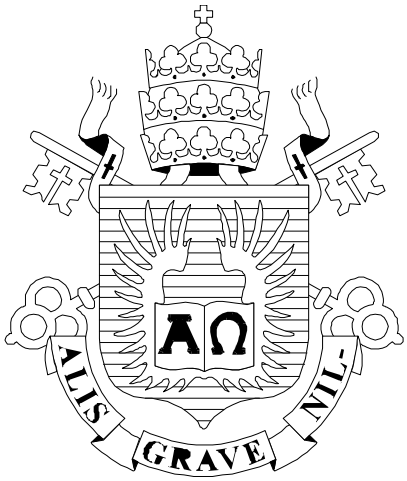

PUC

ISSN 0103-9741

Monografias em Ciência da Computação
n° 27/08

Evolução da Otimização do *Handoff* no *Mobile* IP

Anderson Oliveira da Silva
Sérgio Colcher

Departamento de Informática

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO
RUA MARQUÊS DE SÃO VICENTE, 225 - CEP 22451-900
RIO DE JANEIRO - BRASIL

Monografias em Ciência da Computação, No. 27/08 ISSN: 0103-9741
Editor: Prof. Carlos José Pereira de Lucena Julho, 2008

Evolução da Otimização do *Handoff* no *Mobile* IP*

Anderson Oliveira da Silva e Sérgio Colcher

Departamento de Informática – Pontifícia Universidade Católica (PUC-Rio)

{anderson, colcher}@inf.puc-rio.br

Abstract. Mobile IP is intended to enable nodes to move from one IP subnet to another. Although its architecture be suitable for its purpose, the process associated to node transition among IP subnets that change the point of attachment, known as handoff or handover, presents two factors that disturb real-time applications and interactive or delay sensitive ones. The first factor is the high latency of this process that generates a long period of time without receiving packets. The second one refers to the high number of packets dropped or delayed because of the change of the point of attachment. This monograph aims to present the evolution of MIP handoff optimization with focus on proposals that were published as RFCs and Drafts, also presenting results of researches that demonstrate the effective gain of these optimizations.

Keywords: Handoff, MIP, HMIPv6, FMIPv6, Enhanced Route Optimization

Resumo. O Mobile IP foi concebido para permitir a movimentação de nós de uma subrede IP para outra. Embora sua arquitetura atenda seu propósito, o processo de transição de um nó entre subredes IP com a mudança do ponto de acesso, chamado de *handoff* ou *handover*, apresenta dois fatores que prejudicam aplicações de tempo real, interativas ou sensíveis a atrasos. O primeiro fator é a grande latência do processo, que gera um longo período de tempo sem recepção de pacotes. O segundo se refere ao grande número de pacotes descartados ou atrasados em função da mudança do ponto de acesso. Essa monografia visa apresentar a evolução das otimizações do handoff para o MIP com enfoque nas propostas que foram publicadas como RFCs e Drafts, abordando ainda, os resultados de estudos que demonstram o ganho efetivo dessas otimizações.

Palavras-chave: Handoff, MIP, HMIPv6, FMIPv6, Enhanced Route Optimization.

---

* Trabalho patrocinado pelo Ministério de Ciência e Tecnologia da Presidência da República Federativa do Brasil (e agência de fomento e o número do processo, se aplicável). (Em Inglês: This work has been sponsored by the Ministério de Ciência e Tecnologia da Presidência da República Federativa do Brasil)

Responsável por publicações

Rosane Teles Lins Castilho
Assessoria de Biblioteca, Documentação e Informação
PUC-Rio Departamento de Informática
Rua Marquês de São Vicente, 225 - Gávea
22453-900 Rio de Janeiro RJ Brasil
Tel. +55 21 3527-1516 Fax: +55 21 3527-1530
E-mail: bib-di@inf.puc-rio.br
Web site: http://bib-di.inf.puc-rio.br/techreports/

Sumário

1 Introdução

O Mobile IP foi concebido para permitir a movimentação de nós de uma subrede IP para outra. A mobilidade pode ser feita através de mídias homogêneas ou heterogêneas, ou seja, independente da tecnologia aplicada na camada inter-rede, contanto que o endereço IP do nó móvel permaneça o mesmo após tal movimentação. [1]

Embora sua arquitetura atenda seu propósito, o processo de transição de um nó entre subredes IP com a mudança do ponto de acesso, chamado de *handoff* ou *handover*, apresenta dois fatores que prejudicam aplicações de tempo real, interativas ou sensíveis a atrasos. O primeiro fator é a grande latência do processo, que gera um longo período de tempo sem recepção de pacotes. O segundo se refere ao grande número de pacotes descartados ou atrasados em função da mudança do ponto de acesso.

A primeira especificação de suporte à mobilidade foi feita para o IPv4, dando origem ao MIPv4 (Mobile IPv4) [1]. Com o advento do IPv6, o suporte à sua mobilidade foi elaborado com base nas experiências relacionadas ao MIPv4 e com aproveitamento das características peculiares do IPv6. Essa nova especificação deu origem ao MIPv6 (Mobile IPv6) [6]. Ambos têm evoluído no sentido de otimizar o handoff, minimizando sua latência e reduzindo o atraso e a perda de pacotes. Normalmente, as soluções para uma especificação são adaptadas para outra, e vice-versa.

Esse trabalho visa apresentar a evolução das otimizações do handoff para o MIP com enfoque nas propostas que foram publicadas como RFCs e Drafts, abordando ainda, os resultados de estudos que demonstram o ganho efetivo dessas otimizações.

2 Mobilidade no IPv4

Esse capítulo faz uma abordagem básica do suporte à mobilidade IP no IPv4, conforme especificado em [1]. Os objetivos são: (i) apresentar as entidades funcionais do MIPv4 (Mobile IPv4); (ii) apresentar as operações de suporte à mobilidade; (iii) apresentar as extensões para otimização do roteamento do MIPv4; e (iv) identificar os problemas que afetam a comunicação durante o handoff.

2.1 Entidades Funcionais do MIPv4

O Mobile IP é formado pelas seguintes entidades funcionais: [1]

- ***Mobile Node (MN)*** – representa um host ou um roteador que altera seu ponto de acesso quando migra de uma rede ou subrede para outra. Pode mudar de localização sem modificar seu endereço IP e pode continuar a se comunicar com outros nós da Internet em qualquer localização utilizando seu endereço IP (constante), assumindo-se que uma conectividade do nível de enlace a um ponto de acesso esteja disponível.
- ***Home Agent (HA)*** – representa um roteador na *home network* (HN) de um MN que faz o tunelamento de datagramas para entrega ao MN quando o mesmo se encontra fora de seu home, além de manter informação sobre a corrente localização do MN.

- ***Foreign Agent (FA)*** – representa um roteador na rede visitada pelo MN, também conhecida como *foreign network* (FN), que provê serviço de roteamento ao MN enquanto está registrado. O FA entrega ao MN os datagramas recebidos através do túnel estabelecido com o HA. Para os datagramas enviados pelo MN, o FA pode servir como roteador default para MNs registrados.

Além dessas entidades, os hosts com os quais o MN se comunica são conhecidos como *correspondent nodes* (CNs). Esses hosts podem ser móveis ou estacionários.

2.2 Operação do MIPv4

Os passos a seguir descrevem a operação do MIPv4 de forma sucinta.

1. Anúncio de Presença

Os agentes de mobilidade (HA e FA) anunciam suas presenças enviando periodicamente mensagens de *Agent Advertisement*. No entanto, o MN pode opcionalmente solicitar uma mensagem de Agent Advertisement de qualquer agente de mobilidade acessível através da mensagem *Agent Solicitation*. A Figura 1 ilustra essa operação na HN.

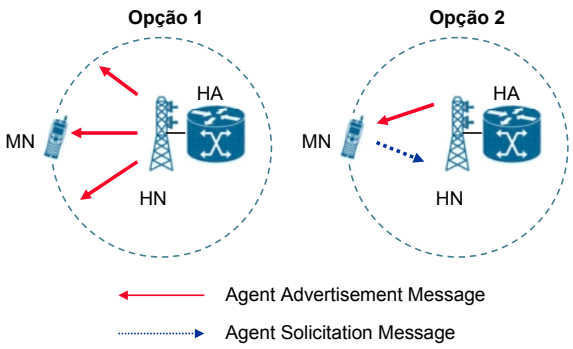

Figura 1 – Anúncio de presença.

2. Determinação da Rede

Através das informações existentes na mensagem Agent Advertisement, o MN determina se está na HN ou na FN. Se o MN estiver na HN, sua operação será equivalente a um nó estacionário, ou seja, sem serviço de mobilidade. A Figura 2 ilustra essa operação.

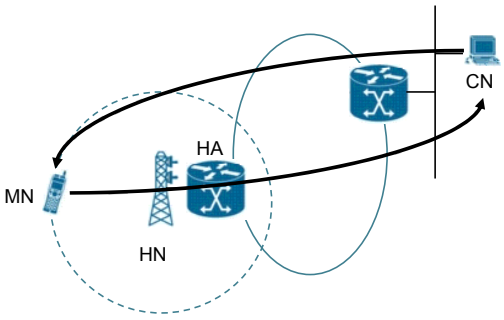

Figura 2 – Operação do MN na HN.

3. Registro do MN na FN

Quando o MN detecta que se moveu para uma FN, um endereço *care-of address* (CoA) deve ser obtido nessa FN. Esse endereço pode ser obtido a partir do conteúdo da mensagem Agent Advertisement, conhecido assim como *foreign agent care-of address* (corresponde ao endereço do FA), ou por algum mecanismo de atribuição externo, como DHCP, conhecido assim como *co-located care-of address* (corresponde a um endereço válido na FN). Em seguida, o MN registra seu novo care-of address em seu HA através da troca das mensagens *Registration Request* e *Registration Reply*, via FA ou diretamente, dependendo do care-of address obtido. A Figura 3 ilustra o registro do care-of address em ambos os casos.

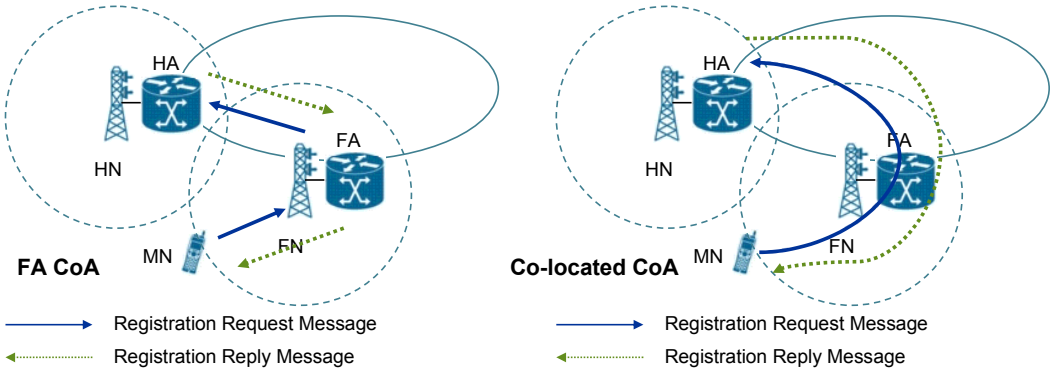

Figura 3 – Registro do care-of address no HA.

4. Tunelamento de Datagramas

Datagramas enviados para o home address do MN são interceptados pelo HA e tunelados pelo HA para o CoA do MN, recebidos no ponto final do túnel (que pode ser o FA ou o próprio MN, dependendo do CoA obtido), e finalmente entregues ao MN. A figura 4 ilustra a operação de tunelamento.

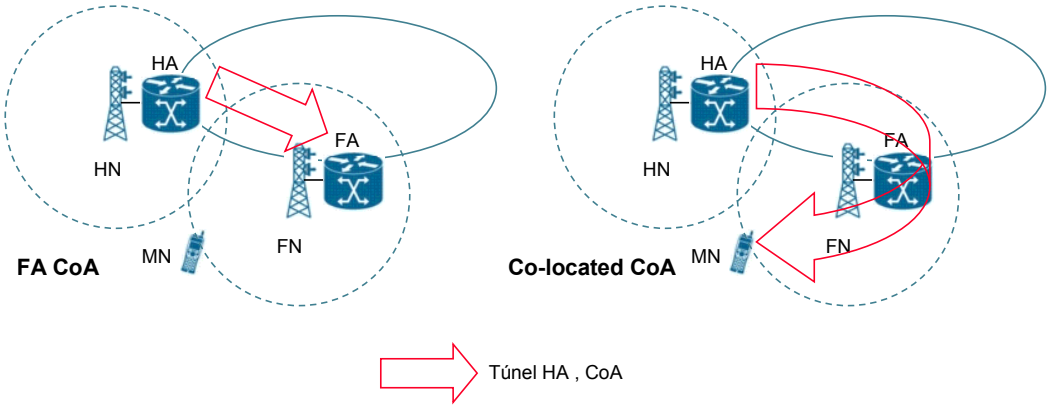

Figura 4 – Tunelamento de datagramas entre o HA e o CoA do MN.

Na direção inversa, os datagramas enviados pelo MN são geralmente entregues ao destino através dos mecanismos tradicionais de roteamento IP, sem necessariamente

passar pelo HA. A figura 5 ilustra essa operação de comunicação entre o MN e o CN, com MN localizado na FN.

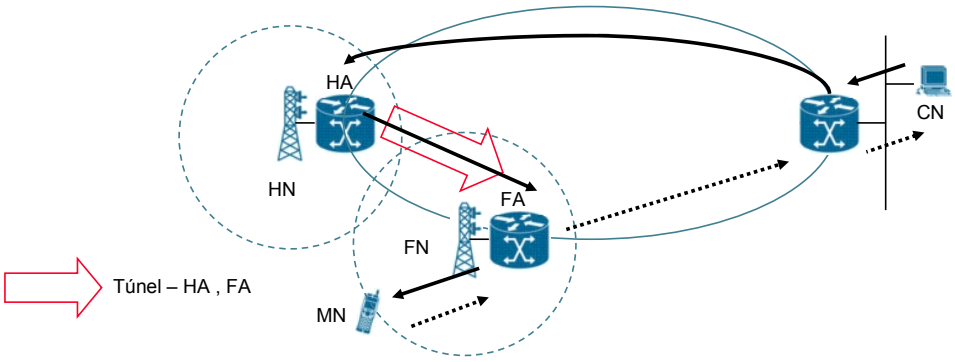

Figura 5 – Comunicação entre o MN e o CN, com MN localizado na FN.

5. Registro do MN na HN

O registro do MN na HN ocorre apenas quando o MN retorna para sua HN. O objetivo é cancelar o registro do CoA previamente registrado. Isso também é feito através da troca das mensagens Registration Request e Registration Reply entre o MN e o HA na HN.

O esquema de operação do MIPv4 permite uma interoperação transparente entre o MN e seus CNs, mas obriga que todos os datagramas destinados ao MN sejam roteados através do seu HA (*triangle routing*). Dessa forma, os datagramas destinados ao MN acabam por vezes sendo roteados ao longo de caminhos significamente mais longos do que o ótimo, em termos de números de enlaces entre o HA e o CoA. Por exemplo, mesmo que o MN esteja visitando a rede onde o CN se encontra, os datagramas do CN para o MN devem ser roteados através do HA do MN, para então serem tunelados para a rede visitada para a entrega final. Esse roteamento indireto atrasa a entrega dos datagramas ao MN e onera as redes e roteadores com um peso desnecessário ao longo do caminho.

Para melhorar a operação do MIPv4, algumas definições de extensões para sua operação foram especificadas em [2]. O objetivo é permitir um melhor roteamento de modo que os datagramas possam ser roteados do CN para o MN sem irem primeiro ao HA. Essas extensões são conhecidas como *Route Optmization Extensions*.

2.3 Otimização de Roteamento para o MIPv4

Conforme especificado em [2], as extensões de otimização de roteamento oferecem meios para que os nós façam cache do *binding* do MN (*mobility binding* – informações de mobilidade associadas ao MN, como HA e CoA) para então tunelar seus próprios datagramas diretamente para o CoA indicado pelo binding, desviando-se o tráfego do HA para o MN. Essas extensões também possibilitam que datagramas em trânsito quando um MN se move e datagramas enviados com base em um binding fora da validade sejam encaminhados diretamente para o MN em seu novo CoA.

A otimização de roteamento é dividida em duas partes: (i) atualização das caches de binding e (ii) gerenciamento do *smooth handoff* entre FAs.

Com relação às caches de binding, cada um dos nós possui meios para manter uma cache de binding contendo o CoA de um ou mais MNs. Quando do envio de um datagrama para um MN, se houver uma entrada na cache de binding para o MN destino, pode-se tunelar o datagrama diretamente para o CoA indicado na cache de binding. Na ausência de uma entrada, os datagramas destinados ao MN devem ser roteados para a HN do MN da forma tradicional de roteamento IP, para então serem tunelados pelo HA para o CoA do MN. Essas entradas possuem um tempo de validade associado que é especificado na mensagem de *Binding Update* recebida pelo nó para atualização da cache de binding. Após a expiração da validade, o binding é apagado da cache. A Figura 6 ilustra a otimização do roteamento do MIPv4 quando o CN possui binding para o MN.

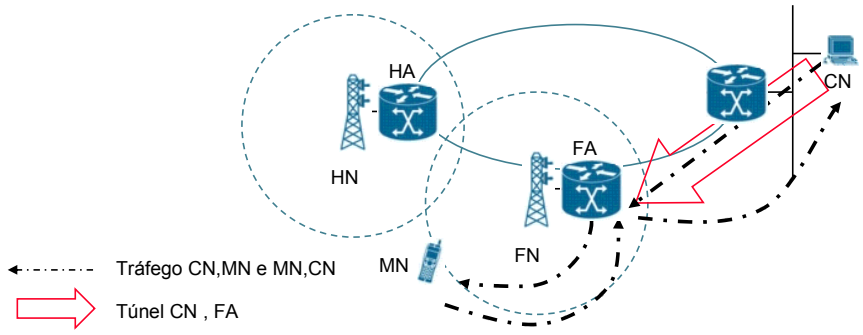

Figura 6 – Otimização do roteamento do MIPv4 quando o CN possui binding para o MN

Quando o HA de um MN intercepta um datagrama de um CN destinado a um MN para ser tunelado, o HA pode deduzir que o CN não possui uma entrada em sua cache de binding para o MN. Nessa situação, o HA deve enviar uma mensagem de Binding Update para o CN informando sobre o mobility binding corrente do MN. Não há necessidade de confirmação de recepção da mensagem Binding Update tendo em vista que futuros datagramas adicionais interceptados pelo HA vão provocar a transmissão de outra mensagem de Binding Update. No entanto, opcionalmente, o HA pode marcar a flag de confirmação de recebimento na mensagem Binding Update fazendo com que o CN envie a mensagem de *Binding Acknowledgment*. A Figura 7 ilustra a atualização da cache de binding de um CN.

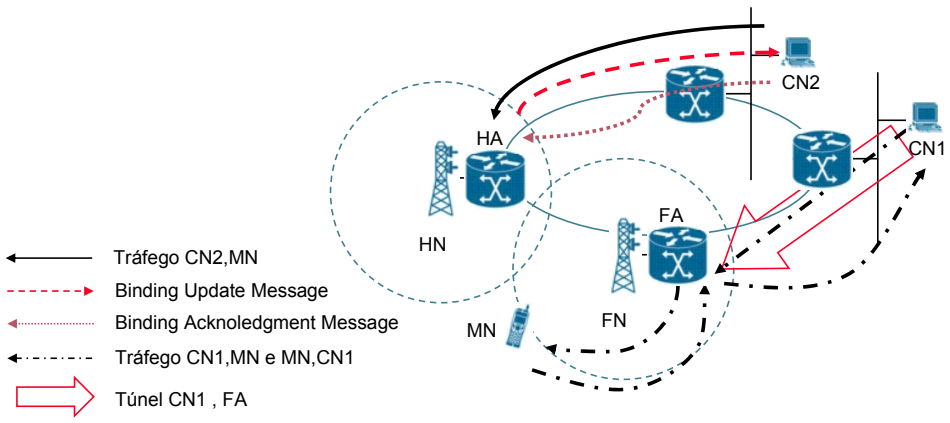

Figura 7 – Atualização da cache de binding de um CN.

De modo semelhante, quando qualquer nó (por exemplo, um FA) receber um datagrama tunelado, se houver uma entrada na cache de binding para o MN destino (e, por essa razão, não há entrada na lista de visitantes para o MN), o mesmo pode deduzir que o nó que tunelou o datagrama possui uma entrada na cache de binding fora da validade para o MN. Nesse caso, o nó que recebeu o datagrama tunelado deve enviar uma mensagem de *Binding Warning* para o HA do MN aletertando sobre a necessidade de se enviar uma mensagem de Binding Update para o nó que tunelou o datagrama. A comunicação com o HA do MN é possível pois essa informação se encontra na entrada da cache de binding associada ao MN, que foi aprendida da mensagem de Binding Update que provocou a criação da própria entrada. Já, o endereço do nó que tunelou o datagrama pode ser determinado do datagrama encapsulado no túnel. Também não há necessidade de confirmação de recepção da mensagem Binding Warning tendo em vista que futuros datagramas adicionais tunelados para o MN vão provocar a transmissão de outra mensagem de Binding Warning. A Figura 8 ilustra o envio da mensagem de alerta do FA para o HA de um MN.

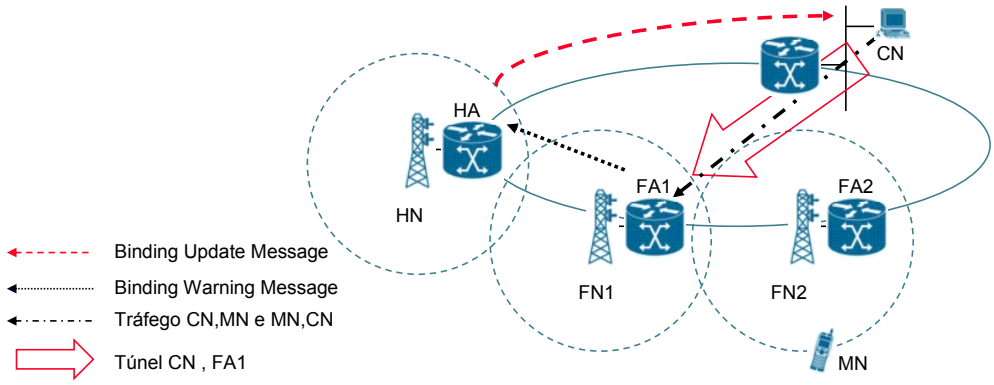

Figura 8 – Envio da mensagem de alerta do FA para o HA de um MN.

Para o gerenciamento do smooth handoff entre FAs, são oferecidos recursos para que o antigo FA do MN seja notificado de forma confiável sobre o novo mobility binding do MN, permitindo que os datagramas em trânsito para o antigo FA do MN sejam encaminhados para o novo CoA do MN. Essa notificação também permite que quaisquer datagramas tunelados para o antigo FA, a partir de um CN com uma entrada desatualizada na cache de binding para o MN, sejam encaminhados para o novo CoA do MN. Por fim, essa notificação também permite que quaisquer recursos consumidos pelo MN no antigo FA (ex: reservas de canal de rádio) sejam liberados imediatamente, ao invés de se aguardar pela expiração da validade do registro do MN.

Como parte do procedimento de registro, o MN pode solicitar ao seu novo FA que tente notificar seu antigo FA em seu nome, adicionando a extensão *Previous Forein Agent Notification* na mensagem de Registration Request enviada para o novo FA. Como conseqüência, o novo FA envia uma mensagem de Binding Update para o antigo FA como parte do procedimento de registro, requerendo a confirmação de recebimento do antigo FA. Essa notificação enviada para o antigo FA contém o novo CoA do MN, o que possibilita a atualização das informações de mobilidade do MN na cache de binding do antigo FA, permitindo que mesmo passe a funcionar como um ponto de encaminhamento para a nova localização do MN. Todos os datagramas tunelados para o MN que cheguem ao antigo FA após a criação do ponteiro de encaminhamento, podem

então ser re-tunelados para o novo CoA do MN. A Figura 9 ilustra o cenário após o procedimento de registro do MN no novo FA.

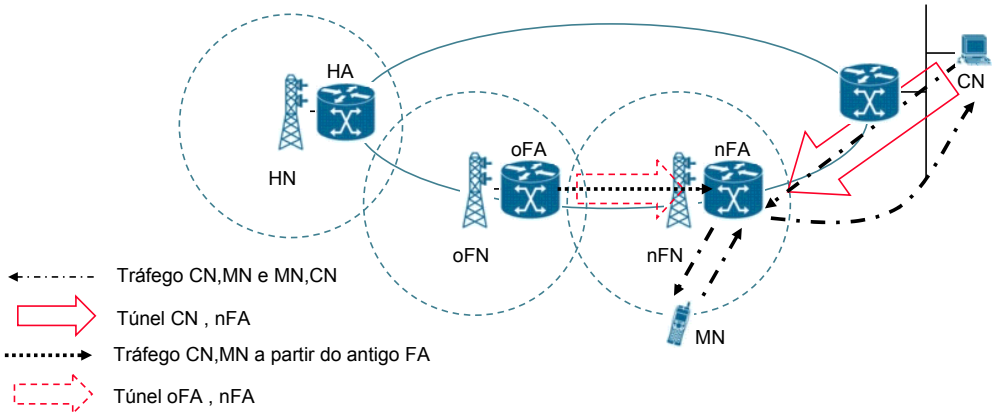

Figura 9 – Cenário após o procedimento de registro do MN no novo FA.

Por questões de compatibilidade, os FAs que suportam smooth handoff devem marcar a nova flag incluída na extensão *Mobility Agent Advertisement* da mensagem de *Agent Advertisement* para indicar esse suporte. Ocasionalmente, o MN é responsável pela retransmissão de uma mensagem de Binding Update para o antigo FA até que a respectiva mensagem de Binding Ackkowledgment seja recebida ou até que o MN tenha certeza que o antigo FA expirou seu binding.

Os resultados obtidos em [3] para a simulação do MIPv4 com e sem otimização de roteamento, mostram que quando o MN se move para uma FN com otimização, o valor mínimo do atraso dos datagramas fim-a-fim é bem menor que sem a otimização, assim como a média do atraso dos datagramas fim-a-fim se mantém no mesmo nível de quando o MN se encontra em sua HN, o que ilustra a eficiência das extensões de otimização.

2.4 Handoff no MIPv4

Conforme definido em [1], o FA deve continuamente enviar mensagens de Agent Advertisement para que os MNs já registrados nele saibam que não se moveram para fora do limite de cobertura do FA e que o mesmo não se encontra em falha. Sendo assim, o handoff no MIPv4 é tipicamente determinado quando o MN recebe uma nova mensagem de Agent Advertisement oriunda de um novo FA.

Quando em uma nova FN, o MN executa o procedimento padrão para registro do novo CoA no seu HA. Conforme já apresentado, o registro é feito através da troca das mensagens Registration Request e Registration Reply, via FA ou diretamente, dependendo do CoA obtido. Quando o registro é completado, o HA cancela o túnel estabelecido com o antigo CoA, para, em seguida, estabelecer o novo túnel com o novo CoA. Após esse processo, o HA passa a encaminhar os datagramas destinados ao MN via o novo túnel.

Embora o handoff ocorra de forma a manter a comunicação entre o MN e os CNs, esse processo não atende as características das aplicações de tempo real e sensíveis a atrasos devido à latência do mesmo, conforme descrito em [4]:

1. A latência na detecção do movimento ocorre devido à necessidade de se detectar o movimento de forma confiável para a nova rede (sem o efeito ping-pong). Isso ocorre em função da freqüência das mensagens de anúncio dos roteadores, assim como do alcance dos mesmos;
2. A latência na obtenção do CoA depende o tipo de CoA obtido. Se o modo co-located CoA for utilizado em conjunto com DHCP, a latência será alta e inaceitável;
3. A latência do procedimento de registro ocorre devido à necessidade de troca de mensagens de sinalização com componetes externos à nova rede.
4. Os atrasos associados às operações da camada de enlace são específicos da tecnologia utilizada e contribuem para o desempenho do handoff. Por exemplo, no IEEE 802.11, a operação do handoff tipicamente envolve varredura dos pontos de acesso em todos os canais disponíveis, seleção do ponto de acesso adequado e associação com o mesmo, podendo ainda envolver operações de controle de acesso tal como especificado no IEEE 802.1X [5].

Outro fator que compromete algumas aplicações durante o handoff é a perda de datagramas. No MIPv4, o MN permanece sem recepção de datagramas até que o procedimento de registro seja completado e o túnel entre o HA e o novo CoA seja estabelecido para encaminhamento dos datagramas. Assim sendo, durante o tempo do processo descrito, ocorre a *perda completa* dos datagramas em trânsito pelo túnel estabelecido entre o HA e o antigo CoA;

Mesmo com a utilização do smooth handoff, conforme especificado nas extensões de otimização do MIPv4, o MN permanece sem recepção de datagramas até que a notificação do Binding Update seja enviada para o antigo FA e o túnel entre o antigo FA e o novo CoA seja estabelecido para o encaminhamento dos datagramas. Assim sendo, durante o tempo do processo descrito, ocorre uma *perda parcial* dos datagramas em trânsito pelo túnel estabelecido entre o CN e o antigo FA.

Com o advento do IPv6, seu suporte à mobilidade foi especificado com base na especificação do MIPv4, utilizando as características peculiares do IPv6. Por essa razão, o MIPv6 (Mobile IPv6) apresenta os mesmos problemas que foram apontados para o handoff no MIPv4 e, normalmente, as soluções podem ser adaptadas entre ambos. Assim, as propostas apresentadas neste trabalho para otimização do handoff serão focadas no MIPv6.

3 Mobilidade no IPv6

Esse capítulo faz uma abordagem básica do suporte à mobilidade IP no IPv6, conforme especificado em [6]. Os objetivos são: (i) apresentar as vantagens do MIPv6 (Mobile IPv6) em relação ao MIPv4; (ii) apresentar as entidades funcionais do MIPv6; (iii) apresentar as operações de suporte à mobilidade; e (iv) identificar os problemas que afetam a comunicação durante o handoff.

3.1 Vantagens do MIPv6 em relação ao MIPv4

Conforme apresentado em [6], o suporte à mobilidade IP no IPv6 (Mobile IPv6) se beneficia das experiências obtidas no desenvolvimento do MIPv4 (Mobile IPv4) e das facilidades providas pelo IPv6. Por essa razão, o Mobile IPv6 compartilha muitas características operacionais do Mobile IPv4, no entanto, é integrado ao IPv6 e oferece muitos

outros aprimoramentos. Algumas das principais diferenças entre o MIPv4 e o MIPv6 são listadas a seguir:

- Não existe necessidade de configurar roteadores especiais como foreign agents (FAs) como no MIPv4. O MIPv6 opera em qualquer localidade sem qualquer requisito de suporte especial do roteador local;
- O suporte à otimização de roteamento é uma parte fundamental do protocolo, ao invés de um conjunto de extensões não padronizadas;
- A otimização de roteamento do MIPv6 pode operar seguramente mesmo sem associações de segurança pré-definidas, podendo ser implantada em escala global entre todos os mobile nodes (MNs) e correspondent nodes (CNs);
- Existe suporte integrado no MIPv6 para prmitir a coexistência eficiente da otimização de roteamento com roteadores que fazem filtragem de ingresso;
- Muitos dos pacotes enviados para o MN quando o mesmo se encontra em uma rede estrangeira no MIPv6 são enviados com a utilização de um cabeçalho de roteamento do IPv6 ao invés de encapsulamento IP, reduzindo a quantidade do custo envolvido comparado com o MIPv4;
- O MIPv6 está desassociado de qualquer camada de enlace particular pois utiliza o IPv6 Neighbor Discovery [11] ao invés do ARP;
- A utilização do encapsulamento IPv6 (e do cabeçalho de roteamento) elimina a necessidade do MIPv6 gerenciar o *soft-state* dos túneis;
- O mecanismo de descoberta dinâmica do endereço do home agent (HA) no MIPv6 retorna uma única resposta ao MN. A abordagem de difusão direcionada utilizada no IPv4 retorna respostas separadas para cada HA. Essa abordagem é proposta para o MIPv4 em [14].

3.2 Entidades Funcionais do MIPv6

O Mobile IPv6 é formado pelas mesmas entidades funcionais definidas no MIPv4, com exceção do FA. Conforme [6], qualquer roteador IPv6 de um enlace estrangeiro (*foreign link*) pode funcionar como o roteador default do MN em uma localidade estrangeira. Esse roteador é responsável por prover o prefixo da rede estrangeira (*foreign subnet prefix*) e o *care-of address* (CoA) para o MN. Não existe qualquer requisito de configuração especial para o roteador, tendo em vista que o CoA é meramente um endereço unicast roteável associado ao MN durante sua visita no enlace estrangeiro, cujo prefixo de subrede desse endereço IP é um prefixo da subrede estrangeira (equivalente ao co-located care-of address do MIPv4). Em particular, o CoA registrado no HA do MN e associado ao seu *home address* é chamado de *primary care-of address*.

3.3 Operação do MIPv6

A operação do MIPv6 é bastante semelhante à operação do MIPv4 com a primeira parte da extensão de otimização de roteamento [2], que permite a atualização das caches de binding presentes no HA e nos CNs. Assim como no MIPv4, a especificação do MIPv6 também é compatível com entidades que não suportam mobility binding. Para isso, o MN sempre pode ser endereçado através do seu *home address*, independente de estar em seu enlace home ou longe dele. O home address é um endereço IP associado ao MN com o prefixo da subrede home no enlace home.

Quando o MN está em algum enlace estrangeiro longe de seu home, também pode ser endereçado através do seu care-of address (CoA). O CoA é um endereço IP associado ao MN com o prefixo de subrede de um enlace estrangeiro particular. O MN pode obter seu CoA através de mecanismos IPv6 convencionais, ou seja, através de autoconfiguração com estado (ex: DHCPv6 [15]) ou sem estado [12]. Enquanto estiver nessa localização, os pacotes endereçados ao seu CoA serão roteados para o MN.

O processo de registro do CoA no HA também é feito de forma semelhante ao MIPv4. Porém, a mensagem de registro enviada pelo MN para o HA é a mensagem de *Binding Update*, enquanto que a mensagem de confirmação do registro enviada pelo HA para o MN é a mensagem de *Binding Acknowledgement*.

Existem dois modos possíveis para comunicação entre o MN e o CN: (i) tunelamento bidirecional (*bidirecional tunneling*) e (ii) otimização de roteamento (*route optimization*). A Figura 10 ilustra os dois modos de comunicação do MIPv6.

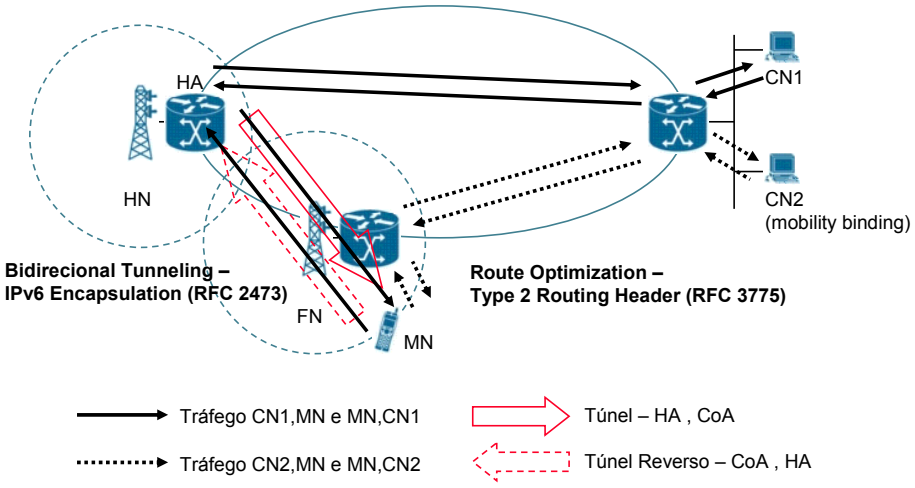

Figura 10 – Modos de comunicação do MIPv6

O *tunelamento bidirecional* não requer o suporte à MIPv6 no CN e está disponível mesmo se o MN não fizer o registro do seu binding atual no CN. Os pacotes do CN são roteados para o HA e então tunelados para o MN. Os pacotes para o CN são tunelados do MN para o HA através de *tunelamento reverso* e então roteados normalmente da home network para o CN. Nesse modo, o HA utiliza o esquema de *proxy Neighbor Discovery* para interceptar qualquer pacote IPv6 endereçado ao home address do MN no enlace home. Cada pacote interceptado é tunelado para o primary CoA do MN. O tunelamento é feito com encapsulamento IPv6 [13].

A *otimização de rotamento* requer que o MN registre seu binding atual no CN. Para isso, é necessário que o CN suporte mobility binding e que o MN execute o procedimento de *registro no correspondente*. Como parte desse procedimento, o teste chamado *return routability*, que é descrito em [6], deve ser executado para autorizar o estabelecimento do binding. Esse teste fornece ao MN as informações de segurança necessárias para construir a mensagem de *Binding Update* que deve ser enviada para o CN atualizar o binding do MN.

No modo de otimização de roteamento, os pacotes do CN podem ser roteados diretamente para o CoA do MN. Quando pacotes são enviados para qualquer destino IPv6, o CN busca uma entrada em sua cache de bindings para o endereço de destino do pa-

cote. Se for encontrada uma entrada, o nó utiliza um novo tipo de cabeçalho de roteamento IPv6, chamado *Type 2 Routing Header* [6], para rotear o pacote para o MN através do CoA indicado no binding. Para o correto roteamento, o CN preenche o endereço de destino no cabeçalho IPv6 com o CoA do MN e o novo tipo de cabeçalho com o home address do MN. Esse roteamento encurta o caminho de comunicação a ser utilizado e também elimina congestionamento no HA do MN e no enlace home. Ainda como conseqüência, o impacto de possíveis falhas associadas ao HA ou às redes no caminho entre o MN e o HA é reduzido.

De forma semelhante, os pacotes do MN podem ser roteados diretamente para os CNs. Para isso, o MN preenche o endereço de origem do cabeçalho IPv6 do pacote com seu CoA e o endereço de destino com o endereço do CN. Em seguida, o MN adiciona uma nova opção, chamada *IPv6 Home Address Destination* [6], para carregar seu home address. A inclusão do home address nesses pacotes torna o uso do CoA transparente para as camadas de rede superiores (ex: na camada de transporte).

O MIPv6 também oferece suporte à multiplos HAs, e um limitado suporte para reconfiguração da HN. Nesses casos, o MN pode não saber o endereço IP de seu próprio HA, e até mesmo os prefixos das subredes home podem mudar ao longo do tempo. Um mecanismo conhecido como *dynamic home agent address discovery* permite que um MN dinamicamente descubra o endereço IP de um HA em seu enlace home, mesmo quando o MN está fora de casa. Os MNs também podem aprender novas informações sobre os prefixos da subrede home através do mecanismo *mobile prefix discovery*.

3.4 Handoff no MIPv6

A especificação do MIPv6 [6] considera que o objetivo primário da detecção de movimento é detectar handoffs da camada 3 (*L3 handovers*), descrevendo um método genérico que utiliza as facilidades do *IPv6 Neighbor Discovery* [11], incluindo o *Router Discovery* e o *Neighbor Unreachabillity Detection*.

Essa detecção genérica de movimento utiliza o Neighbor Unreachability Detection para detectar quando o roteador default deixa de ser alcançável de forma bidirecional, momento em que o MN deve descobrir um novo roteador (normalmente em um novo enlace). No entanto, essa detecção ocorre apenas quando o MN tem pacotes para enviar. Sendo assim, na ausência das contínuas mensagens de Router Advertisement ou de indicações da camada de enlace, o L3 handoff pode não ser percebido pelo MN. Por essa razão, recomenda-se que o MN suplemente esse método com alguma outra informação sempre que a mesma estiver disponível (ex: a partir de protocolos das camadas inferiores).

Quando um L3 handoff é percebido, o MN deve executar o procedimento de *Duplicate Address Detection* [12] para seu endereço local de enlace, selecionar um novo roteador com o procedimento de Router Discovery, e então executar o procedimento de Prefix Discovery com o novo roteador para formar o novo CoA. Em seguida, o MN deve registrar o novo CoA primário com o HA para então atualizar suas informações de mobilidade (mobility bindings) nos CNs com os quais o mesmo opera no modo de otimização de roteamento.

Conforme a especificação do MIPv6 [6], as informações recebidas através das mensagens de Router Advertisement podem ser utilizadas para detectar L3 handoffs. Para isso, os seguintes pontos devem ser considerados:

- Podem existir múltiplos rotadores no mesmo enlace, por isso, mensagens recebidas de um novo roteador não necessariamente constituem um L3 handoff;

- Múltiplos roteadores no mesmo enlace podem anunciar diferentes prefixos, logo, mensagens recebidas de um novo roteador com um novo prefixo podem não ser uma indicação confiável de um L3 handoff;
- Os endereços locais de enlace dos roteadores não são globalmente únicos, assim, após completar um L3 handoff, o MN pode continuar recebendo mensagens de Router Advertisement com o mesmo endereço local de enlace como origem.

Outros eventos também podem ser considerados como indicações de que um L3 handoff possivelmente ocorreu. Diante dessas indicações, o procedimento de Router Discovery deve ser executado para se descobrir roteadores e prefixos no novo enlace, conforme descrito em [11].

- Se uma mensagem de Router Advertisement informa o valor de tempo definido para o *Advertisement Interval*, o MN pode utilizar esse valor como uma indicação da freqüência com a qual futuros anúncios do roteador devem ser recebidos. Se esse tempo for extrapolado sem a recepção de um novo anúncio, o MN pode assegurar que pelo menos um anúncio foi perdido. Assim, com base em uma política própria, o MN pode determinar quantos anúncios perdidos oriundos de seu roteador default constituem uma indicação de L3 handoff.
- Como um L2 handoff não necessariamente implica em um L3 handoff, à menos que se tenha certeza da implicação, ao invés de imediatamente difundir uma solicitação por roteador, é melhor tentar verificar se o roteador default ainda se encontra com alcance bidirecional. Para isso, deve-se enviar uma mensagem unicast de Neighbor Solicitation e aguardar pela mensagem de Neighbor Advertisement com a flag de solicitação marcada. Se não houver resposta do roteador default, deve-se proceder com a difusão na mensagem de Router Solicitation.

Assim como no MIPv4, embora o handoff ocorra de forma a manter a comunicação entre o MN e os CNs, esse processo não atende as características das aplicações de tempo real e sensíveis a atrasos pelas mesmas razões já expostas para o MIPv4, ou seja, sua grande latência, conforme resumido abaixo:

1. Latência na detecção do movimento;
2. Latência na detecção do roteador default e obtenção do CoA;
3. Latência no procedimento de registro do CoA no HA;
4. Atrasos associados às operações da camada de enlace durante o handoff.

A perda de datagramas durante o handoff também ocorre de forma semelhante ao MIPv4. No modo de operação de tunelamento bidirecional, o MN permanece sem recepção de datagramas até que o procedimento de registro seja completado e o túnel bidirecional entre o HA e o novo CoA seja estabelecido para encaminhamento dos datagramas. Assim sendo, durante o tempo do processo descrito, ocorre a *perda completa* dos datagramas em trânsito pelo túnel bidirecional estabelecido entre o HA e o antigo CoA.

Mesmo com a utilização do modo de operação de otimização de roteamento, o MN permanece sem recepção de datagramas até que a notificação do Binding Update seja enviada para todos os CNs. Assim sendo, até a atualização do mobility binding associado ao MN nos CNs, ocorre *perda completa* dos datagramas enviados pelos CNs desatualizados com o antigo CoA.

Diante dos problemas expostos, a comunidade científica vem buscando aprimorar o suporte à mobilidade no IP através de propostas de otimização que venham a reduzir a

perda de datagramas e a latência do handoff, minimizando o tempo sem recepção de datagramas, com o objetivo de oferecer um handoff transparente (*seamless handoff*).

As seções a seguir apresentam as principais propostas de otimização do handoff com enfoque nas que foram publicadas como RFCs e Drafts, abordando ainda, os resultados de estudos que demonstram o ganho efetivo dessas otimizações.

4 Otimizações para o Handoff no MIPv6

Este capítulo apresenta algumas das principais otimizações propostas para o MIPv6. O principal objetivo dessas propostas é minimizar a latência do handoff e reduzir o atraso e a perda de datagramas durante essa operação. De modo geral, as propostas visam soluções para: (i) minimizar o tempo de registro do CoA; (ii) minimizar o tempo de mudança do ponto de acesso; e (iii) evitar o atraso e a perda dos datagramas.

4.1 Hierarchical Mobile IPv6 Mobility Management (HMIPv6)

Conforme apontado anteriormente, um dos problemas que afetam a comunicação no MIPv6 é a latência referente à efetivação do registro do novo CoA. Essa operação é lenta pois envolve a troca de mensagens de sinalização com componentes fora da nova rede, em particular, com o HA e com os CNs que suportam otimização de roteamento.

Para minimizar essa latência, o esquema de handoff hierárquico divide a mobilidade em duas categorias: (i) *micromobilidade* (geralmente intra-domínio) e (ii) *macromobilidade* (geralmente inter-domínio). O elemento central desse esquema é a entidade conceitual chamada de *Mobility Anchor Point* (MAP) [7], que define um domínio MAP formado por uma ou mais redes. A movimentação de um MN entre redes de um mesmo domínio MAP determina uma micromobilidade, e a movimentação do MN entre redes de domínios MAP diferentes determina uma macromobilidade.

Cada uma das redes de um domínio MAP possui um Access Router (AR) que corresponde ao roteador default dos MNs em sua região de alcance. A presença do MAP do domínio ao qual o AR pertence, é anunciada na mensagem de Router Advertisement. Assim, a mudança de um domínio MAP é percebida pelo MN quando um novo anúncio com a informação de um novo MAP é recebida pelo MN.

Conforme especificado em [7], quando em um novo domínio MAP, o MN faz o binding do seu CoA obtido na rede local, conhecido como *Local CoA* (LCoA), com um endereço na subrede do MAP, conhecido como *Regional CoA* (RCoA) e que, normalmente, é o endereço do próprio MAP. Agindo como um local HA, o MAP intercepta todos os pacotes destinados ao MN e os encapsula e encaminha diretamente para o LCoA. Se o MN mudar para outra rede do mesmo domínio MAP, apenas o registro do novo LCoA é feito junto ao MAP com uma mensagem de Binding Update. E então, apenas o RCoA precisa ser registrado, através de outra mensagem de Binding Update, no HA e nos CNs com os quais o MN se comunica. Esse RCoA não se modifica se a movimentação do MN for ao longo de um mesmo domínio MAP. Isso torna a micromobilidade do MN transparente com relação ao HA e aos CNs. A Figura 11 ilustra o esquema do MIPv6 hierárquico.

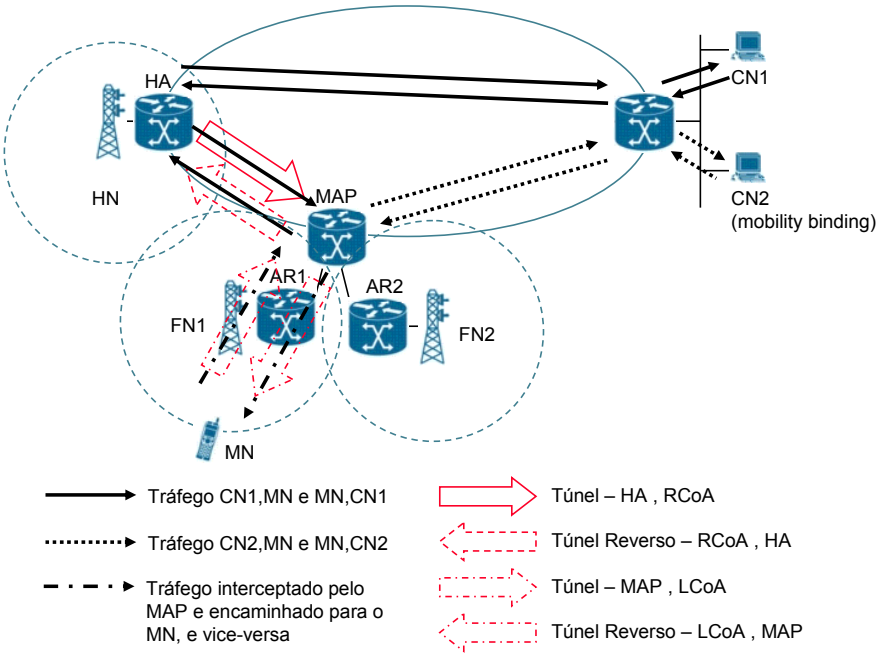

Figura 11 – Esquema do MIPv6 hierárquico

Com o objetivo de acelerar o handoff entre MAPs e reduzir a perda de pacotes, o MN deve enviar uma mensagem de Binding Update para seu MAP anterior, especificando seu novo LCoA. Os pacotes que estiverem em trânsito para o MAP anterior serão então encaminhados para o novo LCoA. Também é permitido que MNs enviem mensagens de Binding Updates contendo o LCoA (ao invés do RCoA) para CNs que estão presentes na mesma rede visitada. Dessa forma, os pacotes serão roteados diretamente sem atravessarem o MAP.

O esquema de handoff hierárquico descrito também foi definido para o MIPv4, conforme a especificação apresentada em [8].

4.2 Fast Handovers for Mobile IPv6 (FMIPv6)

Conforme descrito em [9], a habilidade de imediatamente enviar pacotes a partir de um novo enlace de subrede depende da latência da conectividade IP, que por sua vez, depende da latência da detecção de movimento e da latência de configuração do novo CoA. Uma vez restaurada a capacidade IP do MN, a mensagem de Binding Update pode ser enviada ao seu HA e a todos os seus CNs. A partir do processamento bem sucedido do Binding Update pelos seus CNs, o que tipicamente envolve a execução do procedimento de return routability [6], o MN pode receber pacotes no novo CoA. Sendo assim, a habilidade de receber pacotes a partir de CNs diretamente para seu novo CoA depende da latência do Binding Update e da latência da conectividade IP.

O protocolo definido em [9] possibilita que o MN rapidamente detecte sua movimentação para uma nova rede pois provê informação sobre o novo ponto de acesso (Access Point – AP) e sobre o prefixo de subrede associado enquanto o MN ainda se encontra conectado à sua subrede atual, cujo roteador default passa a ser chamado de *roteador de acesso anterior* (Previous Access Router – PAR). Por exemplo, um MN pode descobrir os APs disponíveis utilizando mecanismos do nível de enlace (ex: operação *scan* na WLAN) e então requisitar informações da subrede correspondente a um ou

mais dos APs descobertos. Essa requisição é feita com o envio da mensagem de *Router Solicitation for Proxy Advertisement* (RtSolPr) para o seu roteador de acesso. O MN pode executar essa operação depois do procedimento de router discovery ou a qualquer momento quando se encontrar conectado ao seu rotedor corrente.

O resultado da resolução do identificador associado a um AP é a tupla [AP-ID, AR-Info], onde AP-ID é o identificador do AP e AR-Info é composto pelo endereço L2 do roteador, endereço IP do roteador e um prefixo válido na subrede a qual o AP está conectado. Essa resposta é enviada pelo AR para o MN na mensagem de *Proxy Router Advertisement* (PrRtAdv).

Com as informações obtidas, o MN formula um novo CoA (NCoA) em potencial e envia uma mensagem de *Fast Binding Update* (FBU) quando ocorre um evento de handoff específico de enlace. Essa mensagem tem o propósito de autorizar o PAR a fazer o binding do PCoA (Previous CoA) para o NCoA., de modo que os pacotes que cheguarem possam ser tunelados para a nova localização do MN. Sempre que possível, o FBU deve ser enviado a partir do enlace do PAR. Quando não for, o FBU é enviado a partir do novo enlace. Com a execução desse procedimento, a latência referente à descoberta do novo prefixo subsequente ao handoff é eliminado.

Como confirmação de recebimento do FBU, o PAR deve enviar a mensagem de *Fast Binding Acknowledgment* (FBack). Dependendo se a mensagem FBack é recebida ou não ainda no enlace anterior, dois modos de operação são definidos:

1) O MN recebe a mensagem FBack no enlace anterior. Isso significa que o tunelamento de pacotes já se encontrará em progresso no momento em que o MN fizer o handoff para o NAR. Logo, o MN deve enviar a mensagem de *Fast Neighbor Advertisement* (FNA) imediatamente após se conectar ao NAR, de modo que os pacotes que estejam chegando e os que foram armazenados sejam encaminhados para o MN.

Antes do envio de uma mensagem FBack para um MN, o PAR pode determinar um NCoA aceitável pelo NAR através da troca das mensagens *Handover Initiate* (HI) e *Handover Acknowledge* (HAck). Quando o modo *assigned addressing* é utilizado, o NCoA proposto pelo MN na mensagem FBU é carregado na mensagem HI que é enviada pelo PAR para o NAR, que pode atribuir o NCoA ao MN. Esse NCoA deve então ser retornado na mensagem HAck enviada pelo NAR para o PAR, que por sua vez, deve prover o NCoA atribuído na mensagem FBack. Se existir um NCoA retornado na mensagem FBack, o MN deve utilizá-lo, ao invés do NCoA proposto, quando se conectar ao NAR.

2) O MN não recebe a mensagem FBack no enlace anterior pois o MN não enviou a mensagem FBU ou o MN deixou o enlace após enviar a mensagem FBU (que pode ter sido perdida), mas sem receber a mensagem FBack. Sem ter recebido a mensagem FBack no último caso, o MN não tem como se certificar quanto ao processamento bem sucedido da mensagem FBU enviada para o PAR. Por essa razão, o MN re-envia uma mensagem FBU assim que se conecta ao NAR. Para permitir que o NAR encaminhe os pacotes imediatamente (no caso em que a mensagem FBU foi processada pelo PAR) e verifique se o NCoA é aceitável, o MN deve encapsular a mensagem FBU na mensagem FNA. Se for detectado que o NCoA está em uso quando a mensagem FNA for processada, o NAR deve descartar o pacote interno com a mensagem FBU e enviar uma mensagem de Router Advertisement com a opção Neighbor Advertisement Acknowledge (NAACK) na qual o NAR pode incluir um endereço IP alternativo para o MN utilizar.

O cenário no qual o MN envia uma mensagem FBU e recebe uma mensagem FBack no enlace do PAR é caracterizado como *operação em modo pré-indicado ou antecipado* (*predictive*), e é ilustrado na Figura 12.

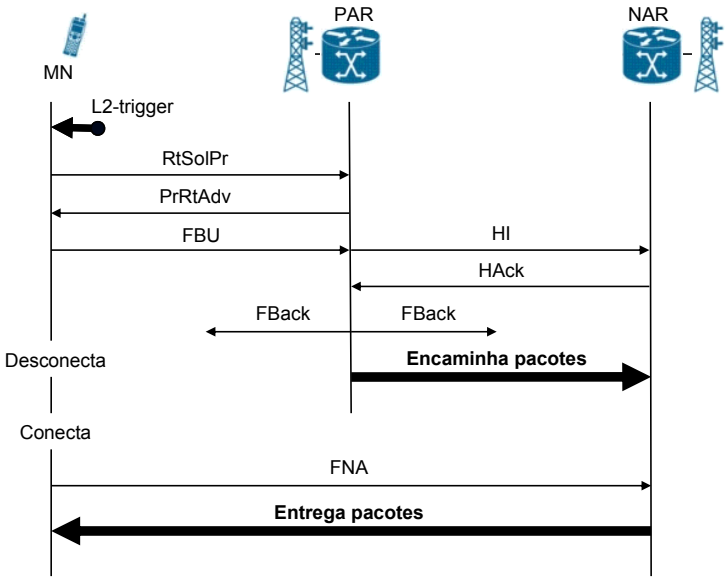

Figura 12 – Fast Handover: operação em modo pré-indicado ou antecipado

O cenário no qual o MN envia a mensagem FBU a partir do enlace do NAR é caracterizado como *operação em modo reativo*, e é ilustrado na Figura 13. Esse modo também atende o caso no qual a mensagem FBU é enviada a partir do enlace do PAR, mas uma mensagem FBack ainda não foi recebida.

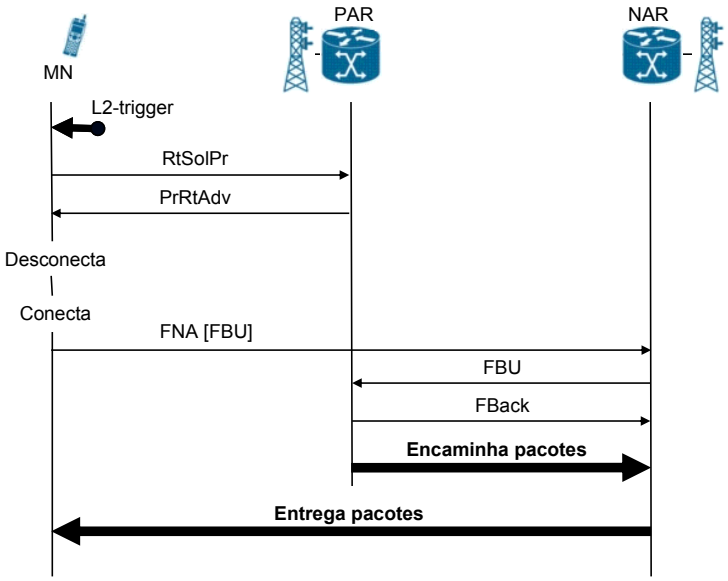

Figura 13 – Fast Handover: operação em modo reativo

Por fim, a mensagem PrRtAdv pode ser enviada de forma não solicitada, ou seja, sem o envio anterior da mensagem RtSolPr. Essa operação possibilita que o MN se

mantenha informado sobre redes geograficamente adjacentes, reduzindo, assim, a quantidade de tráfego necessária para obter o mapa de topologia da vizinhança de enlaces e subredes.

Já, as mensagens HI e HAck podem ainda ser utilizadas para transferência de informações referentes ao contexto de rede, como controle de acesso, QoS e compressão de cabeçalho, em conjunto com o handoff.

4.3 Enhanced Route Optimization for Mobile IPv6

A otimização de roteamento prevista no MIPv6 possibilita que o MN e o CN se comuniquem através de um caminho direto independente das mudanças que ocorrem na conectividade IP no lado do MN. Conforme descrito na seção 3.3 , esse suporte envolve a utilização do Type 2 Routing Header no pacote que percorre o sentido CN-MN, e a utilização da opção de cabeçalho IPv6 Home Address Destination no pacote que percorre o sentido MN-CN. Ambos os pacotes carregam informações sobre o atual CoA e o home address do MN. Dessa forma, a mobilidade IP é transparente para as camadas superiores, como a transporte.

Para que o processo de comunicação com otimização de roteamento seja mantido entre o MN e o CN, o MN precisa manter o CN atualizado com seu CoA corrente. Para isso, o MN deve manter sua informação de mobility binding atualizada na cache do CN. Isso é feito através do registro do novo CoA no CN, que implica no envio da mensagem BU após uma mudança de CoA.

Sob perspectiva da segurança, o estabelecimento de um novo binding associado ao MN no CN requer que o CN vefique se o MN tem a propriedade do home address e do CoA em questão. Para isso, o processo de registro no CN incorpora um procedimento que implica em testar o home address e o CoA, conhecido como *return routability* [6]. Esses dois testes permitem ao CN verificar se o MN é alcançável através do home address e do CoA de forma conjunta. A verificação bem sucedida de ambos os endereços indica (embora não garanta) a propriedade que o MN tem desses endereços e, assim sendo, que o binding é legítimo.

O procedimento return routability é formado por 4 mensagens, conforme ilustrado na Figura 14 [6]. As mensagens *Home Test Init* (HoTI) e *Care-of Test Init* (CoTI) são enviadas ao mesmo tempo. Esse procedimento requer muito pouco processamento por parte do CN, o que permite que as mensagens *Home Test* (HoT) e *Care-of Test* (CoT) sejam retornadas rapidamente, possivelmente até simultâneamente.

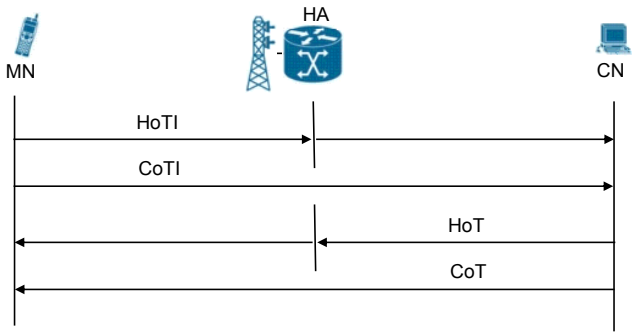

Figura 14 – Procedimento return routability [6]

A mensagem HoTI é enviada ao CN através do HA do MN com o objetivo de informar o home address do MN ao CN. Essa mensagem transporta o parâmetro *home init cookie*, criado pelo MN para controle da troca de mensagens. Ao receber essa mensagem, o CN responde com a mensagem HoT que transporta os parâmetros *home init cookie*, *home keygen token* e *home nonce index*. O primeiro parâmetro é copiado da mensagem HoTI e o segundo é gerado em função do home address, da chave secreta do CN (Kcn – valor aleatório de 20 octetos) e de um *nonce*, indicado pelo terceiro parâmetro.

A mensagem CoTI é enviada pelo MN diretamente para o CN com o objetivo de informar o CoA do MN ao CN. Essa mensagem transporta o parâmetro *care-of init cookie*, criado pelo MN para controle da troca de mensagens. Ao receber essa mensagem, o CN responde com a mensagem CoT que transporta os parâmetros *care-of init cookie*, *care-of keygen token* e *care-of nonce index*. O primeiro parâmetro é copiado da mensagem CoTI e o segundo é gerado em função do CoA informado pelo MN, da chave secreta do CN (Kcn – valor aleatório de 20 octetos) e de um *nonce*, indicado pelo terceiro parâmetro.

Como resultado do procedimento return routability, o MN recebe os dados para gerar a chave de binding (Kbm) de 20 octetos, formada a partir do hash SHA1 da concatenação dos tokens recebidos (ilustrado na Figura 15), necessária para enviar a mensagem BU para o CN.

Kbm = SHA1 (home keygen token | care-of keygen token)

Figura 15 – Chave de binding para registro do CoA do MN no CN [6]

A mensagem BU também pode ser utilizada para remover uma informação de binding do MN da cache do CN. Nesse caso, o care-of keygen token não é utilizado e a chave de binding é gerada pelo hash SHA1 do home keygen token, como ilustrado na Figura 16.

Kbm = SHA1(home keygen token)

Figura 16 - Chave de binding para remoção do registro do CoA do MN no CN [6]

Conforme descrito em [16], a vantagem do procedimento return routability é que o mesmo é leve e não depende de uma infra-estrutura de chaves públicas nem de um relacionamento pré-existente entre o MN e o CN. Isso facilita sua larga implantação. Por outro lado, esse procedimento tem um impacto adverso no atraso do handoff já que ambos os testes consistem em trocas de mensagem fim-a-fim entre o MN e o CN. Particularmente, a latência do teste do home address é alta pois é roteado através do home agent (HA). O procedimento também é vulnerável a atacantes que se encontram em uma posição onde podem intervir no teste do home address ou do CoA. Embora o risco seja limitado, já que o procedimento deve se repitir em intervalos de no máximo 7 minutos, mesmo que não ocorra mudança de conectividade IP, existe claramente um aumento no overhead de sinalização. Conforme apresentado em [18], muitos esforços já foram feitos para aprimorar a otimização de roteamento do MIPv6 visando mitigar essas desvantagens.

O Enhanced Route Optimization [16] é um aprimoramento que visa proteger o home address do MN contra impersonalização com a utilização de um par de chaves pública/privada. A idéia básica é gerar o identificador de interface (ou seja, os 64 bits mais à direta, conforme definido em [20]) do endereço IPv6 que representa o home ad-

dress a partir da computação de um hash criptográfico da chave pública. O endereço IPv6 resultante é então conhecido como um *Cryptographically Generated Address* (CGA) [19]. Esse esquema possibilita ao MN comprovar a propriedade de seu home address criptograficamente sem uma infra-estrutura de chaves pública, permitindo que outros nós autentiquem o dono do CGA de forma segura e autônoma a partir da corretude da assinatura digital das mensagens recebidas. Sendo assim, após um teste inicial do home address, testes subsequentes são desnecessários. Isso viabiliza menores atrasos no handoff e maiores tempos de vida aos bindings, bem como a redução do overhead de sinalização. Opcionalmente, os CNs também podem fazer uso de CGAs para provar a propriedade do endereço IP.

Como a autenticação baseada em CGA envolve criptografia de chave pública, que é computacionalmente bem menos eficiente que autenticação através de chave secreta compartilhada [21], o Enhanced Route Optimization utiliza essa autenticação apenas para fazer a troca segura do *home keygen token permanente* entre um MN e um CN. Esse token é utilizado para autenticar o MN de forma mais eficiente em registros subsequentes feitos no CN, podendo ser renovado a qualquer momento. Isso constitui uma informação que não é constante nem de curto tempo de vida, caracterizando a associação de segurança entre o MN e o CN como *semi-permanente*.

Conforme descrito em [19], os CGAs em si não são certificados, o que possibilita um atacante criar um novo CGA com qualquer prefixo de subrede e com sua própria chave pública, ou com a chave pública de qualquer outro nó. No entanto, o atacante não pode utilizar um CGA criado por alguém para enviar mensagens assinadas que pareçam ter vindo do verdadeiro dono do endereço. Nesse sentido, para evitar que um atacante crie um CGA com o prefixo de subrede de um MN e, então, tente registar esse endereço para um CoA de sua propriedade, um teste inicial do home address é requerido para o estabelecimento de uma associação de segurança semi-permanente entre o MN e o CN. Esse teste deve ser executado de forma pró-ativa para evitar um custo potencialmente expressivo de troca de mensagens através do home agent durante o período crítico do handoff. Após um teste bem sucedido do home address, outros não precisam ser repetidos em movimentos futuros.

Outra característica do Enhanced Route Optimization é permitir que o CN inicie o envio de pacotes para o novo CoA do MN antes do MN provar sua alcançabilidade no novo CoA. Esse esquema é conhecido como *Concurrent Care-of Address Test*. Quando a mudança de connectividade IP ocorre, o MN primeiro atualiza seu binding no CN com seu novo CoA sem fornecer uma prova de alcançabilidade. O CN então registra o novo CoA como *estado não verificado*. Isso permite a troca bidirecional de pacotes via o novo CoA, enquanto a alcançabilidade do MN no CoA é verificada concorrentemente. O CN muda o CoA para *estado verificado* uma vez que a verificação de alcançabilidade seja completada. Para proteger o CN contra possíveis ataques de enchurrada baseada em redirecionamento, conforme descrito em [16], utiliza-se o esquema de *Autorização Baseada em Crédito*. Nesse esquema, a medida e o limite do esforço de um CN para enviar pacotes são realizados através do conceito de *crédito*. Esse crédito é mantido pelo CN e incrementado proporcionalmente quando se envia pacotes para CoAs em estado verificado, e decrementado proporcionalmente quando se envia pacotes para CoAs em estado não verificado. A ausência de crédito impede o envio de pacotes.

Ainda, com respeito à outra otimização que contribui para a redução do atraso do handoff, o Enhanced Route Optimization permite que o MN execute os registros do novo CoA no CN e no seu HA em paralelo, não sendo necessário aguardar pela recepção da mensagem de Binding Acknowledgment que indica um registro bem sucedido no HA antes de iniciar o registro no CN.

Os diagramas apresentados nas figuras Figura 17, Figura 18 e Figura 19 ilustram a operação do Enhanced Route Optimization baseada em algumas poucas trocas de mensagens selecionadas. A Figura 17 ilustra a troca de mensagens para o registro em um CN onde uma mensagem de *early Binding Update* (early BU) é autenticada via comprovação do MN conhecer o home keygen token permanente. A mensagem early BU possui a opção *Care-of Test Init* que requisita ao CN adicionar um novo care-of keygen token na opção *Care-of Test* da mensagem de Binding Acknowledgment. O MN finalmente conclui o registro no CN com um mensagem de Binding Update.

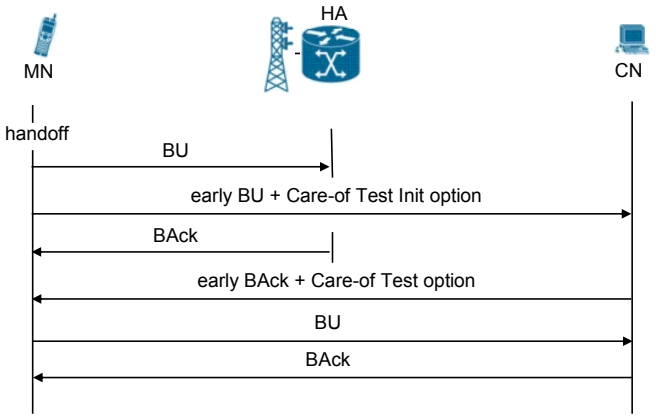

Figura 17 – Registro no CN com autenticação via comprovação do conhecimento do home keygen token permanente; teste simultâneo do CoA

A Figura 18 ilustra o procedimento de registro em um CN onde a mensagem de Binding Update é autenticada com base na verificação de alcançabilidade do home address. O teste do home address é pró-ativamente executado antes do handoff, permitindo ao MN enviar a mensagem BU logo após o handoff. A mensagem BU é novamente uma mensagem early BU, e um care-of keygen token é retornado ao MN na mensagem de Binding Acknowledgment.

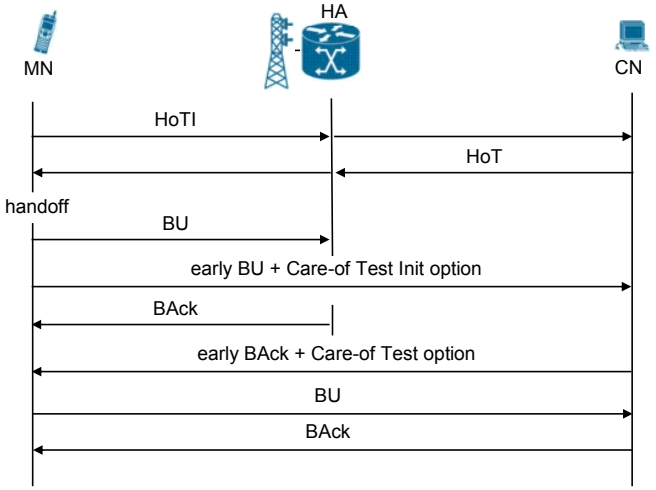

Figura 18 - Registro no CN com autenticação baseada na verificação de alcançabilidade do home address; teste simultâneo do CoA

A Figura 19 ilustra um registro no CN onde o MN inicialmente obtém um novo care-of keygen token através da troca das mensagens Care-of Test Init e Care-of Test. O MN envia em sequência uma mensagem BU completa que é autenticada com a propriedade CGA do home address.

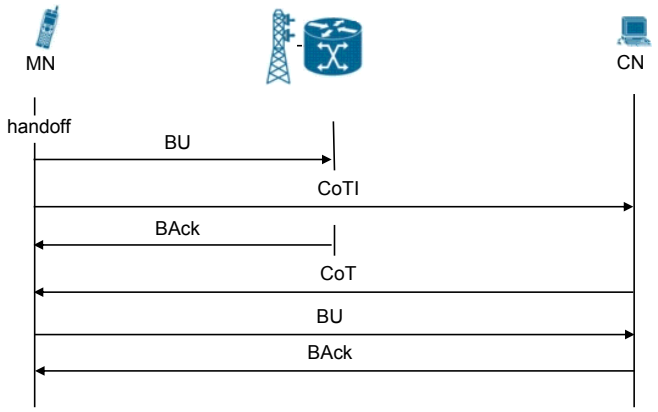

Figura 19 - Registro no CN com autenticação via comprovação do conhecimento do home keygen token permanente; teste explícito do CoA

4.4 Análise Comparativa das Otimizações do Handoff

Os resultados apresentados em [17], demonstram que as otimizações propostas podem realmente minimizar a latência do handoff e a perda dos pacotes com relação ao MIPv6. No entanto, a quantidade de estações competindo pelo enlace wireless pode impactar em um resultado contrário.

Na simulação feita em [17], conforme o gráfico apresentado na Figura 20, pode-se observar que com até 20 MNs presentes no cenário, os resultados são como esperados, tendo em vista que o fator dominante da latência do handoff é o atraso nos enlaces cabeados. O desempenho da latência do HMIPv6 supera o do MIPv6 pois a distância percorrida nos enlaces cabeados para atualização da entidade que encaminhará os pacotes para o MN é sempre menor. Por sua vez, o desempenho do FMIPv6 supera o do HMIPv6 já que o MN prepara o handoff antecipadamente e assim, após o handoff, não tem que aguardar que o PAR seja atualizado para iniciar a recepção de pacotes novamente. No FMIPv6 os pacotes são encaminhados do PAR para o NAR através do enlace cabeado e, dessa forma, apenas esse atraso é observado. O melhor desempenho de todos é observado na composição do HMIPv6 com o FMIPv6 pois quando o MN recebe o FBack do MAP indicando que o handoff deve ser executado, os pacotes redirecionados já o estarão aguardando no NAR.

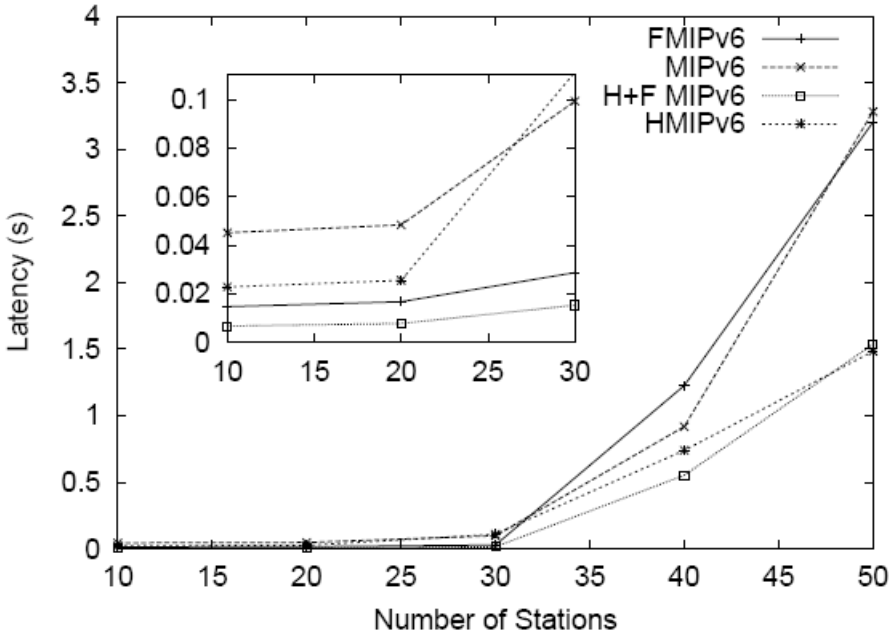

Figura 20 – Impacto do número de estações na latência do handoff [17]

Um caso excepcional pode ser observado para 30 MNs, onde o MIPv6 apresenta um desempenho um pouco melhor que o HMIPv6. Devido ao encapsulamento que o HMIPv6 sempre faz do MAP para o novo LCoA obtido pelo MN, ocorre um aumento de carga no canal e, assim, o HMIPv6 alcança condições de saturação mais cedo, aumentando o atraso wireless que, nessa situação, prevalece sobre o atraso existente no enlace cabeado. Embora o mesmo problema de encapsulamento ocorra na composição do HMIPv6 com o FMIPv6, essa diferença não é observada pois o mecanismo de fast handover do FMIPv6 prepara o handoff antecipadamente.

No entanto, quando o atraso wireless se torna muito alto devido a saturação do canal, como, por exemplo, no caso de 40 a 50 estações, o desempenho do HMIPv6 é melhor quando comparado ao do MIPv6 devido a duas razões. Primeiro, no caso do HMIPv6, a mensagem BU é enviada ao MAP logo após o acoplamento ao novo enlace, o que rapidamente redireciona todo tráfego do CN recebido pelo MAP para o novo LCoA do MN. Por sua vez, no MIPv6, a mensagem BU é primeiramente enviada para o HA antes do envio para o CN, o que introduz um atraso wireless adicional. Segundo, enquanto as mensagens BAcks são obrigatórias para o HA e para o MAP, a mesma é opcional para o CN. Assim, se a mensagem BU para um CN for perdida, o MN apenas a enviará novamente quando um pacote de dados originado pelo CN for encaminhado pelo HA, ao invés de diretamente pelo CN. Sob condições de grande saturação do canal, a probabilidade de perda de uma mensagem BU é alta, e assim, se o MIPv6 é utilizado e uma mensagem BU é perdida, não ocorre retransmissão, o que incrementa significamente a latência. Por outro lado, quando a mensagem BAck do MAP não é recebida pelo MN, a mensagem BU é retransmitida.

Embora o FMIPv6 tenha sido criado para minimizar a perda de pacotes e a latência durante o handoff, pode-se observar na Figura 21 que o seu desempenho é pior se comparado ao do MIPv6 quando a saturação é alcançada. Para entender o ocorrido, é importante observar que nessa situação a carga no canal wireless é alta, resultando em um canal com um longo tempo de acesso e alta taxa de colisão. No FMIPv6, o NAR ini-

cia o envio dos pacotes destinados ao NCoA através do meio wireless tão logo a mensagem F-NA seja enviada pelo MN e recebida pelo NAR, introduzindo uma carga ainda maior no canal wireless sobrecarregado. Esse processo é viabilizado no FMIPv6 pois o NAR aprende o endereço da camada de enlace do MN antes mesmo de ter pacotes para entregar ao mesmo (via recepção da mensagem PrRtSol pelo PAR que dispara o handshake HI-HAck). No caso do MIPv6 e do HMIPv6, faz-se necessário a utilização da resolução de endereço baseada no Neighbor Discovery (ND). Durante o processo de resolução de endereço apenas uma pequena quantidade de pacotes são armazenados para o mesmo endereço destino. Mesmo assim, o descarte de pacotes que ocorre na entrada da fila do ND acaba contribuindo menos para a perda de pacotes global do que a saturação do canal wireless.

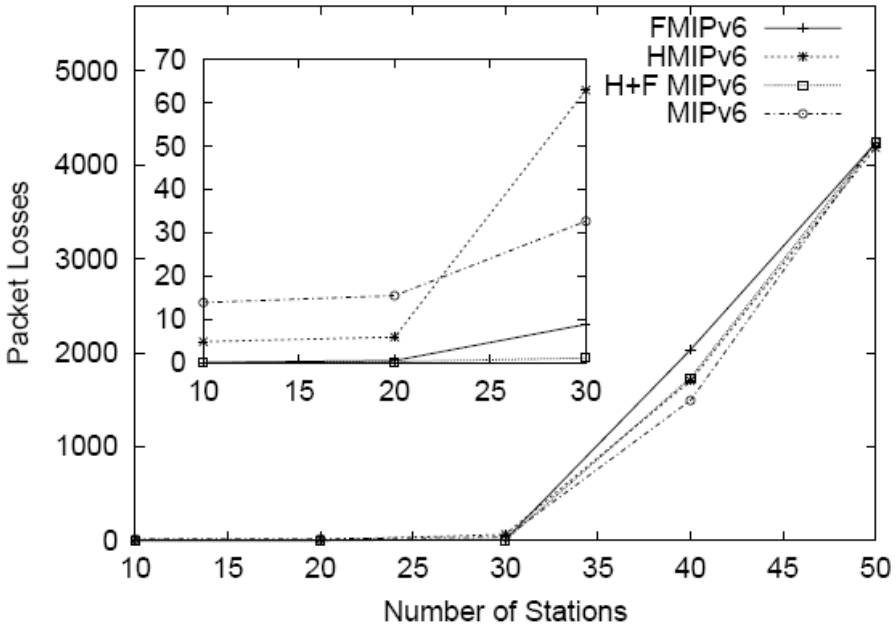

Figura 21 – Impacto do número de estações na perda de pacotes [17]

Embora existam diferenças com respeito à situação de congestionamento de tráfego, pode-se observar que uma vez atingido o nível de saturação por todos os protocolos, se o número de MNs for aumentado, as perdas de pacotes tendem a convergir. Isso ocorre pois para todos os casos o canal wireless se apresenta com uma alta taxa de colisão e um longo tempo de acesso ao canal reduzindo, então, o impacto das diferenças entre as abordagens discutidas.

Considerando a incorporação do Enhanced Route Optimization no MIPv6, no HMIPv6, no FMIPv6 e na composição do HMIPv6 com o FMIPv6, acredita-se que o ganho de otimização será equivalente e proporcional a quantidade de mensagens BUs enviadas aos CNs por todos esses protocolos após um handoff. Isso se deve ao fato da otimização atuar na minimização da execução do procedimento return routability, necessário para o envio confiável das mensagens BUs após um handoff, com o objetivo de atualizar a informação de mobility binding do MN nos CNs.

5 Conclusão

Embora o handoff no MIPv4 e no MIPv6 ocorra de forma a manter a comunicação entre o MN e os CNs, esse processo não atende as características das aplicações de tempo real e sensíveis a atrasos devido à dois principais fatores: (i) grande latência e (ii) perda de pacotes.

Com o objetivo de minimizar esses fatores, algumas propostas de otimização foram publicadas pelo IETF. Todas foram apresentadas e analisadas comparativamente na seção 4.4 com enfoque nos fatores de interesse, ressaltando as principais características de cada otimização. De forma resumida, o HMIPv6 permite minimizar a latência referente à efetivação do registro do novo CoA, e o FMIPv6 permite minimizar a latência do Binding Update e a latência da conectividade IP, podendo ainda ser combinado com o HMIPv6. Para aprimorar a otimização de roteamento, a última proposta apresentada permite reduzir ainda mais a latência do Binding Update, assim como assegurar a propriedade de um home address e um CoA.

A análise comparativa apresentada na seção 4.4 também demonstra que mesmo com as otimizações já publicadas pelo IETF, o MIPv6 ainda carece de soluções escaláveis que possam minimizar a latência e a perda de pacotes no processo de handoff.

Referências

[1] C. Perkins, IP Mobility Support for IPv4, RFC 3344, August 2002.

[2] C. Perkins, David B. Johnson, Route Optimization in Mobile IP (draft-ietf-mobileip-optim-11.txt). Mobile IP Working Group. Internet-Draft.

[3] H. Chen, L. Trajkovíc, Simulation of Route Optimization in Mobile IP.

[4] R. Koodli, C. Perkins, Mobile IPv4 Fast Handovers (draft-ietf-mip4-fmipv4-07.txt). MIP4 Working Group. Internet-Draft. May 17, 2007.

[5] IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control. Technical report, IEEE.

[6] D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6, RFC 3775, June 2004.

[7] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier, Hierarchical Mobile IPv6 Mobility Management (HMIPv6), RFC 4140, August 2005.

[8] E. Fogelstroem, A. Jonsson, C. Perkins, Mobile IPv4 Regional Registration (draft-ietf-mip4-reg-tunnel-04). MIP4 Working Group. Internet-Draft. October 23, 2006.

[9] R. Koodli, Fast Handovers for Mobile IPv6, RFC 4068, July 2005.

[10] P. McCann, Mobile IPv6 Fast Handovers for 802.11 Networks, RFC 4260, November 2005.

[11] Narten, T., Nordmark, E. and W. Simpson, Neighbor Discovery for IP Version 6 (IPv6), RFC 2461, December 1998.

[12] Thomson, S. and T. Narten, IPv6 Stateless Address Autoconfiguration, RFC 2462, December 1998.

[13] Conta, A. and S. Deering, Generic Packet Tunneling in IPv6 Specification, RFC 2473, December 1998.

[14] M. Kulkarni, A. Patel, K. Leung, Mobile IPv4 Dynamic Home Agent (HA) Assignment, RFC 4433, March 2006.

[15] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315, July 2003.

[16] J. Arkko, C. Vogt, W. Haddad, Enhanced Route Optimization for Mobile IPv6, RFC 4866, May 2007.

[17] Xavier Pérez-Costa, Marc Torrent-Moreno, Hannes Hartenstein, A performance comparison of Mobile IPv6, Hierarchical Mobile IPv6, fast handovers for Mobile IPv6 and their combination. ACM SIGMOBILE Mobile Computing and Communications Review. Volume 7 , Issue 4 (October 2003), Pages: 5 – 19. ACM 2003.

[18] C. Vogt, J. Arkko, A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization, RFC 4651, February 2007.

[19] Aura, T., Cryptographically Generated Addresses (CGA), RFC 3972, March 2005.

[20] Hinden, R. and S. Deering, Internet Protocol Version 6 (IPv6) Addressing Architecture, RFC 3513, April 2003.

[21] Burnett, S. and Paine, S., Criptografia e Segurança – O Guia Oficial RSA, RSA Press, Editora Campus.