contendo os endereços dos MAPs locais, no passo (2) MN envia um *Local Binding Update* (LBU) ao MAP e um *Binding Update* (BU) para o seu *Home Agent*, passo (3), informando seu novo *Local Care-of Address* (LCoA) e *Regional Care-of Address* (RCoA). Dessa forma, o tráfego dirigido à sua rede doméstica é encaminhado para o MAP, que encapsula os pacotes para o LCoA de MN, passo (4). Isso é necessário até que o NM informe o seu RCoA novo para o CN, possibilitando uma comunicação direta entre MN e CN, passo (5).

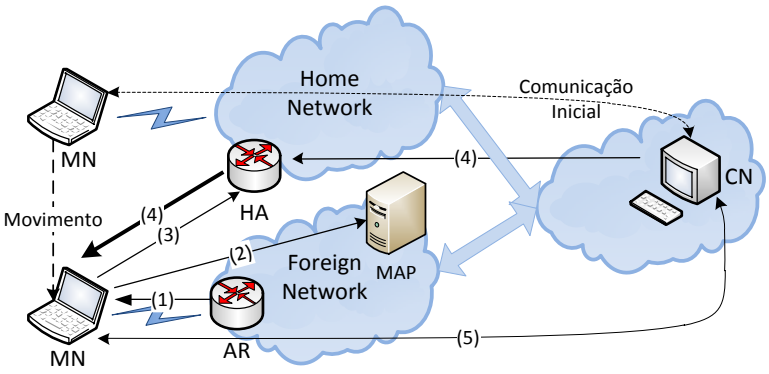

Fig. 3. Processo de configuração da conexão no HMIPv6

2.4. Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) tem uma abordagem diferente, propondo criar um ponto central no controle da mobilidade. Utilizando esse conceito, o MN não precisa executar qualquer operação de troca de mensagens durante a migração de sua rede local para uma rede estrangeira. Esta responsabilidade será feita por duas novas entidades: o *Mobile Access Gateway* (MAG), localizado na rede estrangeira, e o *Local Mobility Anchor* (LMA), situado na sua rede local. Para explicar o funcionamento desta proposta, a Figura 4 a seguir, ilustra o fluxo da troca de mensagens.

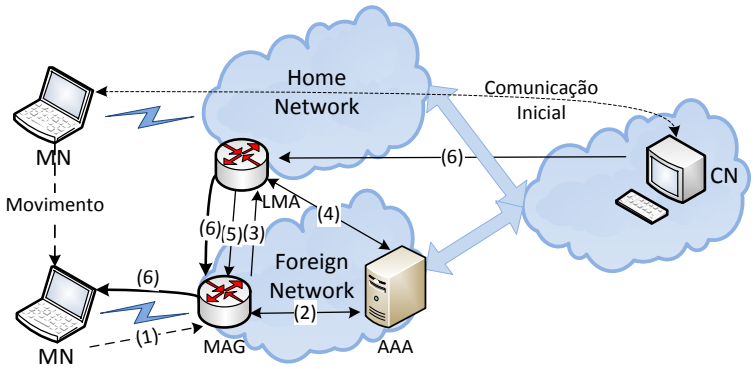

Fig. 4. Processo de configuração da conexão no PMIPv6

Na etapa (1), quando o MN acessar uma rede estrangeira, é realizado um procedimento de autenticação. No passo (2), o MAG obtém o perfil do MN em um *AAA Server (Authentication, Authorization and Accounting Server)*. Então, no passo (3), o MAG envia um *Proxy Binding Update* (PBU) para o LMA, em nome da MN.

Em (4), uma vez que a LMA recebe uma mensagem PBU e verifica as políticas de segurança, ele aceita a mensagem PBU. Em seguida, no passo (5), o LMA envia um *Proxy Binding Acknowledgment* (PBA) para MAG, incluindo o prefixo da rede do MN e atualiza a rota para a rede do MN sobre um túnel até o MAG.

Finalmente, em (6), após realizar a configuração do túnel, o MAG envia *um Router Advertisement* (RA) para o MN com as configurações de sua rede. A partir deste ponto, todas as mensagens enviadas e recebidas por MN será realizada através do MAG, utilizando o túnel até o LMA [Kong; Lee, 2008].

2.5. HIP - Host Identity Protocol

Em contraponto aos protocolos apresentados, o protocolo HIP assim como o LISP – *Locator / ID Separation Protocol* [Farinacci et al, 2011] e o SHIM6 - *Site Multihoming by IPv6 Intermediation* [Liu; Bi; Wang, 2009] propõem uma nova abordagem ao realizar a separação entre a identificação (ID) e a localização (LOC) de um nó na rede.

No HIP, o host possui um par de chaves assimétricas e, através de um *hash* da chave pública, obtém o *Host identity Tag* (HIT), utilizado para **identificar** o *host* enquanto o endereço IP é utilizado para **localizar** o *host*.

Para realizar a comunicação entre *hosts*, utilizando apenas os endereços HIT, necessita-se conhecer a localização do HIT de destino, o que pode ser obtido com o uso de um novo campo *Resource Record* (RR), incluído nos servidores de DNS. Assim, quando um nó da rede necessita descobrir o IP de *Correspondent Node* (CN), ele realiza uma consulta DNS através do identificador HIT, recebendo como resposta o IP do CN.

Quando a comunicação a ser estabelecida é entre um MN e um CN, necessita-se uma constante atualização do DNS para saber a atual localização do MN, o que resulta em falhas de comunicação devido ao tempo de convergência das informações na hierarquia de servidores DNS. No intuito de resolver esta dificuldade, foi proposta a inclusão de um novo agente, o *Rendez-vous Server* (RVS), com o objetivo de manter atualizada a informação de localização dos nós móveis que utilizam HIP. Assim, conforme a Figura 5, quando um CN realizar a requisição do endereço IP de um MN ao DNS (1), receberá como resposta o endereço de um RVS (previamente cadastrado no DNS). No momento que o CN iniciar a comunicação com um RVS, este agente verificará em sua tabela a atual localização do MN e encaminhará o pacote a ele (2), que responderá diretamente ao CN (3), pois recebeu o endereço de CN no pacote redirecionado pelo RVS [Moskowitz et al, 2008]. Após a descoberta dos endereços de localização, a comunicação ocorrerá através dos endereços HIT, já conhecidos por ambos os nodos.

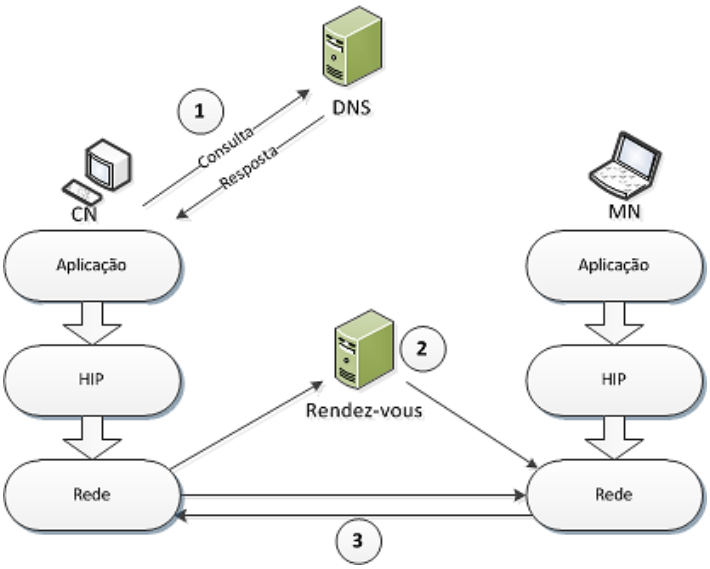

Figura 5. HIP-Comunicação entre CN e MN

2.6. LISP - Locator/ID Separation Protocol

O LISP é um protocolo que tem por objetivo prover *multihoming*, isto é, permitir que uma rede possa ser acessada independente de sua localização atual. Para isto, o LISP separa o endereçamento IP em duas partes: o *Endpoint ID* (EID), referente ao endereço IP permanente de identificação de um nó na rede e o *Routing Locator* (RLOC), um endereço IP roteável atribuído aos roteadores de borda da rede.

Basicamente, o LISP trabalha encapsulando os pacotes entre dois endereços EID através dos roteadores de borda de rede, chamados de *Ingress Tunnel Router* (ITR) e *Egress Tunnel Router* (ETR). Esses dispositivos são responsáveis por armazenar o mapeamento de endereços entre EID e RLOC. Por exemplo: quando um ponto interno da rede necessita se comunicar com um site remoto, ele realiza uma consulta DNS que retorna o endereço EID do destino, com isto, o pacote é enviado até um ITR na borda da rede utilizando um protocolo IGP (*Interior Gateway Protocol*), que encapsulará seu pacote em um novo pacote LISP, contendo o endereço RLOC de origem e o endereço RLOC do destino. Quando este pacote chegar ao ETR de destino ele será desencapsulado e encaminhado ao EID [Farinacci et al, 2011].

Com estas características, o LISP pode ser utilizado para mobilidade, pois MN pode possuir uma implementação de ITR/ETR e, na ocorrência de troca de rede, quando um MN entrar em uma nova rede, este receberá um novo endereço de localização que podemos chamar de LLOC (referente ao RLOC Local). Com isto, a mensagem a ser enviada ao CN será encapsulada em um pacote LISP contendo seu novo endereço de localização LLOC e endereçada ao endereço RLOC do destinatário. Esta mensagem quando recebida pelo ITR da borda da rede, será novamente encapsulada e encaminhada a um Proxy ETR, que realizará a primeira desencapsulação e encaminhará ao ETR, que por sua vez entregará ao CN. Quando o CN responder à mensagem ao MN, o ITR de

CN encaminhará a mensagem para o endereço LLOC de MN, encapsulada em um pacote LISP endereçado ao endereço RLOC do ETR, de onde se encontra MN. O fluxo deste processo pode ser observado na Figura 6.

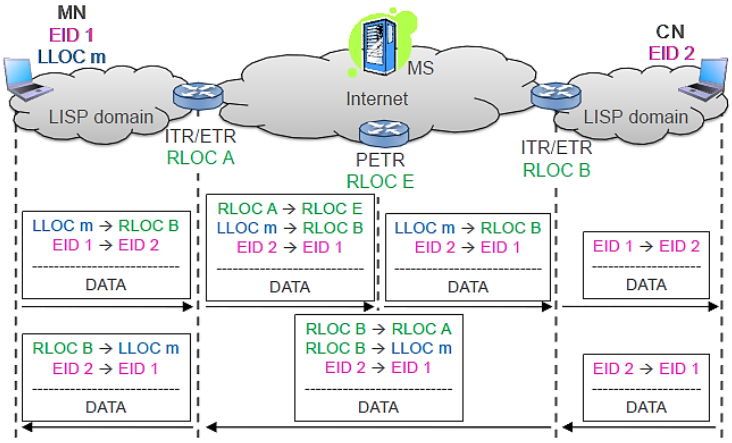

Figura 6: Comunicação entre MN e CN em redes LISP [Menth; Klein; Hartmann, 2010]

Assim, utilizando os endereços EID como origem / destino de mensagens, as camadas superiores da pilha TCP/IP não percebem a alteração de rede, garantindo a conectividade.

2.7. SHIM6 - Site Multihoming by IPv6 Intermediation

SHIM6 é uma nova subcamada entre a camada de rede (*layer*-3) e a camada de transporte (*layer*-4) que contém um ou mais endereços dos hosts de origem e destino, utilizados para servir como **localizador** e **identificador** de uma conexão.

Quando uma sessão inicia, a camada SHIM6 escolhe um par de localizadores de ambos os lados para configurar uma sessão de transmissão, utilizando os endereços ULID (*Upper Layer Identifier*) para estabelecer uma conexão. Na ocorrência de falha na conexão ou congestionamento, a camada SHIM6 fica responsável pela comutação do tráfego para um novo par localizador (contexto). Este processo ocorre sobre a camada IP e todo o processo é absolutamente transparente para aplicações das camadas superiores [Barré; Ronan; Bonaventure, 2011].

3. Trabalhos relacionados

Li e Yang [2009] comparam o *handover* do HMIPv6 e MIPv6, não explicitando a metodologia utilizada em seus experimentos. Oliveira, Cascardo e Loureiro [2003] realizam a comparação de *Bind Updates* enviados pelos referidos protocolos através de simulações. Kong e Li [2008], em sua pesquisa, comparam o tempo de *handover* dos protocolos MIPv6, HMIPv6, FMIPv6 e PMIPv6 através de simulações e análise das mensagens descritas nas especificações dos protocolos, assim como Costa, Moreno e Hartenstein [2003], que através de simulações analisaram o tempo de *handover* e a quantidade pacotes perdidos pelos protocolos FMIPv6, HMIPv6 e suas subversões,

levando em consideração nas suas simulações a escalabilidade dos protocolos em situações com até quatro *Access Points* e cinquenta *Mobile Nodes*.

Estes e outros trabalhos demonstram o anseio pela comparação entre os protocolos de mobilidade a fim de demonstrar suas funcionalidades e aplicabilidades sobre o mesmo viés. Contudo, mesmo a partir destes trabalhos não é possível classificar os referidos protocolos quanto ao tempo de *handover* e as funcionalidades implementadas devido as diferentes metodologias utilizadas nos trabalhos referenciados.

4 Metodologia

Para analisar os protocolos supracitados, utilizamos a estrutura mostrada na Figura 7, compostas de: um Pentium 4 de 2,8 GHz e 1 GB de RAM para atuar como CN; um Netbook Aton N550 com 2 GB de RAM para atuar como MN; dois *Access Points* e duas máquinas virtuais para atuarem como roteadores, auxiliando e/ou controlando a mobilidade do MN entre as redes. As máquinas virtuais utilizadas em todos os testes possuiam um único *core*, 768 MB RAM e o sistema operacional Ubuntu 10.04.2 LTS 32 bits, virtualizados sobre um computador Intel i3 de 3,1 GHz e 4 GB de RAM.

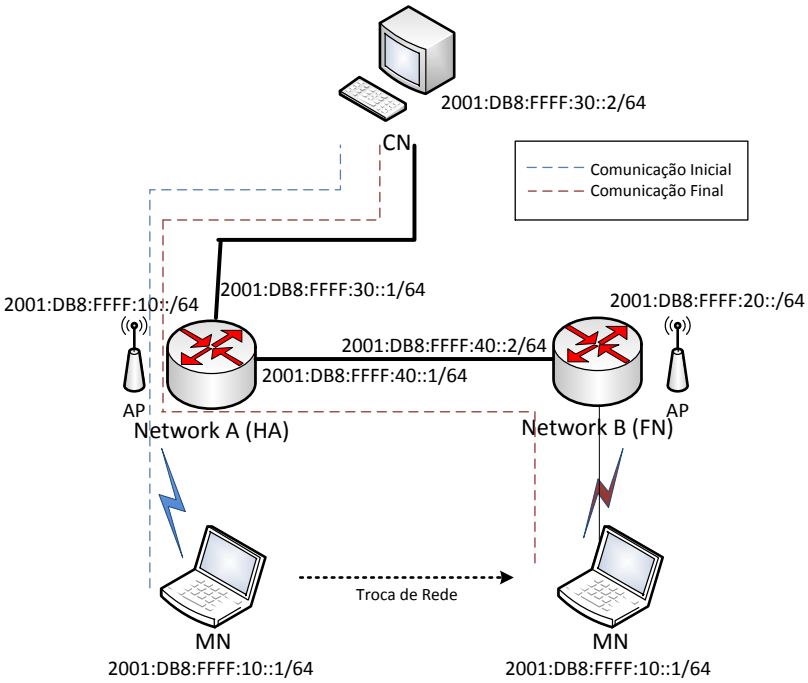

Fig. 7. Estrutura de rede utilizada nos experimentos

Nesta estrutura, analisamos as seguintes implementações:

- MIPv6: umip versão 2.0.2-0.4 [UMIP, 2011].
- FMIPv6: fmip versão 1.0-rc1 [FMIPV6, 2011].
- HMIPv6: versão 0.9.7 [Silva; Almeida, 2011] e radvd [Daley; 2011].
- PMIPv6: pmip6d [EURECOM, 2011].

- HIP: HIPL versão 1.0.6-5193. [InfraHIP, 2011].
- LISP: OpenLISP versão 0.1.0. [OpenLISP, 2011].
- SHIM6: LinShim6 [Barré; Ronan; Bonaventure, 2011].

Para analisar o tempo de *handover* foram utilizados dois métodos: o primeiro com envio de pacotes ICMP a uma taxa de um pacote por milissegundo e outro através da transferência de dados por TCP entre MN e CN.

5. Resultados

Primeiramente analisou-se o tempo de *handover* físico, ou seja, o tempo que o hardware e o sistema operacional demoram para desconectar de um *Access Point* e reconectar em outro. Este tempo é uma constante, pois é um valor independente do protocolo.

Neste experimento obteve-se um tempo de 5,152 segundos, tempo em que o nó móvel ficou desconectado de qualquer *Access Point (AP).* Todos os experimentos foram executados cinco vezes, e obtiveram um coeficiente de variação igual ou inferior a 0,02.

Nos experimentos, foi mensurado o tempo de *handover* total, isto é, o físico somado ao lógico. O *handover* lógico inclui o tempo gasto com endereçamento e estabelecimento de conectividade entre MN e CN. Na Figura 8(a), demonstramos o *handover* nos protocolos classificados como IPv6 "puros": MIPv6, FMIPv6, HMIPv6 e PMIPv6. Nestes casos foi obtido um *handover* total entre 1,904 e 9,432 segundos com o envio de pacotes ICMP. A grande diferença em favor do FMIPv6 é justificada pelo uso de duas interfaces *wireless,* necessárias para o funcionamento da implementação durante o processo de *handover* e não realmente uma melhora do *handover* lógico, pois somando o *handover* físico (5.152s), o *handover* total eleva-se em mais de três vezes (7.056s). O PMIPv6 obteve o melhor *handover, apenas* 21 milissegundos acima do *handover* físico, devido ao envio da mensagem de *Router Solicitation* executada pelo MN, que dispara o processo de mobilidade ao MAG e ao LMA, não necessitando de qualquer processamento adicional por parte de MN.

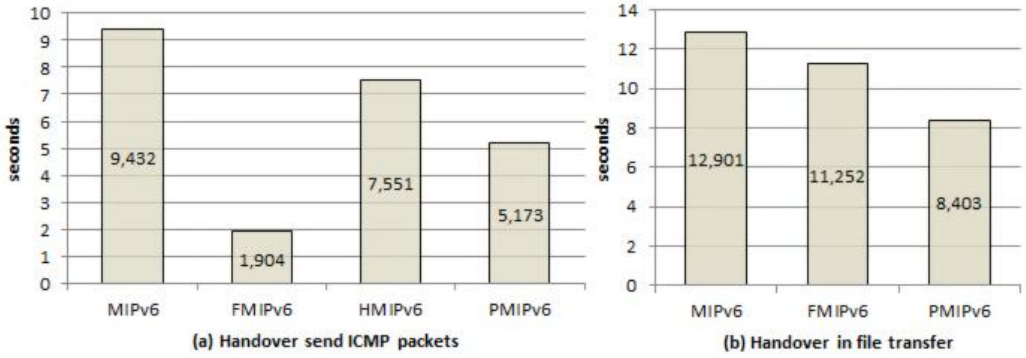

Figura 8. Tempos de *handover dos* protocolos puros

A fim de simular a utilização real dos protocolos foram realizados *handovers* durante a transferência de dados por TCP. Nestes experimentos foram obtidos *handovers* maiores devido à ocupação do canal de comunicação pela transferência de

dados, que, de acordo com a Figura 8(b), resultaram em tempos entre 8,403 e 12,901 segundos. Nestes experimentos, não foi possível mensurar a transferência de dados utilizando o protocolo HMIPv6 devido a problemas na implementação do mesmo (o túnel entre HA e CN não estabelece depois que o MN acessa a FN).

Na análise do tempo de *handover* dos protocolos híbridos (HIP, LISP e SHIM6), como demonstrado no gráfico resumo da Figura 9, o SHIM6, apesar de parecer uma boa solução, onde MN possui múltiplos endereços de localização, apresentou uma baixa performance de *handover*, pois só realiza a troca de contexto (endereçamento) após o tempo de *keepalive* definido na implementação do protocolo, valor este definido em 15 segundos por sugestão dos desenvolvedores, apresentando instabilidades com valores inferiores. Neste mesmo protocolo, não foi possível mensurar o tempo de *handover* por ICMP, já que o procedimento de troca de contexto só é ativado na pré-existência de uma conexão TCP entre os nodos envolvidos.

Entretanto, uma possível utilização do SHIM6 para mobilidade foi proposta por Barré, et al. [2009], na utilização em conjunto com o MIPv6, onde após o processo *handover* executado pelo MIPv6, SHIM6 poderia ser utilizado para estabelecer uma conexão direta entre CN e MN, sem a necessidade de criar um túnel passando pelo *Home Agent* do MN.

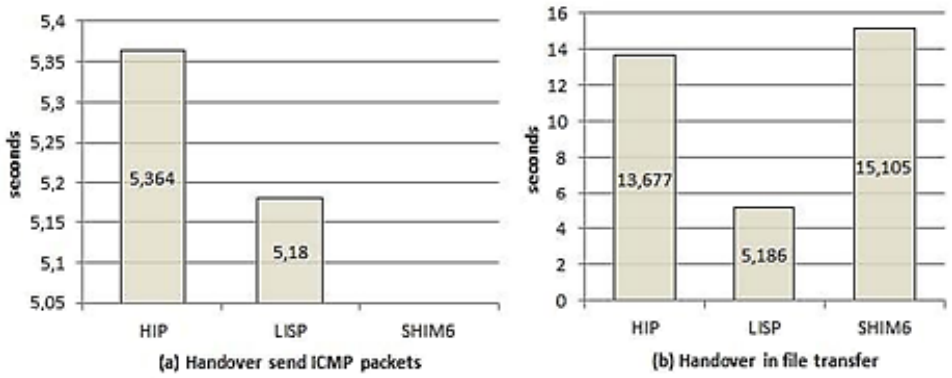

Figura 9: **Tempos de h*andover dos protocolos híbridos***

Na análise do protocolo LISP, este apresentou o melhor tempo de troca de rede, tanto nos experimentos utilizando ICMP como nos experimentos de transferência de arquivos, pois utiliza um tunelamento *IP-over-UDP*, sem a realização de autenticações ou IPsec como nos protocolos MIPv6, FMIPv6 e HMIPv6. Contudo, é um protocolo que por definição em RFC, utiliza endereços privados para a identificação de um nodo, necessitando a utilização de *Proxy* ou *Network Address Translation* (NAT) para o encaminhamento de pacotes na Internet e, adicionalmente, uma nova estrutura de servidores para armazenar o mapeamento de endereços (*MAP Server*) [Fuller; Farinacci, 2010] ou de uma nova tabela BGP formada com endereços EID e endereços RLOC (LISP-ALT) [Fuller at al., 2011], o que aumenta consideravelmente a quantidade de agentes na rede.

No protocolo HIP, o nível de segurança da comunicação são mais elevados se comparados com o LISP. Neste protocolo, ao ser identificada a troca da rede é realizada uma nova autenticação entre os nodos, o que eleva o seu tempo de estabelecimento de conexão e consequentemente o tempo de *handover* total. Entretanto, se comparado aos protocolos de mobilidade de IPv6 “puros” que utilizam IPsec, seu tempo de *handover* encontra-se no mesmo limiar, porém com as vantagens da validação de endereços, o que provê uma maior segurança.

Na análise sobre a facilidade de implantação dos protocolos de mobilidade e de seus agentes, verificamos que nenhuma das implementações disponíveis até o momento pode ser considerada "*user frendly*"', pois nenhuma possui um *wizard* ou ambiente gráfico de configuração para nenhum de seus agentes. Sendo assim, classificamos os protocolos pelo número de aplicações/agentes necessários a serem configurados e pela complexidade de configuração de cada um deles, utilizando para esta classificação a quantidade de parâmetros e opções a serem alteradas em seus arquivos de configuração.

Como demonstrado na Tabela 1, o MIPv6, FMIPv6 e HMIPv6 receberam um alto grau de complexidade devido as configurações do IPSec necessárias para seu funcionamento, em contrapartida o PMIPv6 é simples de configurar e não necessita de nenhuma configuração no *Mobile Node*. Os protocolos HIP e SHIM6 possuem comportamentos parecidos, contudo o HIP possui agentes bem definidos e mais estáveis que o SHIM6. Por fim, o protocolo LISP apesar de estável, possui uma implementação que não percebe automaticamente a ocorrência da mobilidade, não sendo indicado atualmente para este propósito.

Tabela 1. Complexidade das implementações de mobilidade analisadas

	Mobile Node		Home Network		Foreign Network		Correspondent Node	
Protocolo	**Agentes**	**Complexidade**	**Agentes**	**Complexidade**	**Agentes**	**Complexidade**	**Agentes**	**Complexidade**
MIPv6	1	Alta	2	Alta	1	Baixa	--	--
FMIPv6	2	Alta	3	Alta	3	Média	--	--
HMIPv6	1	Alta	2	Alta	2	Média	--	--
PMIPv6	--	--	1	Baixa	1	Baixa	--	--
HIP	1	Média	--	--	--	--	1	Média
LISP	--	--	2	Média	2	Média	--	--
SHIM6	2	Alta	--	--	--	--	2	Alta

6. Conclusão

Neste artigo testamos algumas propostas de provimento de mobilidade para IPv6, demonstrando a usabilidade de cada protocolo estudado. Na análise realizada por transferência de dados, não houve problemas de perda de conexão. Na análise do tempo de *handover*, FMIPv6 tem o menor tempo, no entanto, é incomum a existência de duas interfaces *wireless* em dispositivos móveis hoje em dia, o que elege a implementação do protocolo PMIPv6 como o melhor resultado a este respeito, com um tempo aceitável de

handover, baixa utilização do pacote de controle e compatibilidade com qualquer sistema operacional utilizado no *Mobile Node*, pois o *Mobile Node* não precisa realizar qualquer gestão sobre a mobilidade. Porém, este protocolo não implementa a segurança advinda do IPsec, implementada nos outros protocolos classificados como "puros".

Nos protocolos "híbridos", o HIP se mostrou o protocolo mais viável a utilização, porque implementa segurança de dois níveis (de endereçamento e de comunicação), através de troca de chaves criptográficas, sem a utilização de NAT proposta pelo LISP e com um tempo de *handover* melhor que o SHIM6. No entanto, é necessário analisar melhor o impacto da criação de túneis entre cada nó móvel e sua *home network*, como realizado por Costa, Moreno e Hartenstein [2003], pois uma grande quantidade de túneis podem gerar problemas de escalabilidade em grandes redes.

Concluímos que a mobilidade sobre IPv6 como uma solução fim-a-fim, precisa evoluir. Identificou-se que mais estudos são necessários para prover serviços utilizando mobilidade sobre IPv6 para o usuário final. Neste ponto pretendemos avançar os estudos sobre mobilidade utilizando protocolos de *layer*-2 do modelo de referência OSI, como MPLS e *OpenFlow*.

7. Referências

Barré, S., Dhraief, A., Montavont, N. and Bonaventure, O. (2009) "MipShim6: une approche combinée pour la mobilité et la multi-domiciliation". Actes du 14ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP), pp. 113-124.

Barré, S., Ronan, J. and Bonaventure, O. (2011) "Implementation and evaluation of the Shim6 protocol in the Linux kernel". Computer Communications Journal, pp. 1685-1695.

Costa, X. P., Moreno, M. T. and Hartenstein, H. (2003) "A performance comparison of Mobile IPv6, Hierarchical Mobile IPv6, fast handovers for Mobile IPv6 and their combination". Sigmobile, pp. 5-19.

Daley, G. (2011) "Hierarchical Mobile IPv6 Research at CTIE", http://www.ctie.monash.edu.au/ipv6/hmipv6.htm

EURECOM (2011) "Open Air Interface - Proxy Mobile IPv6", http://www.openairinterface.org/components/page1095.en.htm

Farinacci, D., Fuller, V., Meyer, D. and Lewis, D. (2011) "Locator/ID Separation Protocol (LISP)". draft-ietf-lisp-10.txt. IETF.

FMIPV6 (2011), "FMIPV6.org", http://www.fmipv6.org/

Fuller, V. and Farinacci, D. (2010) "LISP Map Server". draft-ietf-lisp-ms-06.txt. IETF.

Fuller, V., Farinacci, D., Meyer, D. and Lewis, D. (2011) "LISP Alternative Topology (LISP+ ALT)". draft-ietf-lisp-alt-05.txt. IETF.

InfraHIP (2011) "Infrastructure for HIP", http://infrahip.hiit.fi

Johnson, D., Perkins, C. and Arkko, J. (2004) “RFC3775 - Mobility Support in IPv6”. IETF.

Kong, K. and Lee, W. (2008) “Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6”. IEEE Wireless Communications, pp. 36-45.

Koodli, R. (2009) “RFC5268 - Mobile IPv6 Fast Handovers”. IETF.

Le, D., Fu, X. and Hogrefe, D. (2006) “A review of mobility support paradigms for the internet”. IEEE Communications Surveys & Tutorials, pp. 38-51.

Leung, K., Devarapalli, V., Chowdhury, K. and Patil, B. (2008) “RFC5213 - Proxy Mobile IPv6. IETF.

Limoncelli, T. A. and Cerf, V. G. (2011) “Successful Strategies for IPv6 Rollouts. Really”. Commun. ACM, vol. 54, no. 4, pp. 44-48.

Liu, S.; Bi, J. and Wang, Y. (2009) “A Shim6-Based Dynamic Path-Selection Mechanism for Multi-homing”. Evolving Internet 2009, pp. 46-51.

Menth, M., Klein, D. and Hartmann, M. (2010) “Improvements to LISP Mobile Node”. 22nd International Teletraffic Congress (ITC), pp.1-8.

Morr, D. (2011) “T-Mobile is pushing IPv6. Hard”, http://www.personal.psu.edu/ dvm105/blogs/ipv6/2010/06/t-mobile-is-pushing-ipv6-hard.html.

Moskowitz, R., Nikander, P., Jokela, P. and Henderson, T. (2008) “RFC5201 – Host Identity Protocol”. IETF.

Nordmark, E. and Bagnulo, M. (2009) “RFC5333 - Shim6: Level 3 Multihoming Shim Protocol for IPv6”. IETF.

Oliveira, E. R. de, Cascardo, T. L. de S. and Loureiro, A. A. F. (2003) “Análise dos Mecanismos de Gerenciamento de Mobilidade no IPv6”. XXI Simpósio Brasileiro de Redes de Computadores.

OpenLISP (2011) “The OpenLISP Project”, http://www.openlisp.org/

Perkins, Charles E. (2002) “Mobile IP”. IEEE Communications Magazine, Maio.

Silva, C. M. and Almeida, F. M. “Mobilidade em Redes IP: Análise dos Protocolos MIPv6 e HMIPv6”, http://code.google.com/ p/projfin-hmip/

Soliman, H., Castelluccia, C., ElMalki, K. and Bellier, L.“RFC5380 - Hierarchical Mobile IPv6 (HMIPv6) Mobility Management”. IETF.

UMIP (2011), “UMIP.org”, http://www.umip.org/

Viinikainen, A., Puttonen, J., Sulander, M., Hämäläinen, Ylönen, T. and Suutarinen, H. (2006) “Flow-based fast handover for mobile IPv6 environment – implementation and analysis”. Computer Communications, no. 16. vol 29. pp. 3051-3065.

Wang, Z., Li, X. and Yan, B. (2009) “Fast inter-MAP handover in HMIPv6”. First International Workshop on Education Technology and Computer Science, pp. 918-922.