Host Identity Protocol: Uma proposta para o Gerenciamento da Mobilidade

Lauro Martins, Gaspare Bruno

Curso de Ciência da Computação – Centro Universitário La Salle
Av. Victor Barreto, 2288 – 92010-000 – Canoas/RS – Brasil

lauro_martins@pop.com.br, gaspare.bruno@gmail.com

Resumo. *Atualmente uma das áreas da computação em desenvolvimento é a provisão de mobilidade, tendo como principal desafio o gerenciamento tanto dos serviços móveis quanto dos terminais de usuários. A complexidade do gerenciamento se dá principalmente por que a arquitetura utilizada nas redes atualmente é baseada no endereço IP, utilizando-o como localizador e identificador de um host ou serviço ao mesmo tempo. Uma das propostas a resolver este problema é o Host Identity Protocol, que entre seus objetivos, está o de separar o localizador do identificador, apresentando uma proposta nova e interessante para suportar o gerenciamento da mobilidade. Este trabalho expõe em ambiente Virtual uma rede com HIP para ser estudada onde será efetuada a análise de funcionamento do protocolo.*

1. Introdução

Concebida no início da década de 60, arquitetura da Internet não acompanhou o avanço tecnológico como o aumento da banda disponível e o crescimento exponencial no número de usuários [WONG, 2006]. Uma das principais características desta arquitetura é a troca de informações entre *hosts* estáticos e sem segurança.

Nos últimos anos, os avanços nas redes sem fio e o crescimento difundido de redes móveis IP, asseguram que a maioria dos utilizadores da Internet será móvel [NOVÁCZKI at al. 2006].

Este trabalho realizou uma análise de funcionamento do protocolo *Host Identity Protocol* (HIP) em um ambiente de máquinas virtuais. Os aspectos levados em consideração foram apenas de experimentos com a mobilidade do *host.*

Esta seção descreveu as principais motivações para o estudo de novas propostas de arquitetura da Internet. As próximas seções do trabalho estão organizadas da seguinte forma: na seção dois será estudado a nova proposta de arquitetura HIP; a seção três irá tratar da metodologia que será utilizada; na seção quatro serão encontrados os resultados do trabalho realizado utilizando máquinas Virtuais.

2 Host Identity Protocol (HIP)

HIP [KOPONEN, GURTOV e NIKANDER 2008] é uma proposta de um nível intermediário que funciona entre os níveis de rede e de transporte. Tem como objetivo prover um método de identificação de nós, que separa a identificação da localização hierárquica do endereço IP. O HIP introduz um novo espaço de nomes para identificação

de um nó (HI, Host Identity) entre os níveis de rede e de transporte. Durante a comunicação entre nós, o HIP provê uma identificação única (HI) para estabelecer e atualizar a comunicação.

2.1 Escalabilidade de um novo Espaço de Nomes

Host Identity namespace: representa uma forma escalável de nomear *host* a ponto de suprir algumas necessidades [MOSKOWITZ e NIKANDER 2006] dentre as principais podemos destacar:

- Deve separar a camada de rede das camadas superiores. Os nomes devem substituir todas as ocorrências de endereços do IP dentro das aplicações;
- A introdução da formação de nomes não deve demandar infra-estrutura administrativa;
- Os nomes devem ter uma representação de largura fixa, para a fácil inclusão nos cabeçalhos do *datagrama* e em relações de programação existentes;
- Uma remota colisão de nomes;
- Compatível com os protocolos existentes e APIs;
- Deve prover autenticação na formação de nomes;

Host Identifiers (HI): Responsável por duas funções básicas. A primeira é separar a camada de rede da camada de transporte, isso permite que as camadas evoluam de forma independente. Tratado no HIP como sendo uma chave pública, permite autenticação utilizando o protocolo seguro IPSec [MOSKOWITZ e NIKANDER 2006].

Host Identity Tag (HIT): É a representação do *Host Identity* em 128 *bits*, criado a partir de criptografia *hash* correspondendo ao *Host Identifier* [AL-SHRAIDEH 2004].

Local Scope Identifier (LSI): É a representação em 32 bits do *Host Identity*, facilita a utilização do *Host Identities* em protocolos e APIs existentes. Permitindo que aplicações legadas como, por exemplo, o FTP possa estabelecer um *socket* com a nova arquitetura.

2.2 Estrutura das camadas

Na atual arquitetura, as camadas são estruturadas como mostra a Figura 1 à esquerda, segundo[NIKANDER e YLITALO, 2003] os processos são a fronteira para *sockes* da camada de transporte. Os *socket* são identificados pelo endereço IP e portas, concomitantemente. O resultado é uma estrutura amarrada a processos para uma determinada topologia e localização, dificultando a migração dos processos para novas localidades.

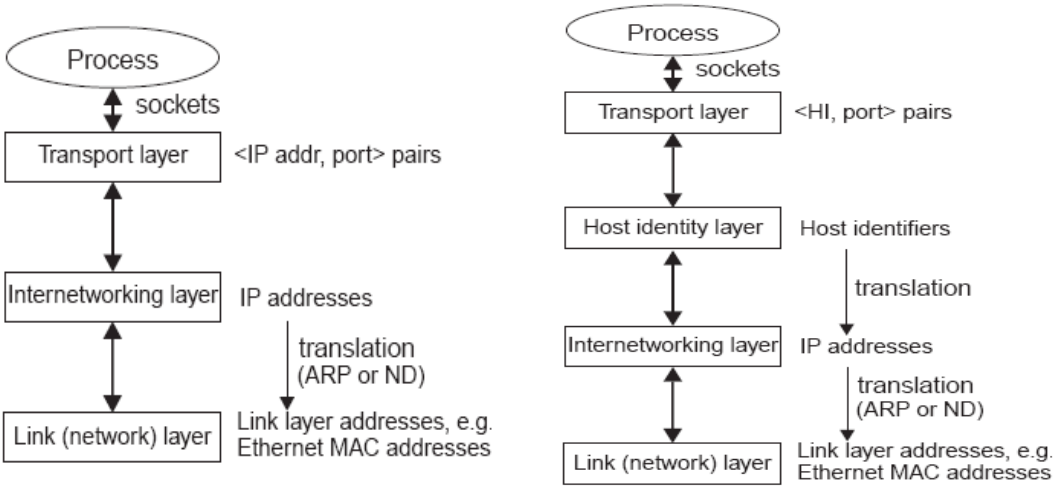

Figura 1: Arquitetura Atual (E) e a proposta para nova arquitetura (D) [NIKANDER e YLITALO, 2003].

Na nova estrutura, a camada *Host Identity Layer* é responsável por traduzir o *Hosts Identifiers* em endereços IPs. Este processo faz a ligação (*bind*) entre *Host Identifier* em endereços. Podendo ser de um para vários endereços IPs. A tradução é efetuada dinamicamente resultando no suporte a mobilidade e a relação dinâmica de um para muitos, provendo suporte *multihoming* [NIKANDER e YLITALO, 2003].

Comparado com a arquitetura atual, o processo de *bind* entre entidades computacionais não é efetuado utilizando apenas o endereço IP como referência de localização e de ligação e sim da seguinte forma: um cliente (*end-point*) estabelece uma ligação (*bind*) com o *Host Identifier* do servidor, que por sua vez resolve dinamicamente a localização do cliente.

A atualização da localização do cliente pode ser efetuada de diversas maneiras duas delas são: o cliente após estabelecer a conexão com a nova rede informa seu novo endereço IP ao Servidor; ou o cliente informa sua nova localização a uma entidade (Ex.: DNS e/ou *Rendezvous Server*) e o servidor consulta esta entidade para resolver a localização do cliente.

2.3 Base Exchange

É um protocolo para troca de mensagens utilizada pelo HIP, seu propósito é gerenciar o estabelecimento das conexões entre: quem inicia uma requisição e quem responde esta requisição [WILTERDINK 2006]. Este processo é denominado associação HIP.

Após o sucesso do *Base Exchange*, a transferência dos dados é formatada utilizando o *Encapsulated Security Payload* (ESP), especificado como parte do IPSec. Esta transferência não precisa ser obrigatoriamente segura pelo ESP, mas a não adoção da mesma compromete a segurança da comunicação.

O procedimento de *Base Exchange* autentica as entidades para que seja estabelecida uma chave simétrica que será utilizada na criptografia dos dados através da troca de quatro mensagens.

O *Base Exchange* quando o *Initiator* inicia a troca de parâmetros com o envio da mensagem I1, que contém o HIT de origem e o HIT de destino. O *Responder*, ao receber a mensagem I1, responde com a mensagem R1, contendo os parâmetros Diffie-Hellman e um desafio (*puzzle)* .

O *puzzle* contido na mensagem R1 é um desafio que visa a busca por um número aleatório que satisfaça a condição enviada por R. O *puzzle* consiste no envio de um número aleatório juntamente com o nível de dificuldade.

Ao receber a mensagem R1, o *Initiator* verifica a assinatura digital e busca a solução do *puzzle*. Ao encontrar a solução, o *Initiator* computa a chave simétrica a partir dos parâmetros Diffie-Hellman recebidos e então envia a mensagem I2 contendo a solução do *puzzle*, os parâmetros Diffie-Hellman e o seu HI, assinando digitalmente a mensagem. Ao receber a mensagem o *Responder*, computa a chave simétrica a ser utilizada pelo modelo de segurança do HIP a partir dos parâmetros Diffie-Hellman e responde com a mensagem R2 que é assinada digitalmente, concluindo o procedimento de *Base Exchange*. A mensagem R2 contém o *Keyed-Hashing for Message Authentication* (HMAC) do pacote HIP, e tem por objetivo evitar ataques DoS (Denial of Service).

2.4 Rendezvous Server

O estabelecimento da comunicação entre duas entidades inicia-se com o envio de uma mensagem, se o serviço estiver ativado, destinado a um elemento da infraestrutura do HIP chamado de *Rendezvous Server* (RVS). O RVS armazena os mapeamentos de identificadores em localizadores e é responsável pelo encaminhamento da mensagem inicial para o estabelecimento da comunicação entre os nós pares [MOSKOWITZ e NIKANDER 2006]. Além disso, o RVS provê o suporte à mobilidade simultânea dos nós, também conhecido como *double jump*.

Primeiramente, o RVS inclui um parâmetro adicional (REG_INFO) em todos os seus pacotes R1 utilizados na *Base Exchange*, informando a disponibilidade do serviço de *Rendezvous*. Após a localização do RVS o requisitor pode continuar sua *Base Exchange* com um parâmetro adicional (REG_REQUEST) em seu pacote I2, que informa sua condição de requisitor do serviço RVS.

3 Outras propostas

Para suportar a mobilidade no plano de dados existem outras propostas, algumas são listadas abaixo:

3.1 Mobile IP

Nesta tecnologia, um endereço estático é atribuído para cada nó móvel (NM), que tem como objetivos identificar e indicar a localização do dispositivo[ABELEM at al. 2007], conhecido como *home address* (HA).

Em um evento de mobilidade (handoff) para outras redes o NM recebe um endereço temporário chamado de *Care-of-Address* (CoA), compatível com a nova localização do nó. O CoA muda a cada evento de mobilidade entre redes.

O *foreing agent* (FA) é responsável por registrar a localização dos NM, assim que estes efetuem o registro.

O *handoff* é gerenciado pelos agentes de mobilidade HA e FA em sentido de cooperação para prover conexão constante.

Se o NM estiver dentro da sua rede original, recebe os pacotes normalmente e responde como um terminal fixo [KROB e BRUNO 2008]. Caso ele esteja em uma rede estrangeira o HA captura os pacotes destinados a ele e encaminha para sua nova localização. Para que isto seja possível, o NM precisa efetuar um registro com sua rede original e informar sua localização ao FA.

Diferentemente do HIP, propõe a resolução da mobilidade provendo a habilidade de comunicar um host móvel utilizando o endereço IP permanentemente

3.2 Mobile Stream Control Transport Protocol (SCTP)

O Mobile STCP ou simplesmente MSTCP, é uma extensão do STCP com mecanismos de configuração dinâmica de endereços IPs. Tendo como principal objetivo explorar as características de *multihome* do STCP. Isso irá permitir o handoff garantindo assim a "mobilidade do terminal"[COSTA 2006].

O SCTP é um protocolo orientado a conexões, com uma elevada eficácia na transferência de dados[LIMA, NAVAS e SILVEIRA 2004]. Além disso, fornece duas novas facilidades em relação aos protocolos de transporte anteriores:

- Multihoming: permite o acesso a determinado destino por múltiplos endereços IP;
- Multistreaming: permite a existência de diversos fluxos independentes de dados sobre a mesma conexão.

Assim como o HIP o SCTP pode utilizar o componentes do IPSec para garantir a segurança na transmissão dos dados [RATOLA 2004].

O uso de multistreams está incluso no SCTP, enquanto no HIP esta transmissão paralelamente de multistreams, segundo [WILTERDINK 2006], pode ser fornecida por camadas superiores.

4 Metodologia

Conforme mencionado anteriormente, este trabalho tem como objetivos a configuração de uma topologia de rede, onde estarão presentes elementos da arquitetura proposta pelo HIP que possibilitam a mobilidade.

Este trabalho irá avaliar a mobilidade do HIP quanto ao aspecto de funcionamento, principalmente entre as suas diferentes mensagem de controle.

Outro experimento será a execução forçada de um *handoff* será medido da seguinte forma: a diferença entre o tempo em que o último pacote de dados foi recebido da rede de origem e o tempo em que o primeiro pacote de dados foi recebido na rede visitada. Esta é uma métrica importante para a avaliação do HIP, e para todos os protocolos que se propõem a resolver a mobilidade, pois dela depende a transparência

para usuários e aplicações. Este experimento é importante para verificação da continuidade das aplicações após a troca de endereço IP.

5 Resultados com Máquinas Virtuais

Parte do trabalho foi configurada uma topologia de rede com máquinas Virtuais com a finalidade de verificar o funcionamento do gerenciamento da mobilidade oferecida pelo HIP.

5.1 Metodologia para Ambiente Virtual de Experimentos

A metodologia utilizada foi a construção de um ambiente Virtual utilizando o VMWare com as seguintes características:

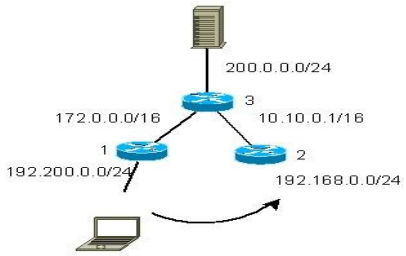

Figura 2: Topologia utilizada nos experimentos no Ambiente Virtual

A Figura 2, mostra a topologia de rede configurada nas máquinas virtuais.

5.2 Objetivos Gerais

Os objetivos gerais para a configuração em um ambiente Virtual foram:

- Verificar o funcionamento da *Base Exchage* sem o serviço de *Rendezvus Server* e seus estágios;
- Disponibilizar uma aplicação entre Cliente e Servidor utilizando *sockets* HIP;
- Verificar o funcionamento do gerenciamento da mobilidade modificando o Cliente da rede 192.200.0.0 para a rede 192.168.0.0, observando a perda de pacotes e suas mensagens de *updates*;
- Verificar a troca de pacotes entre Servidor e Cliente encapsulada em ESP;
- Servir de base para os trabalhos no segundo semestre, quando deverão ser entregue os resultados das pesquisas.

5.3 Resultados Obtidos

A fim de testar o funcionamento do protocolo foi configurada, uma rede onde podemos acompanhar o as mensagens do protocolo. Além disso, foi possível extrair algumas métricas de desempenho.

Para testar a *Base Exchange* foi utilizado o comando *ping* do Cliente para o Servidor e tivemos os seguintes resultados:

Com o WireShark foi possível visualizar as mensagens do *Base Exchange* nas transcorrendo em um tempo de aproximadamente 0,69s e as mensagens encapsuladas ;

Além disso, foi possível visualizar que após acontecer a *Base Exchange* o envio do pacote do Cliente (192.200.0.2) para o servidor (200.0.0.2) foi encapsulado com o ESP.

Para verificar a perda de pacotes, o endereço do Cliente foi modificado com um *script* que automaticamente retira o Cliente da rede 192.200.0.0 e o coloca na rede 192.168.0.0, a aplicação utilizada foi novamente o envio de um comando "ping" com contador finalizando em 20. O seguinte comportamento foi observado

- Uma mensagem de HIP de *update*, informando o novo endereço IP do Cliente ao servidor;
- As perdas foram de 10% dos pacotes;
- O tempo transcorrido para que a troca de pacotes voltasse ao normal foi de aproximadamente 0,98s.

A aplicação que foi utilizada para verificar a continuidade das aplicações após o *Handoff* foi um *Secure Shell* SSH, e novamente o *script* para desconectar de uma rede e conecta-lo a outra foi executado, e os resultados foram os seguintes:

- Como proposto não houve desconexão da aplicação SSH, transcorrendo um tempo de 2,28s.

5.4 Conclusão dos Experimentos

O protocolo HIP com camada *Host Identity Layer* funcionou como o esperado mantendo a conexão entre Cliente e Servidor SSH, com sua tradução dinâmica entre *Host Identifier* em endereços IPs. Suas mensagens de inicialização do *Base Exchage* foram apresentadas como descrito em LAGANIER e EGGERT 2008.

6 Trabalhos Futuros

Como o foco principal dos experimentos foi o funcionamento do HIP, ficando para trabalhos futuros as seguintes sugestões:

- Experimentos em um ambiente sem fio, verificando como métricas a análise do impacto do protocolo em um evento de *Handoff*. Verificar qual o impacto do "Over Head" gerado pelo ESP nativo do protocolo. Perda de Pacotes;

- Compara-lo com o Mobile-IP, verificando qual exerce o menor impacto nas comunicações de entre os *hosts*, principalmente no "*Over Head*" gerado por cada uma das duas tecnologias;

Referências Bibliográficas

WONG, Walter (2006) ***"Proposta de implementação de uma arquitetura para a Internet de nova geração"***. Dissertação (Mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação, Natal 2006.

VMWARE ***"Migrate Virtual Machines with Zero Downtime"***(2008). Disponível em http://www.vmware.com/products/vi/vc/vmotion.html.Acessado em 22/06/2008.

NIKANDER, Pekka; YLITALO, Jukka. (2003) ***"Integrating Security, Mobility and Multi-Homing in a HIP Way"*** Network and Distributed System Security Symposium, San Diego, California, USA.

MOSKOWITZ, R.; NIKANDER, P.(2006) "***Host Identity Protocol (HIP) Architecture"***. IETF Request for Comments, RFC4423. Maio.

WILTERDINK, R.J.W. (2006)"***Host Identity Protocol: A state of the art research"***. Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, the Netherlands. Citeseerx.

KROB, Andréa Collin; BRUNO, Gaspare Giuliano E. (2006) "***Análise de desempenho do handoff no Mobile IP"*** . Escola Regional de Redes *2006* IV. Agosto.

AL-SHRAIDEH, Fayez. (2004) "***Host Identity Protocol"***. Networking Laboratory, Helsinki University of Technology. IEEE. Abril.

LAGANIER, J.; EGGERT, L .(2008) "***Host Identity Protocol (HIP) Rendezvous Extension"*** . IETF Request for Comments, RFC5204. Abril.

LIMA, Carlos Alberto Fróes; NAVAS, José Ricardo Portillo; SILVEIRA, Loreno Menezes da. (2004) "***Tutoriais Banda larga e VOIP: Transporte de Sinalização em Redes IP"***. Disponível em http://www.teleco.com.br. Pg 4. Acessado em 22/06/2008.

KOPONEN, T.; GURTOV, A., NIKANDER, P.,(2005) "***Application Mobility with HIP"***. Disponível em http://infrahip.hiit.fi/papers/appmob.pdf. Acessado em 22/06/2008.

COSTA, Daniel Gouveia. (2006) "***Uma arquitetura baseada em SCTP e SIP parasuporte a aplicações VoIP móveis e a especificação formal do seu módulo de controle".*** Universidade Federal do Rio Grande do Norte - Centro de Tecnologia. Disponível em http://biblioteca.universia.net/. Maio.

RATOLA, Mika. (2004) ***"Which Layer for Mobility? - Comparing Mobile IPv6, HIP and SCTP"***. Helsinki University of Technology Telecommunications Software and Multimedia Laboratory. Citeseer .