2
Mobilidade IP – Protocolos

Neste capítulo serão apresentados alguns dos protocolos que, de alguma forma, provêem ou auxiliam na mobilidade do IPv6:

- o Mobile IPv6 (MIPv6) e suas otimizações: o Hierarchical MIPv6 (HMIPv6) e o Fast Handover;
- o Host Identity Protocol (HIP).

Todos esses protocolos foram propostos pelo IETF e procuram facilitar o restabelecimento das conexões e diminuir o tráfego de dados de registro num ambiente de mobilidade ou criar mecanismos que diminuam a latência e o número de pacotes perdidos durante o processo de handoff.

2.1.
MIPv6 – Mobile IPv6 e suas otimizações

O MIPv6 (Mobility for IPv6) [10] especifica um protocolo que permite que os nós móveis continuem acessíveis enquanto se movimentam na rede IPv6 fornecendo aos usuários uma forma de transparência em relação à movimentação. Para isso, o MIPv6 determina o uso de dois endereços IP pelo dispositivo móvel: um endereço referente a sua rede original, conhecido como *Home Address* (HoA), e um endereço que é obtido na rede em que o dispositivo móvel se encontra a cada momento, conhecido como *Care-of Address* (CoA). Dessa forma, o HoA passa a identificar o dispositivo móvel (*Mobile Node* – MN) de forma independente de sua localização, enquanto que o CoA identifica sua posição atual. A partir dessas duas identificações, o MIPv6 propõe o mecanismo que permite a comunicação com o MN ao longo do seu deslocamento pelas diferentes redes, conforme descrito a seguir.

Cada vez que um MN muda de rede e, conseqüentemente, de CoA, ele cadastra esse novo endereço em um dispositivo específico existente na rede de origem chamado *Home Agent* (HA). O HA passa a agir como uma espécie de "substituto" ou "representante" do nó móvel ausente de sua rede original. O papel

do HA é o de receber as mensagens destinadas aos MNs e encaminhá-las utilizando os endereços CoAs cadastrados em sua lista. A forma de encaminhamento dos pacotes recebidos pelo HA para o MN depende da modalidade de CoA utilizado, isto é, da forma como o endereço CoA foi fornecido ao MN, da versão do IP e das otimizações que estejam sendo utilizadas.

Para permitir a obtenção e o registro do CoA no HA, o MIPv6 especifica alguns procedimentos e utiliza mensagens de sinalização próprios. Em primeiro lugar, o MN, ao perceber que mudou de rede (pelo uso de mecanismos de detecção da vizinhança fornecidos pelo próprio IPv6 [19]), obtém e configura um novo CoA usando o procedimento de auto-configuração do IPv6. De posse do CoA, o MN envia uma mensagem de *Binding Update* ao HA informando sua nova localização. O HA, ao receber essa mensagem do MN, atualiza sua lista fazendo a associação entre o HoA e o CoA, enviando então uma mensagem de *Binding Acknowledgement* para o MN. Essa troca de mensagens tem como efeito também o estabelecimento de um túnel entre o HA e um dispositivo que pode ser

- o próprio MN ou
- o dispositivo de entrada (roteador de acesso) da rede visitada.

Caso o dispositivo terminador do túnel seja o roteador de acesso da rede visitada, ele passa a ser o responsável por encaminhar as mensagens ao endereço CoA do MN. Caso contrário, as mensagens serão entregues diretamente ao MN via o túnel estabelecido.

O MN, ao receber a mensagem encaminhada pelo HA, identifica o endereço do nó com quem está se correspondendo – o *Correspondent Node* (CN) – e envia uma mensagem *Binding Update* para esse CN informando seu endereço CoA. O CN então pode passar a se comunicar diretamente com endereço CoA do MN. A figura 1 apresenta um esquema que resume todo esse processo.

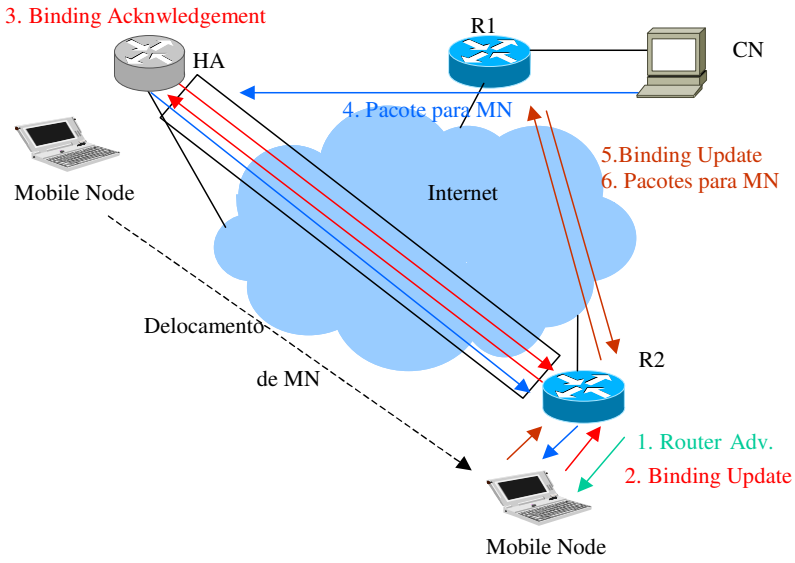

Figura 1: Comunicação usando MIPv6

Porém, mesmo com a utilização do MIPv6, durante o período de handoff, pacotes trocados com o dispositivo móvel que se deslocou podem sofrer atrasos maiores do que o desejado ou até mesmo serem perdidos. Esse efeito acaba por diminuir a qualidade da comunicação, situação que se torna especialmente crítica quando se está lidando com dados multimídia. No intuito de diminuir a latência do *handoff* e a perda de pacotes durante esse período, foram desenvolvidas algumas propostas de otimização, das quais salientamos:

- o Binding Update e Routing Optimization [2][10];
- o Home Agent Discovery [10];
- o HMIPv6 – Hierarchical MIPv6 [24];
- o FMIPv6 – Fast Handover em MIPv6 [12].

2.1.1. Binding Update e Routing Optimization

O Binding Update é uma extensão já incorporada ao MIPv6 que consiste no envio de mensagens especiais que informam ao CN a localização atual do MN para que eles se comuniquem sem utilizar o HA, como apresentado na figura 1. Já o Route Optimization [2] permite o estabelecimento de um túnel entre o roteador de acesso da rede nova e o da rede antiga de forma que os datagramas enviados para o MN que foram encaminhados ao roteador de acesso da rede antiga durante o período de registro do MN na nova rede possam ser encaminhados ao novo

roteador. Isso permite a diminuição da perda de pacotes por desconhecimento da localização do MN.

2.1.2. Home Agent Discovery:

Caso o MN não conheça o endereço IP do Home Agent em sua rede doméstica, ele deve enviar uma mensagem *ICMP Home Agent Address Discovery Request* para o endereço *anycast* de Home Agents IPv6 [9], subnet definida pelos onde últimos 7 bits do endereço IP iguais a 126 (decimal) ou 7F (hexadecimal), com o prefixo de sua rede doméstica. O HA que receber a mensagem deve retornar uma mensagem *ICMP Home Agent Discovery Reply* para o MN com os endereços unicast dos HAs ativos em sua rede.

Ao receber a mensagem de resposta, o MN deve enviar seu Binding Update de registro para qualquer um dos endereços *unicast* presentes na lista. Ele também pode tentar enviar o BU para cada um dos HAs listados até obter uma resposta. Para usar esse mecanismo, o MN deve esperar, no mínimo 1,5 vezes o tempo em segundos de retransmissão antes de tentar o próximo HA da lista (a ordem aqui é importante).

Caso o MN possua um registro em um HA de sua rede doméstica e seu registro ainda não expirou, ele deve primeiro tentar gerar uma nova conexão com esse HA, e apenas em caso de falha dessa tentativa, enviar BU para outro HA.

2.1.3. HMIPv6

O HMIPv6 [24] foi projetado para reduzir a troca de sinalização entre o MN, seus CNs e o HA por meio da inserção de um novo comportamento a um ou mais roteadores existentes no modelo MIPv6 chamado de Ponto de Âncora de Mobilidade (*Mobility Anchor Point* - MAP), facilidade que pode ser aplicada em qualquer dos roteadores, incluindo o do roteador de acesso (AR), que serve como ponto intermediário de registro de localização do MN.

O MN, entrando em um domínio que contenha o dispositivo MAP, receberá *Router Advertisements* contendo informações sobre um ou mais MAPs locais.

Para uma operação apropriada de HMIPv6, o MN criará dois CoAs: um CoA Regional (RCoA) obtido na rede visitada e o CoA do link em uso (LCoA). Para se comunicar com CNs e HA, o MN utiliza seu endereço RCoA e para se comunicar com o servidor MAP, o MN utiliza o endereço LCoA.

O MAP age como um HA local, recebendo os datagramas endereçados ao RCoA de MN, encapsulando-os e enviando-os ao endereço LCoA de MN. Se MN muda de LCoA dentro do domínio MAP, espaço de roteadores que divulgam o endereço do mesmo MAP em suas mensagens *Router Advertisements*, ele precisa apenas registrar esse novo endereço no MAP. O RCoA não se altera enquanto o MN se mover dentro do domínio do roteador MAP no qual está registrado. Isso torna transparente a mobilidade do MN para os CNs que se comunicam com ele.

O domínio MAP não precisa ser definido dentro de um domínio físico de mesmo prefixo. Roteadores de diferentes localizações, domínios e tecnologias podem participar de um domínio hierárquico MAP. Toda vez que MN detecta um movimento, ele também detecta se está no mesmo domínio MAP. Se o endereço MAP recebido na mensagem *Router Advertisement* for diferente, MN deve obter um novo RCoA e enviar Binding Updates para os CNs e HA usando o protocolo MIPv6.

Um exemplo de arquitetura é apresentado na figura 2. AR são os roteadores de acesso às redes 1 e 2.

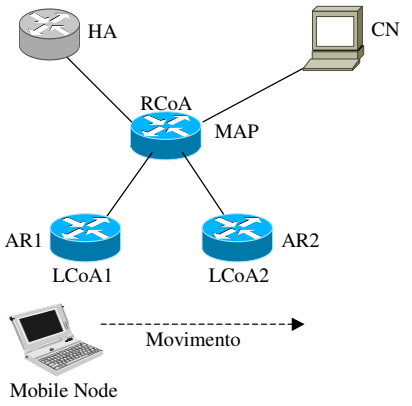

Figura 2: Exemplo de arquitetura com dispositivo MAP no HMIPv6

2.1.4. FMIPv6

O FMIPv6 [12] é uma extensão proposta para MIPv6 com o objetivo de reduzir a latência de *handoff* de forma que um MN envie pacotes tão logo ele

reconheça a presença de uma nova sub-rede e que pacotes sejam entregues a ele assim que sua presença seja identificada pelo Roteador de Acesso (*Access Router* – AR) nessa nova sub-rede.

Para isso, o FMIPv6 adiciona duas novas mensagens ao MIPv6: *Router Solicitation for Proxy Advertisement* (RtSolPr) e *Proxy Router Advertisement* (PrRtAdv). Essas novas mensagens, juntamente com a definição de mensagens de sinalização informativas da camada inferior, servem para auxiliar o MN a rapidamente detectar um iminente movimento, propor um endereço CoA e executar uma série de ações para um *handoff* mais suave entre o antigo e o novo AR usando outras novas mensagens: Fast Binding Update (FBU), Fast Binding Acknowledgment (FBack), Handover Initiate (HI), Handover Acknowledgment (HAck), e Fast Neighbour Advertisement (FNA).

FMIPv6 possui dois modos de operação: modo preditivo e modo reativo. Eles diferem pelo tempo em que o MN recebe a mensagem FBack: antes ou depois do MN se desconectar do antigo AR.

No modo Preditivo, o processo é iniciado com o envio de uma mensagem *PrRtAdv* pelo antigo AR para o MN em resposta ao recebimento da mensagem *RtSolPr* enviada pelo MN ou de qualquer sinal de handover determinado pelo dispositivo de acesso à rede. Quando MN recebe *PrRtAdv*, ele prepara um CoA baseado no prefixo de subnet do AR escolhido usando o método de auto-configuração do IPv6. Feito isso, MN envia uma mensagem *FBU* para o antigo AR solicitando o re-direcionamento de seu tráfego para o novo AR. Para isso o antigo AR compõe uma mensagem *HI* para o novo AR com o objetivo de informar a esse o iminente handover e verificar se o endereço CoA proposto por MN é válido. O novo AR responde com uma mensagem *HAck* que conterá um novo endereço CoA caso o proposto não seja válido. O recebimento da mensagem *HAck* no antigo AR faz com que este envie uma cópia de *FBack* para o endereço CoA de MN pelo link anterior e pelo novo link estabelecido com o novo AR, e depois encaminha o tráfego direcionado a MN para o novo CoA.O MN ao estabelecer conexão com o novo AR envia imediatamente uma mensagem *FNA* para ele informando sua presença. O novo AR passa então a entregar o tráfego de MN ao próprio. Depois disso, MN inicia seu processo de registro do novo CoA no seu HA e realiza testes de *Return Routability* (RR) com cada um dos CNs para otimização de rota.

A diferença para o modo Reativo é que o MN não recebe a mensagem *FBack* antes de perder conectividade com seu antigo AR. Como MN pode não ter como saber quando o a configuração do CoA e o processo de handover suave, ou seja, de encaminhamento de mensagens do antigo para o novo AR, aconteceu sem receber essa mensagem, ele, após se conectar ao novo AR, reenvia uma mensagem *FBU* encapsulada na mensagem FNA. O novo AR verifica a validade do CoA proposto por MN. Se o CoA proposto for válido, o novo AR solicita o envio de *FBack* do antigo AR para MN utilizando-o como ponto de acesso. Em caso negativo, o novo AR envia uma mensagem *Router Advertisement* propondo um CoA válido ao MN. O tráfego destinado a MN passa então a ser encaminhado do antigo AR para o novo que então entrega a MN. Assim que MN confirma seu endereço CoA como válido, ele inicia seu processo de registro do novo CoA no seu HA e executa os testes de RR com cada um dos CNs para otimização de rota.

2.2. HIP – Host Identity Protocol

A proposta do HIP [17][25] é introduzir uma camada intermediária entre as camadas de rede e transporte que permita garantir a mobilidade do nó pela criação de um novo espaço de nomes para identificar hosts de forma independente de sua localização. O endereço IP passa a ser utilizado apenas como subsídio para a localização do nó sob o ponto de vista de encaminhamento dos pacotes pela rede. Associado a esse novo espaço de nomes o HIP define uma forma de garantir uma associação segura entre dispositivos autenticados e uma estrutura de controle para o mapeamento entre esse identificador e o endereço IP que o nó em questão esteja utilizando no momento.

2.2.1. O espaço de nomes HIP

Atualmente, os protocolos da Internet utilizam dois espaços de nomes para a identificação de nós: endereços IP e nomes de domínio DNS [16]. Esses dois espaços de nomes proporcionam várias facilidades, mas também apresentam uma série de problemas. Basicamente, por se tratarem das únicas formas de identificação, há uma sobrecarga de funcionalidades, principalmente quando o

ambiente envolve mobilidade. Em especial, a camada de transporte na arquitetura atual apresenta um forte grau de acoplamento e dependência com os endereços IP. Com esse esquema, a troca dinâmica de endereços IP afeta diretamente o funcionamento das camadas superiores. Esquemas como o MIP, apresentado na seção 2.1, por exemplo, são tentativas de aliviar justamente os problemas desse forte acoplamento do uso do endereço IP para identificação do dispositivo e sua localização.

O espaço de nomes baseado em *Host Identities* (HIs) procura preencher as lacunas deixada pelos endereços IP e os nomes DNS. O identificador, conhecido como *Host Identity* (HI), no espaço de nomes definido pelo HIP representa um nome único e global que identifica um host. Um host pode ter múltiplas identidades, sendo algumas delas "bem-conhecidas" e outras não publicadas ou anônimas. HIs podem ser criados pelos próprios dispositivos ou podem ser criados por um outro dispositivo que forneça credibilidade a essa identificação.

A identidade HI pode ser um nome único global ou pode ser um hash gerado a partir do uso de um par de chaves pública e privada, permitindo a autenticação de pacotes HIP e protegendo o dispositivo de ataques do tipo "man-in-the-middle". Uma vez que a autenticação de datagramas é mandatória para prover proteção contra ataque DoS, a troca Diffie-Hellman [22] no HIP é usada para autenticação.

Cada host terá ao menos um HI, mas, tipicamente, poderá ter vários. Porém, cada HI identifica univocamente um único host, ou seja, não existirá mais de um host com o mesmo HI.

A arquitetura proposta pelo HIP propõe um mecanismo de troca criptografada e segura entre os sistemas. Quando o HIP é utilizado, a troca entre hosts é, normalmente, protegida com o uso do IPsec [11]. HIs são utilizados para criar as associações de segurança do IPsec (*IPsec Security Associations* - SAs) e para a autenticação dos hosts.

2.2.2.
Host Identity Tags

O HIP determina a utilização de *Host Identity Tags* (HITs) na troca de informações e armazenamento dos HIs. Um HIT é uma representação de 128 bits obtida a partir de um *hash* calculado sobre o HI.

Nos pacotes HIP, os HITs identificam a origem e o destinatário do pacote. Por esta razão, o HIT deve ser único pelo tempo que ele estiver em uso. Em um caso extremo em que um único HIT mapeie mais de um HI, as chaves públicas farão a diferenciação final. O tamanho de 128 bits foi escolhido de forma que as portas de comunicação entre as camadas e as estruturas de armazenamento de endereçamento dos dispositivos não precisem ser alteradas para compatibilidade com esse protocolo uma vez que este é o tamanho campo endereço IP versão 6.

2.2.3.
HIP e DNS

A maior parte das aplicações na Internet, antes de estabelecer a comunicação com um parceiro, é levada a traduzir uma identificação, conhecida *nome de domínio* (nome DNS [16]), em um ou mais endereços IP. Esse procedimento está baseado em consultas a servidores específicos conhecidos como *servidores DNS*.

No esquema definido pelo DNS, os nomes de domínio são utilizados pelas aplicações como argumentos para um agente local denominado *resolvedor*, cuja função é devolver à aplicação local o endereço IP que corresponde àquele nome. O resolvedor é, portanto, o responsável por consultar uma base de informações de nomes de domínio. Em geral, essa base de informações encontra-se distribuída em uma hierarquia de servidores capazes de, cooperativamente, determinar o endereço IP desejado. Para a aplicação usuária, essa base de nomes de domínio é única, ficando totalmente transparente qualquer tipo de distribuição ao longo dos servidores. É tarefa do resolvedor prover esse tipo de transparência às aplicações locais, fazendo as consultas necessárias aos servidores remotos e centralizando as respostas a serem devolvidas.

De posse do endereço IP, a camada de transporte na arquitetura tradicional (sem o HIP) é capaz de estabelecer sessões de comunicação (com ou sem conexão) com as aplicações parceiras.

Com o uso do HIP, endereços IP devem passar a ser utilizados apenas pela camada inter-rede, enquanto que a camada de transporte, passa a se referenciar somente a HIs ou a HITs. Conseqüentemente, é necessário um meio de tradução do nome de domínio em um HI ou HIT. A utilização de uma extensão do DNS para essa tarefa é quase que direta [20]: define-se um novo registro de recurso (*Resource Record* – RR)[1] referente ao HIP. Quando há um pedido de tradução de um nome de domínio por parte de uma aplicação, o resolvedor fará, além da busca pelo IP, uma busca do HI (ou HIT) de forma a fornecer para a camada de transporte o HI desejado. Adicionalmente, a camada HIP local fará, internamente, o mapeamento do HI no endereço IP correspondente.

Porém, quando um nó que utiliza o HIP apresenta mudanças freqüentes de endereço IP (como é o caso dos nós móveis), a latência natural de propagação das modificações pela base distribuída do DNS começa a ter um impacto negativo no processo de mapeamento. Para resolver esse problema, a arquitetura proposta pelo HIP introduziu o conceito de *servidor rendez-vous* (*Rendez-vous Server* – RVS) [13]. Assim, um nó móvel publicará o endereço do seu RVS para o DNS, de forma que o RR do HIP não se alterará para esse nó, mesmo quando ele se movimentar para outra rede. Resta ao nó móvel se registrar no RVS antes de passar a utilizá-lo, além de manter atualizado o seu endereço IP atual nesse servidor. Esse processo será apresentado com mais detalhes na seção 2.2.6.

Dessa forma, um host que utiliza o HIP, ao desejar se comunicar, consulta o DNS para descobrir se o seu par possui um cadastro HIP. Após o retorno dessa consulta, o host consulta o DNS para obter a informação de localização desse parceiro (o seu endereço IP). Caso o dispositivo seja um nó móvel, ele terá cadastrado, no campo de endereço IP, o endereço de seu servidor rendez-vous, que é o servidor atualizado toda vez que o nó móvel visita uma nova rede. O RVS, ao receber um pacote, verifica se o endereço HIT de destino é o seu próprio. Caso não seja, verifica se tem registrado em sua base de dados o HIT recebido. Em caso

[1] Um registro de recurso corresponde a um conjunto de informações associado aos nomes de domínio e que é armazenado nos servidores DNS juntamente com os nomes propriamente ditos.

afirmativo, encaminha a mensagem para o dispositivo final utilizando o endereço atual do mesmo. Depois desse procedimento, o dispositivo móvel passará então a se comunicar diretamente com o dispositivo que iniciou o processo, sem a intervenção do RVS, pois ele passará a notificar todas as alterações de endereçamento IP diretamente a ele (bem como ao RVS).

2.2.4. Alterações na arquitetura e suas implicações

Atualmente, o endereço IP acumula duas funções: a de localizador e a de identificador de dispositivos finais, ou seja, cada endereço IP nomeia uma localização topológica na internet, agindo como um vetor de direção de roteamento, conhecido como localizador e, ao mesmo tempo, nomeia a interface física da rede atualmente identificada como ponto de conexão, agindo assim como identificação do dispositivo final.

Considerando meta-sistema um sistema cujas características são adaptadas por um meta-serviço, uma aplicação que age sobre outro serviço, pode-se definir a arquitetura HIP como um meta sistema que separa as funções de localização e identificação exercidas pelo endereço IP através da criação de um novo elemento chamado HI ou HIT que passam a assumir a função de identificadores enquanto o endereço IP continua a exercer seu papel de localizador de dispositivos.

É importante entender que os nomes de dispositivos baseados em HI são ligeiramente diferentes dos nomes de interface; um HI pode ser alcançável, simultaneamente, por diversas interfaces. A atuação da arquitetura HIP sobre a arquitetura TCP/IP é apresentada na figura 3, onde os tracejados identificam funções exercidas pelo endereço identificado.

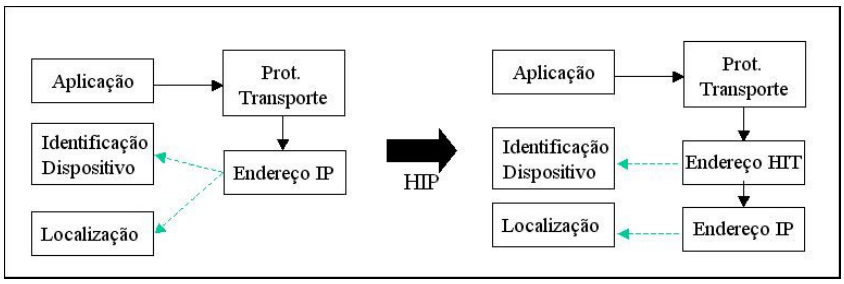

Figura 3: Alteração na pilha de protocolo TCP/IP com uso do HIP

Com a alteração proposta pelo HIP, as conexões TCP e associações UDP não são mais estabelecidas considerando-se o endereço IP dos dispositivos, mas

considerando seus Host Identities (HITs). Desta forma, mesmo que o endereço IP de um dos dispositivos em questão seja alterado, as conexões e associações anteriores não são modificadas.

Esta característica também permite que um único dispositivo físico possua diversos endereços lógicos (cada um possui um HI diferente) e possibilita o processo de migração do host entre redes e de agregação (cluster) de servidores. Ou seja, HIP pode prover, com baixo custo de infra-estrutura, as facilidades de mobilidade e multi-homing.

Um sistema é considerado móvel se seu endereço IP pode mudar dinamicamente por qualquer razão ou pela tradução de endereços redes. Da mesma forma, um sistema é considerado multi-home se possui mais de um endereço IP público ao mesmo tempo. O HIP agrega vários endereços IPs num mesmo HI quando estes endereços correspondem ao mesmo dispositivo.

2.2.5. Operação do HIP

Esta subseção descreve a troca de mensagens usada pelo HIP para estabelecimento das configurações de autenticação e criptografia, se existentes. Este mecanismo é conhecido como *troca de mensagens básica HIP* [18] e tem por principal objetivo gerenciar a máquina de estados do protocolo entre uma origem e seu destino (ou responder) chamado de associação HIP. Após a conexão ser estabelecida com sucesso, os dados são transferidos usando o formato de transporte ESP (*Encapsulated Security Payload*) [11] do IPSec. A troca de mensagens básica do HIP para estabelecimento da conexão é apresentada na figura 6.

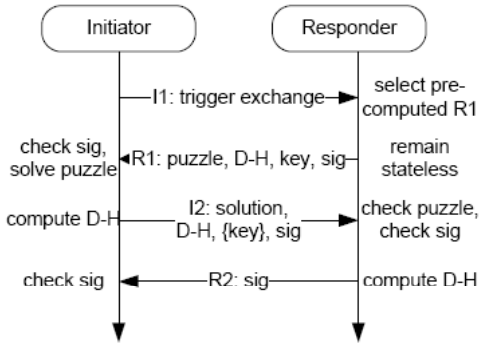

Figura 4: Troca básica de mensagens HIP

Key é a chave pública do HI, *sig* representa a assinatura utilizando essa chave e *D-H* é a chave Diffie-Hellman [22], chave gerada pelo protocolo Diffie-Hellman que permite a troca de uma chave secreta através de um meio inseguro sem uso segredos previamente definidos.

A primeira mensagem, I1, inicia a troca básica HIP. As últimas três mensagens, R1, I2 e R2, constituem o padrão de troca segura de chaves Diffie-Hellman autenticado.

O iniciador (ou a origem) envia a primeira mensagem, I1, para o destinatário. Este pacote serve de disparador para a troca básica HIP. O pacote contém apenas o HIT da fonte e o HIT do destinatário, caso não se esteja utilizando o modo oportuno que permite se estabelecer uma associação HIP sem conhecer o HIT de destino. A segunda mensagem, R1, inicia a troca. O destinatário envia um desafio criptografado, chamado quebra-cabeça HIP, onde a origem deve resolver corretamente para que o processo possa continuar.

O quebra-cabeça HIP é um desafio matemático que deve ser resolvido pela origem da troca de mensagens básica para provar sua boa intenção. O mecanismo de quebra-cabeça protege o destinatário de um número de ataques DoS. O destinatário pode definir o grau de dificuldade do quebra-cabeça para a origem baseado em seu nível de confiança, de acordo com a carga atual ou outros fatores. O destinatário usa heurísticas para determinar se está sob um ataque DoS e pode então definir o valor de dificuldade do quebra-cabeça apropriadamente.

A mensagem R1 também pode enviar sua chave pública Diffie-Hellman, HI e assinatura. O significado da assinatura é permitir autenticação do pacote, uma vez gerado pelo destinatário. A assinatura exclui a si mesma, os parâmetros subseqüentes e alguns parâmetros que tem uma influência direta na assinatura, como o checksum. A assinatura é calculada usando os algoritmos RSA ou DSA.

Na mensagem I2, a origem envia a solução do quebra-cabeça para o destinatário. Se a mensagem I2 não contém a solução correta, ela é descartada. Usando o pacote R1, a origem pode computar a chave de sessão Diffie-Hellman. A associação HIP também é criada usando a chave de sessão. Esta associação pode ser usada para criptografar a chave pública HI. A mensagem resultante I2 contém a chave Diffie-Hellman da origem, a solução do quebra-cabeça HIP, sua chave de autenticação pública (opcionalmente criptografada) e a assinatura. A assinatura em I2 cobre a maior parte dos campos da mensagem.

O destinatário, a partir da I2, extrai da chave pública Diffie-Hellman da fonte e computa sua própria chave de sessão Diffie-Hellman. A associação HIP correspondente é então criada. Se a chave pública de autenticação da origem foi enviada com criptografia, é possível agora decriptografá-la. Por fim, a mensagem R2 é enviada contendo apenas a assinatura, e o cabeçalho HIP. Esta mensagem finaliza a troca de chaves Diffie-Hellman para a geração da chave de sessão para a troca básica HIP.

Depois da criação da associação HIP, um dispositivo pode construir o SA IPSec correspondente usando o material de chave gerado anteriormente. O formato ESP IPSec irá criptografar e autenticar os dados do usuário.

Nem sempre os dispositivos envolvidos na troca de mensagem seguem todos esses passos porque o dispositivo de destino pode escolher recusar a conexão. O dispositivo pode ter várias razões para fazer isso. Por exemplo, se a política dele é ser apenas a origem, então ele deve estar apenas habilitado para iniciar suas conexões de troca HIP e deve rejeitar todas as conexões de troca HIP iniciadas por outros dispositivos.

Se um dispositivo rejeita a entrada em uma troca HIP com a origem, ele deve enviar uma mensagem ICMP “Destination Unreachable, Administratively Prohibited”. A mensagem foi intencionalmente escolhida por ser simples, porque mensagens HIP mais complexas podem criar oportunidades para potenciais ataques DoS.

A máquina de estados do protocolo HIP possui oito estados:

- UNASSOCIATED: início da máquina de estados;
- I1-SENT: iniciando a troca básica de mensagens;
- I2-SENT: aguardando para completar a troca básica;
- R2-SENT: aguardando para completar a troca básica;
- ESTABLISHED: associação HIP estabelecida;
- CLOSING: fechando associação HIP, nenhum dado pode ser enviado;
- CLOSE: associação HIP fechada, nenhum dado pode ser enviado;
- E-FAILED: troca básica HIP falhou.

As transações entre os estados ocorrem com o recebimento de pacotes autenticados e processados com sucesso.

O estado inicial é o *não associado*. O próximo estado, *I1 enviado*, é alcançado quando se deseja estabelecer uma conexão HIP e se envia a mensagem I1 que inicia a troca básica do HIP. O próximo estado é alcançado com o recebimento da mensagem R1 e o envio de I2. Esse estado é chamado de *I2 enviado*. A transação para o estado estabelecido ocorre quando o host recebe a mensagem R2.

A estação que responde às mensagens de estabelecimento de conexão HIP passa do estado não associado para o estado *R2 enviado* ao receber a mensagem I2 e enviar a mensagem R2. O recebimento de um pacote de dados utilizando os parâmetros acordados na troca básica passa a máquina de estado dessa estação para o estado *estabelecido*. É nesse estado que a troca de informações das camadas superiores acontece.

A máquina de estados HIP transita para o estado fechando quando recebe um pedido de fechamento da associação ou quando a mesma não é utilizada num tempo maior que o tempo de expiração especificado. O recebimento da mensagem CLOSE solicitando o fechamento da associação deve ser confirmado com o envio da mensagem CLOSE_ACK. O próximo estado é definido pela mensagem que será recebida ou enviada. O estado passa a ser o *não associado* caso não se receba ou não se envie nenhuma mensagem durante um período pré-determinado.

Todas as mensagens HIP possuem um cabeçalho padrão (vide figura 5). Esse cabeçalho é logicamente uma extensão de cabeçalho IPv6:

- Header Lenght: o comprimento do cabeçalho e dos parâmetros HIP;
- Packet Type: tipo de pacote HIP que está sendo encaminhado. Existem oito tipos básicos de pacotes HIP: quatro para a troca básica do HIP (I1, I2, R1, R2), um para atualização de informações (UPDATE), uma para envio de notificações (NOTIFY) e duas para fechamento da associação HIP (CLOSE, CLOSE_ACK). Cada um desses pacotes será apresentado com mais detalhes posteriormente;
- HIP Version: versão HIP utilizada (atualmente 1). Este valor deve ser incrementado apenas se houver alguma incompatibilidade que altere o protocolo. Para as demais alterações basta se definir novos tipos de pacotes, novos parâmetros ou novos controles;
- Res: reservado para uso futuro (dois primeiros bits são zero);

- Checksum: checksum para todo o pacote;
- Controls: informação sobre a estrutura do pacote e as capacidades do dispositivo. O dispositivo de origem pode escolher enviar uma mensagem anônima (o HI não está listado no diretório). O dispositivo de destino, ao receber uma mensagem deste tipo, pode escolher não aceitá-la. Os demais controles ainda não foram definidos;
- HIT (origem e destino): hash de identificação do dispositivo. Estes campos sempre possuem 128 bits de comprimento;
- HIP Parâmetro: várias opções e extensões do HIP. O comprimento deste campo é variável.

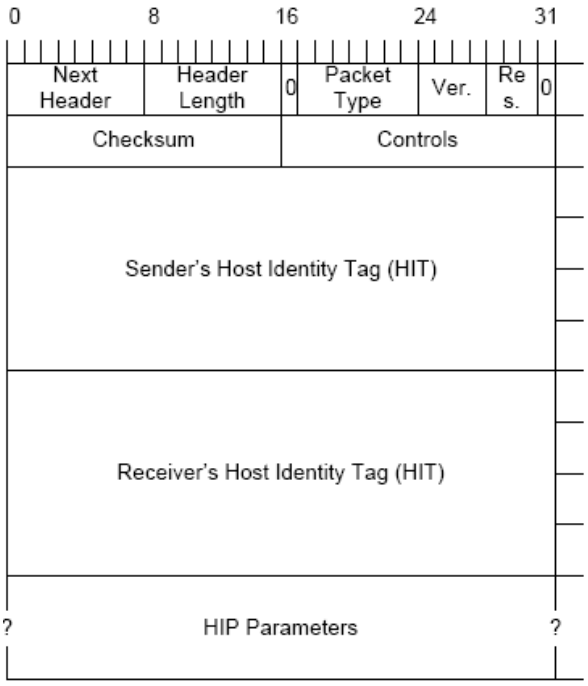

Figura 5: Cabeçalho de mensagem HIP

O campo parâmetro do HIP consiste de zero ou mais parâmetros TLV codificados. Os oito tipos de pacotes definidos apresentam os parâmetros TLV conforme especificação da tabela 1.

TLV	Tipo	Comprimento	Descrição
R1_COUNTER	128	12	Contador de boot de sistema
PUZZLE	257	12	K e Randômico #I
SOLUTION	321	20	K, Randômico #I e Solução do Puzzle J
SEQ	385	4	Atualização do número ID do pacote
ACK	449	variável	Atualização do número ID do pacote
DIFFIE HELLMAN	513	variável	Chave pública
HIP_TRANSFORM	577	variável	Encriptação HIP e Tranformada de Integridade
ENCRYPTED	641	variável	Parte encriptadado pacote I2
HOST_ID	705	variável	Identidade do Host com FQDM ou NAI
CERT	768	variável	Certificado HI usado para transferir certificados
NOTIFICATION	832	variável	Dado Informativo
ECHO_REQUEST_SIGNED	897	variável	Dado a ser respondido na confirmação com assinatura
ECHO_RESPONSE_SIGNED	961	variável	Dado respondido na confirmação com assinatura
HMAC	61505	variável	HMAC baseado no código de autenticação da mensagem como material da chave de HIP_TRANSFORM
HMAC 2	61569	variável	HMAC baseado no código de autenticação da mensagem como material da chave de HIP_TRANSFORM. Parâmetro HOST_ID é usado nesse cálculo
HIP_SIGNATURE 2	61633	variável	Assinatura de pacote R1
HIP_SIGNATURE	61697	variável	Assinatura de pacote
ECHO_REQUEST_UNSIGNED	63661	variável	Dado a ser respondido na confirmação após assinatura
ECHO_RESPONSE_UNSIGNED	63425	variável	Dado respondido na confirmação após assinatura

Tabela 1: Parâmetros TLV do protocolo HIP

Enviar HIs e HITs no cabeçalho de pacotes de dados do usuário aumenta o overhead do pacote. Então, foi planejada uma maneira em que eles não sejam enviados em todos os pacotes, mas que outros parâmetros no cabeçalho sejam usados para mapear os pacotes de dados a seus correspondentes HIs. Em alguns casos, isso faz com que seja possível usar o protocolo HIP sem nenhum cabeçalho adicional nos pacotes de dados do usuário. Por exemplo, quando é utilizado o formato ESP, o SPI, Security Parameter Index, carregado pelo cabeçalho ESP pode ser usado para mapear o pacote de dados criptografado na associação HIP correta. Para isso, a camada HIP passa a interagir com o campo SPI do cabeçalho ESP.

Uma associação HIP pode necessitar ser atualizada ao longo do tempo. Isto pode acontecer devido a trocas na conexão (preservando mobilidade), expiração de SAs IPSec ESP ou pela adição de novas associações HIP (multi-homing). O protocolo de re-endereçamento é assimétrico onde um dispositivo, chamado de dispositivo móvel, informa outro dispositivo, chamado de dispositivo par, sobre as alterações de endereços IP no SPI (Security Parameter Indexes) afetado. Isso é feito através do envio da mensagem UPDATE.

Para conexões onde um dos dispositivos é móvel [5], utiliza-se o parâmetro HIP chamado LOCATOR que contém zero ou mais campos de localizadores, que é uma estrutura que indica como o pacote deve ser encaminhado através da rede e tratado pelo dispositivo final. O parâmetro LOCATOR tem por objetivo identificar o fluxo de dados e facilitar a alteração dos parâmetros necessários em uma associação sem que haja necessidade de reinício do mecanismo de troca

básica. Ele pode ser um simples endereço IP ou possuir contexto adicional para multiplexação e demultiplexação para tratamento de pacotes das camadas inferiores. Ele está inserido inicialmente nas mensagens UPDATE, mas encontra-se em estudo a inserção deste parâmetro nas mensagens I2 e R1.

Esse parâmetro é consiste dos campos padronizados do protocolo HIP, campos tipo (193) e tamanho, seguido por zero ou mais sub-parâmetros Localizador. Cada sub-parâmetro Localizador contém um campo de identificação de tipo de tráfego (sinalização de controle do HIP e dados, apenas sinalização ou apenas dados), tipo de localizador (apenas o endereço IP ou a concatenação do SPI ESP com o endereço IP), o tamanho do sub-parâmetro, um bit de identificação se o localizador é preferencial ou não, e um campo com o tempo de validade da informação. Essa estrutura pode ser observada na figura 6.

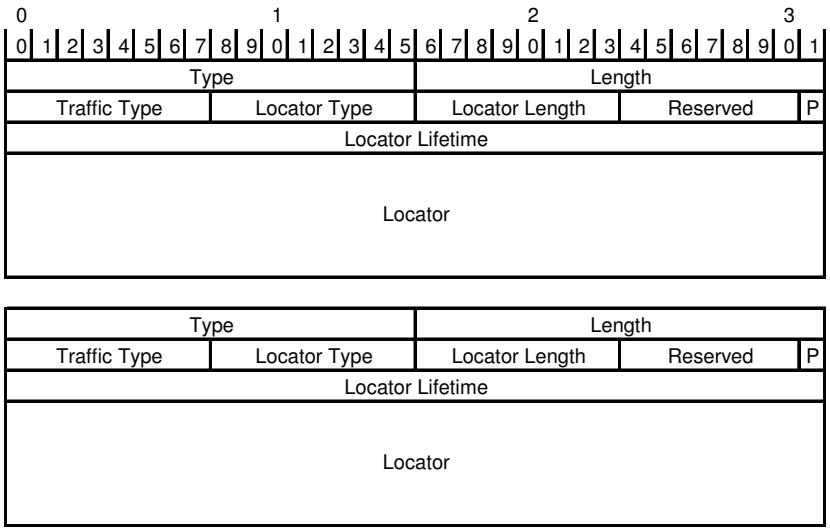

Figura 6: Estrutura do parâmetro LOCATOR no HIP

Quando um nó se move para uma nova rede, ele notifica seu novo endereço ao seu par de comunicação e ao servidor Rendez-vous no qual está registrado enviando um pacote HIP UPDATE que contém o parâmetro LOCATOR. O recebimento do pacote UPDATE deve ser confirmado pelo nó receptor. Para confiabilidade em presença de perda de pacotes, podem-se enviar várias cópias do pacote UPDATE e apenas confirmar a entrega de um. O conteúdo do pacote é autenticado pela assinatura e o hash de chaves do pacote.

Usando-se o modelo de segurança definido, o modo transporte do protocolo ESP [8], o nó móvel pode decidir se deseja trocar as chaves da associação de segurança e gerar uma nova chave Diffie-Hellman no momento em que está

atualizando sua posição; tudo isso é feito através da inclusão de um novo parâmetro no pacote UPDATE, o ESP_INFO.

A alteração do endereço IP não altera as configurações do SA ESP e por essa razão o nó pode continuar a enviar pacotes a seu par sem necessidade de trocar as chaves. O parâmetro ESP_INFO possui dois campos importantes ao HIP: old_SPI e new_SPI. Dependendo do conteúdo desses campos, o nó receptor identifica se a geração de uma nova chave e um novo SPI está sendo solicitada pelo nó móvel ou não.

Para concluir o processo de atualização das características da associação HIP, o pacote UPDATE deve ter suas informações confirmadas pelo nó origem. Essa confirmação tem por objetivo garantir que a solicitação de alteração de endereço foi originada realmente do nó móvel. A verificação de endereço é implementada pelo envio de parte de alguma informação que não possa ser adivinhada para o novo endereço, esperando-se o recebimento de alguma confirmação do nó móvel que indique que esse pedaço de informação foi recebido no endereço novo. Essa confirmação pode ser a troca de um nonce, parâmetro que se altera no tempo usado para prevenir ataque de reenvio ou reprodução de um arquivo, ou a geração de um novo SPI e a observação de chegada de dados neste SPI.

O procedimento de atualização de endereço através de envio de mensagem UPDATE e as informações contidas nessa mensagem são apresentadas a seguir:

1. O nó móvel envia um parâmetro LOCATOR para o seu par numa mensagem UPDATE que também contém o parâmetro ESP_INFO que por sua vez contém os valores do antigo e do novo SPI para a associação segura. No caso onde não ocorre troca de chaves, os valores do antigo e do novo SPI são iguais ao valor do SPI de entrada atual. O parâmetro LOCATOR contém o novo endereço IP e o tempo em que esta informação é válida. Depois disso, o nó móvel aguarda a confirmação do recebimento deste pacote. O parâmetro SEQ deve ser preenchido com o valor “1” caso essa seja a primeira mensagem UPDATE para este fluxo;
2. O nó para que recebeu a mensagem UPDATE a valida e então atualiza qualquer ligação local entre a associação HIP e o endereço de destino desse nó. A confirmação de alteração é então iniciada pelo envio de um nonce no parâmetro ECHO_REQUEST da mensagem UPDATE que é

enviada de volta ao nó móvel, utilizando-se o novo endereço, confirmando o recebimento da mensagem anterior através do parâmetro ACK;

3. O nó móvel então completa o re-endereçamento processando o pacote UPDATE ACK e inserindo o nonce no parâmetro ECHO_RESPONSE. Assim que o nó par do nó móvel recebe esta ECHO_RESPONSE, ele considera o novo endereço verificado e o coloca no estado de uso completo.

Caso deseje-se realizar a troca das chaves no momento de atualização do endereço, basta enviar o parâmetro ESP_INFO com o valor do campo SPI antigo com o valor do SPI atual e no campo novo SPI o valor desejado para SPI, o índice de mapeamento de chave desejado e, opcionalmente, o parâmetro Diffie-Hellman para troca de chaves. Ao receber esse pacote, o nó receptor atende ao pedido de troca de chaves e segue o procedimento do tratamento do pacote UPDATE descrito anteriormente. O primeiro parâmetro a ser processado na mensagem UPDATE é o ESP_INFO, pois ele pode indicar o mapeamento entre o SPI novo com o atual ou a solicitação de criação de um novo SPI. A figura 7 apresenta um resumo desse processo.

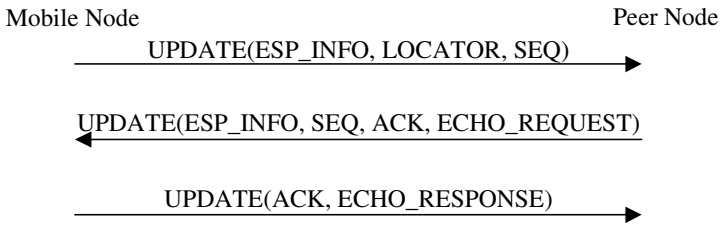

Figura 7: Atualização de conexão HIP sem geração de novas chaves

O controle do estado dos endereços existentes na camada HIP é feito através da classificação desses endereços em três estados:

- UNVERIFIED: indica que o endereço ainda não foi verificado;
- ACTIVE: indica que o endereço foi verificado e confirmado;
- DEPRECATED: indica que o tempo de vida útil do endereço expirou.

Através da observação desses estados, a camada HIP toma a decisão de encaminhar as mensagens ou não usando o novo endereço. Para diminuir o impacto da verificação do novo endereço na comunicação entre o nó móvel e seu par, utiliza-se um algoritmo de autorização baseada no crédito, Credit-Based

Authorization (CBA), para enviar mensagens enquanto o endereço não passa para o estado ACTIVE.

O objetivo do CBA é controlar o envio de mensagens a endereços não confirmados pela quantidade de dados recebidos recentemente daquele nó para prevenir amplificação de ataques de inundação.

Nesse mecanismo, o nó mantém um contador de crédito com cada par. Sempre que um pacote chega do nó par, o nó deve aumentar o contador de créditos desse nó no tamanho do pacote recebido. Quando o nó quer enviar um pacote ao nó par e o endereço presente no parâmetro LOCATOR está no estado UNVERIFIED, ele verifica se o valor do contador de crédito daquele nó par é maior que o tamanho do pacote que se deseja enviar. Se o valor do contador de crédito for menor, o pacote deve ser descartado ou armazenado no buffer até que a verificação seja concluída com sucesso. Quando um pacote é enviado para um nó par por um endereço não validado, o valor do contador de crédito desse nó deve ser reduzido no tamanho do pacote. O contador de crédito de um nó para um endereço que esteja com estado ACTIVE não é alterado pelo envio de pacotes.

Além disso, o nó faz com que os contadores de créditos dos nós participantes das associações seguras que ele mantém sejam decrescidos gradualmente no tempo. Esta ação previne que um nó malicioso não tenha como aumentar seus créditos numa velocidade bem lenta e use isso para gerar um fluxo muito grande de pacotes redirecionados.

2.2.6. Processo de registro HIP e uso do servidor Rendez-vous

Para que o RVS seja usado no registro de DNS de um nó móvel, é preciso que o nó móvel se registre nele. O processo de registro [14] segue o modelo e usa as mesmas mensagens da troca básica do HIP apresentados na seção anterior, acrescentando alguns parâmetros TLV adicionais específicos a essa função.[2]

O processo é iniciado com o nó móvel enviando uma mensagem I1 ao RVS. O servidor então responde com uma mensagem R1 acrescida do parâmetro REG_INFO, que apresenta os serviços disponíveis e suas características.

[2] A maneira como o nó móvel fica ciente da existência do RVS não é definida.

O nó móvel verifica os serviços informados como disponível pelo Servidor Rendez-vous e envia uma mensagem I2 adicionada do parâmetro REG_REQUEST informando o serviço no qual deseja se cadastrar.

O Servidor Rendez-vous, ao receber a mensagem com o parâmetro REG_REQUEST, irá analisar se todos os pré-requisitos foram atendidos e se ele possui recursos disponíveis para atender à solicitação. Caso o nó móvel possa ser atendido, o Servidor Rendez-vous envia uma mensagem R2 com o parâmetro adicional REG_RESPONSE concluindo o processo de registro. Em caso contrário, envia o parâmetro adicional REG_FAILED na mensagem R2 apresentando a razão da falha: falta de recursos ou falta de credenciais para autorização. Um resumo do processo de registro é apresentado na figura 8.

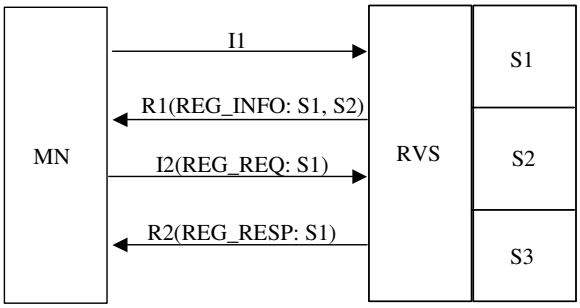

Figura 8: Processo de registro de um nó móvel a um servidor rendezvous

Os registros mantidos pelo Servidor Rendez-vous possuem um tempo de vida limitado e devem ser atualizados sempre que houver uma alteração de endereçamento IP do nó móvel ou quando o tempo de vida do registro estiver terminando, caso se deseje mantê-lo. Para essa finalidade, os parâmetros TLV adicionais específicos para registro são adicionados à mensagem UPDATE do protocolo HIP, conforme figura 9.

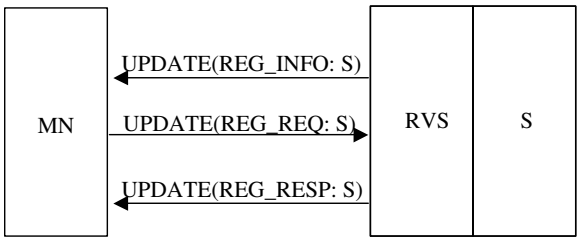

Figura 9: Atualização de registro de nó móvel no servidor rendezvous

Os detalhes dos parâmetros TLV específicos ao processo de registro são apresentados na tabela 2.

TLV	Type	Length	Data
REG_INFO	930	variável	Informação sobre serviço disponível e período mínimo de validade do registro
REG_REQUEST	932	variável	Solicitação de registro a um serviço e proposta de tempo de validade do registro
REG_RESPONSE	934	variável	Serviço registrado com sucesso e tempo de validade do registro
REG_FAILED	936	variável	Serviço não registrado e a razão da falha

Tabela 2: Parâmetros TLV específicos ao processo de registro

Concluída a etapa de registro, o nó móvel pode então divulgar o servidor Rendez-vous no seu registro no servidor DNS. Quando um nó correspondente deseja se conectar ao nó móvel e não conhece o endereço HIT ou seu endereço IP corrente, ele deve realizar uma consulta dessas informações no servidor DNS.

Como o registro aponta para o endereço IP do Servidor Rendez-vous, o nó correspondente envia a mensagem I1 ao Servidor Rendez-vous. Esse, ao receber uma mensagem, verifica se o endereço HIT de destino configurado lhe pertence. Se for, ele entende como um pedido de envio de informações sobre os serviços disponíveis nele. Caso contrário, ele identifica se o endereço HIT de destino pertence a um dos nós móveis presentes em seu cadastro e atualiza o campo de endereço IP de destino com o endereço IP desse nó móvel.

O nó móvel ao receber a mensagem I1 identificada como encaminhamento do Servidor Rendez-vous, verifica se o nó que encaminhou a mensagem é mesmo o servidor, e, apenas se tudo estiver correto, envia a mensagem R1 direto ao nó correspondente que iniciou a associação HIP. A partir desse momento, a troca básica de mensagens HIP é concluída sem o envolvimento do servidor Rendez-vous.

A inserção do Servidor Rendez-vous no HIP acaba por tornar o processo mais complexo devido à característica do protocolo HIP de verificar a integridade dos pacotes. Como ele altera o pacote HIP para inserir os dados atuais de posição do nó móvel em questão, é preciso que o campo Checksum seja recalculado.