Estudo Experimental da Perda de Pacotes em *Soft Handovers* Realizados com SMIP

Ony Kácio Venancio Silva[1], Claudio de Castro Monteiro[2]

[1]Graduando em Sistemas para Internet – IFTO. e-mail: okacio06@gmail.com
[2]Doutor em Engenharia Elétrica – IFTO. e-mail: ccm@ifto.edu.br

Resumo: Este artigo propõe a implementação de um ambiente do SMIP, para estudo e obtenção de dados relevantes sobre a perda de pacotes do protocolo durante o gerenciamento dos *soft handovers*, com apresentação de análise estatística dos resultados obtidos, considerando o envio de *datagramas icmp* na camada de transporte do nó móvel para o nó correspondente.

Palavras–chave: *soft handover*, mobilidade, perda, SMIP

1. INTRODUÇÃO

A grande variedade de dispositivos móveis disponíveis, de tamanhos, formatos e tecnologias diferentes, que em comum possuem a característica de manter conexão com alguma rede, torna a mobilidade algo desejado e necessário. Assim, gerenciar as conexões de rede durante o deslocamento espacial do usuário, que se desconecta de uma rede e conecta–se a outra frequentemente, é imprescindível para que essa experiência seja o máximo imperceptível.

A iniciativa do *Internet Engineering Task Force*(IETF) é a extensão ao protocolo IP, o *Mobile Internet Protocol* (MIP) que permite a movimentação de um nó móvel entre redes sem que as conexões estabelecidas sejam perdidas. Essa iniciativa do IETF é base para muitos estudos mundo afora, grupos que procuram dinamizar o processo de gerenciamento do *handover*, processo no qual o dispositivo móvel fica sem comunicação até que a conexão seja reestabelecida em uma nova rede.

Por este motivo existem diversas variações do MIP, como o HMIP, FMIP, F–HMIP, PMIP e o protocolo base para este trabalho o *Specialized* MIP(SMIP). O SMIP, como as demais variações, propõe reduzir o tempo de descontinuidade experimentado pelo móvel durante sua migração entre redes. [MONTEIRO, 2012]

A descontinuidade dos serviços, durante o processo de gerenciamento do *handover*, inclui o tempo que ele leva para estar reestabelecido na nova rede e quanto ele perdeu de suas conexões ativas durante esse processo de mudança. Este trabalho utiliza como métrica de medida, as perdas no envio de *datagramas icmp*, por meio da aplicação *ping*, durante o processo de *handover*, para que sejam gerados e coletados dados para análise por método estatístico.

A estruturação do trabalho está da seguinte forma: A seção 2 revisa os conceitos relacionados ao MIP e ao SMIP. A seção 3 apresenta uma visão da proposta de implementação do ambiente de testes e dos meios de coleta de dados sobre a perda de *datagramas icmp*, durante o processo de gerenciamento dos *soft handovers* no SMIP. A seção 4 é voltada para a análise da proposta quanto ao seu desenvolvimento. Para finalizar o trabalho, a conclusão resume os principais resultados e aponta novas possibilidades para trabalhos futuros.

2. REFERENCIAL TEÓRICO

Para que a proposta de desenvolvimento do ambiente de testes seja iniciada, é preciso revisar os conceitos do protocolo MIP e do nosso objeto de pesquisa, o protocolo SMIP.

2.1. O PROTOCOLO MIP

O protocolo MIP é uma proposta de mobilidade para o protocolo IP, ou seja, é uma extensão ao protocolo de endereçamento da internet. Cada vez que um nó sai de uma rede para outra, o protocolo IP assume que existe uma rede física relacionada e modifica o seu identificador. Esta alteração do endereço IP, exige que qualquer comunicação estabelecida seja reiniciada, ou seja, ele não mantém as conexões já estabelecidas em sua rede de origem.

ISBN 978-85-62830-10-5

O MIP propõe resolver este problema por meio da técnica de tunelamento. Nesta técnica, o MIP assume que o nó móvel(MN) possuirá dois endereços IP, um é o que ele está registrado na sua rede de origem e que não será modificado, o outro o endereço será o que ele vai adquirir ao visitar outra rede e é chamado de *Care of Address*(CoA), que poderá ser modificado cada vez que ele mude para uma rede que não seja a sua de origem.

O roteador da rede visitada é conhecido como *foreign agent*(FA) e o roteador da rede de origem é o *home agent*(HA) sendo este o responsável pela autenticação e por manter a tabela com os CoAs do nó móvel. Toda vez que o nó móvel sair de sua rede de origem para visitar outra rede, ele deverá enviar uma mensagem ao *home agent*(HA) a partir do seu novo endereço e solicitar a montagem do túnel, para que restabeleça suas conexões iniciadas. A partir daí os dados serão reencaminhados para que o recebimento seja feito pelo túnel, é este o processo do *handover*.

A figura abaixo demonstra como funciona a sinalização do MIPv4:

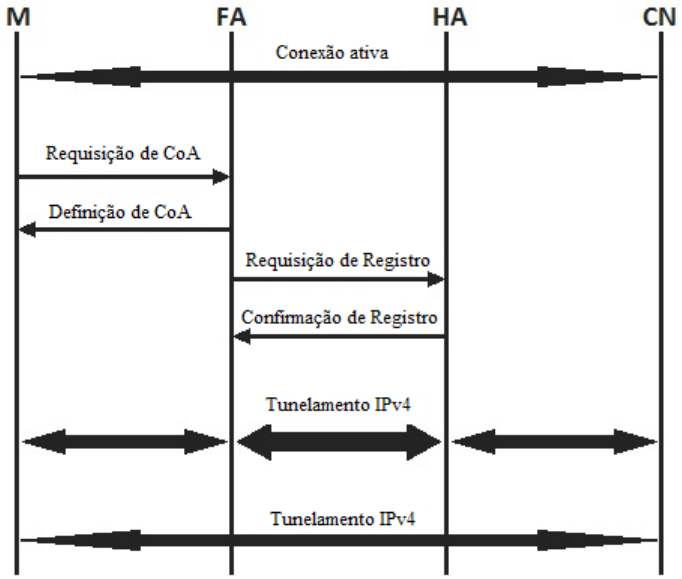

Figura 1 Sinalização do MIPv4 (Adaptado de MONTEIRO)

2.1. O PROTOCOLO SMIP

O SMIP como alternativa ao MIP propõe melhorar o processo de gerenciamento do *handover*, tornando – o mais eficiente e menos perceptível ao usuário do nó móvel. No SMIP parte – se do pressuposto de que o nó móvel tem duas ou mais interfaces de rede disponíveis e que está conectado em pelo menos duas, constituindo assim a sobreposição das redes. Diante desta perspectiva do nó móvel já estar conectado à rede visitada, verificamos que o *home agent*(HA) já conhece pelo menos um CoA, ou seja, para que haja mudança de rede o processo de *handover* não inclui a desconexão e reconexão do nó móvel. Mas apenas a mudança de rota para a rede melhor qualificada a fornecer a conexão e a montagem do túnel entre o *home agent*(HA) e o *correspondent node*(CN). Podemos dizer que esta proposta de protocolo age de forma combinatória das formas preditiva e reativa. Sua sinalização do SMIP é "mais enxuta" do que a sinalização do MIP, fazendo com que o tempo da mudança da rede de origem para a rede visitada seja menor, levando em consideração um número menor de eventos da sinalização, visto que o CoA já é conhecido pelo *home agent*(HA). Na figura 3 observamos o processo de sinalização do protocolo SMIP em sua vesão 4.

ISBN 978-85-62830-10-5

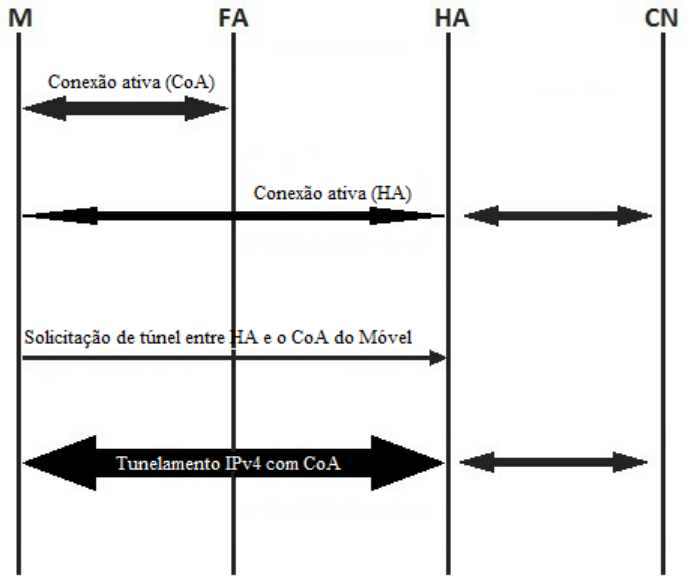

Figura 3 Sinalização do SMIPv4 (Adaptado de MONTEIRO)

Analisando a Figura 1 vista anteriormente e a Figura 3, podemos visualizar as diferenças no processo de *handover*, o que chama atenção é a diminuição de sinais a serem trocados entre o nó móvel e o seu *home agent*(HA).

O funcionamento correto do SMIP depende da implementação de dois módulos: **Módulo Servidor** que atua como *gateway* da rede de origem (HA), tem a função de montar e desmontar o túnel entre o HA e o CoA do nó móvel, além de registrar as mensagens vindas do nó móvel; **Módulo Cliente** que possui a função de verificar as interfaces ativas e registrar no HA seus respectivos endereços IP e solicitar ao HA a montagem e desmontagem do túnel. A Figura 5 abaixo demonstra o modelo de funcionamento destes módulos:

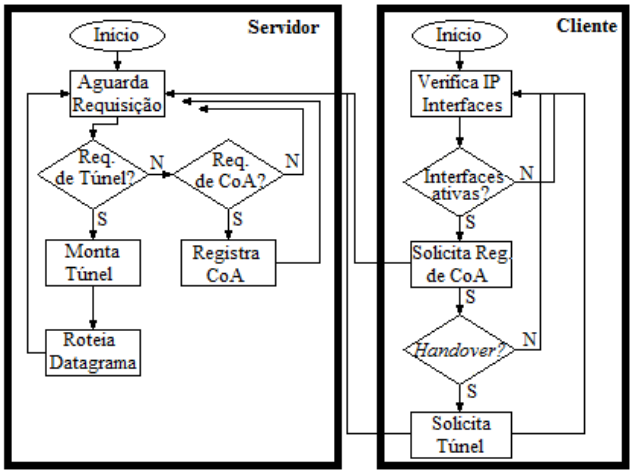

Figura 5 Funcionamento do SMIP (Adaptado de MONTEIRO)

3. A PROPOSTA

A proposta deste trabalho é criar um ambiente de testes, para coletar dados sobre a perda de pacotes do protocolo SMIP. O objetivo é chegar à análise estatística de resultados dos dados coletados. Partindo do pressuposto da efetiva leitura do escrito anteriormente, vamos utilizar as nomenclaturas ao invés dos nomes completos dos agentes do SMIP, assim: HA – *home agent*; FA – *foreign agent*; CN – *Correspondent Node*; MN – *Mobile node*.

ISBN 978-85-62830-10-5

As premissas para o ambiente serão as seguintes:
- O móvel possui duas interfaces aéreas de rede;
- O móvel está conectado a duas redes, a rede do HA e do FA;
- O HA, o FA e o CN estarão conectados por cabo para simular a internet;
- Os testes de perda estarão baseados no envio de *datagramas icmp* do MN para o CN, por meio da aplicação *ping*;
- Os *handovers* serão "forçados" pela aplicação de captura com um tempo programado 15 segundos entre ida e volta;
- O CN também será o *gateway* padrão do HA e do FA.

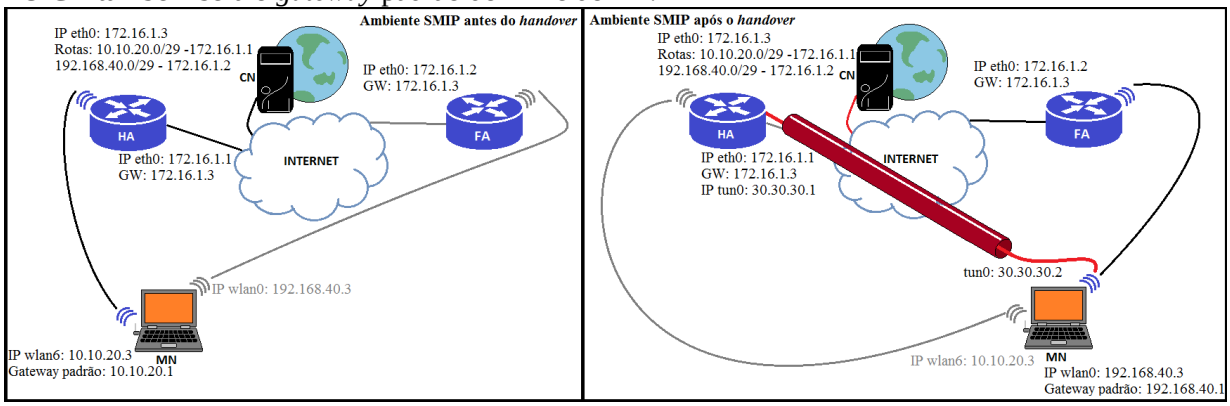

Figura 3 Ambiente de testes

3.1. CONFIGURAÇÃO DO AMBIENTE

Para que o ambiente seja configurado da maneira correta, é necessária a instalação dos sistemas operacionais, dos *softwares* necessários ao SMIP e dos softwares necessários aos *scripts* de coleta e de automatização da configuração do ambiente. As tabelas abaixo descrevem como o ambiente foi preparado.

Tabela 1 - Configurações de *hardware*, para o *Correspondent Node*(CN) - SRVVLC03, *home agent*(HA) - SRVAP01, *foreign agent*(FA), os sistemas operacionais instalados, para o ambiente de testes.

NOME	SISTEMA OPERACIONAL	HARDWARE	PAPEL NO AMBIENTE	INTERFACES
SRVVLC03	Ubuntu Desktop 12.04 32bits	Intel® Celeron(R) CPU 2.80GHz / 3GB / 160GB	CN – GW	eth0
SRVAP01	Ubuntu Server 12.04 32bits	Intel® Pentium 4(R) CPU 2.80GHz / 512MB / 80GB	HA	eth0 / wlan0
SRVAP02	Ubuntu Server 12.04 32bits	Intel® Pentium 4(R) CPU 2.80GHz / 512MB / 80GB	FA	eth0 / wlan0
NOTEMN	Ubuntu Desktop 12.04 32bits	Intel® Core(TM) 2 Duo CPU 2.20GHz / 2GB / 120GB	MN	wlan1 / wlan6
HUB TP LINK	-	HUB 8 PORTAS – 10/100Mbp/s	CONCEN-TRADOR	8 ports

Tabela 2 – Softwares necessários para o funcionamento correto do ambiente, instalados de acordo com o descrito nesta tabela utilizando o comando *apt-get install*.

NOME	COMANDO DE INSTALAÇÃO	APLICAÇÃO
hostapd	apt-get install hostapd	SRVAP01 / SRVAP02 – para que a função de Access Point fosse possível de ser implementada.
dhcp3	apt-get install dhcp3-server dhcp3-common	SRVAP01 / SRVAP02 – Servidor dhcp para que as rede distribuíssem os IPs para o Móvel.
openvpn	apt-get install openvpn	SRVPAP01 / NOTEMN – Para que o túnel seja montado entre o servidor HA e móvel MN.

ISBN 978-85-62830-10-5

gawk	apt-get install gawk	NOTEMN – Pesquisa de palavras em linha de comando, utilizado no script de automação e de testes de *handover*.
gcc	apt-get install gcc -	SRVPAP01 / NOTEMN – Compilador para a aplicação Cliente e para a aplicação Servidor.

Após a instalação dos *softwares* necessários são feitas então as configurações de rede e é dado inicio aos serviços do HA e do MN. A tabela seguinte define os comandos utilizados em cada computador para a configuração da rede, comandos estes que serão adicionados a um *script* na linguagem *python* para que o ambiente possa ser montado da forma automatizada.

Tabela 3 - Configurações dos equipamentos para início dos serviços, esta tabela define os comandos utilizados para configurar os agentes servidores e o cliente utilizados neste trabalho.

NOME	COMANDO	APLICAÇÃO
hostapd	hostapd /etc/hostapd/hostapd.conf	Inicialização do servidor de roteador *wireless, no SRVAP01 o ssid tornou –se REDEHA, já no SRVAP02 o ssid foi ativado como REDEFA.*
dhcpd	dhcpd –cf /etc/dhcp/dhcpd.conf	Inicialização do servidor dhcp nos dois agora roteadores, o SRVAP01 recebeu a rede 10.10.20.0/29, já o SRVAP02 recebeu a rede 192.168.40.0/29
ifconfig	ifconfig <interface> <ip/máscara>	As interfaces de rede com fio do HA, do FA e do CN receberam IPs dentro da rede 172.16.1.0/29. Já as interfaces wlan0 do HA e do FA receberam o IP 1 na rede do *range* configurado anteriormente no servidor *dhcp*.
route	route add default gw <ip_gw> route add –net <rede/máscara> gw <ip>	Este comando foi utilizado na configuração do *gateway* dos servidores do HA e do FA, além é claro do móvel (MN). A rota padrão para o HA e FA é o gateway da rede externa no caso próprio CN atua nesta função, o comando seguido de add –net indica para o CN a qual servidor ele deve direcionar os datagramas de acordo com suas redes.
iptables	Iptables –F ; iptables –t nat -F	Esses comandos foram feitos em todos os computadores para que a tabela do *iptables* estivesse sempre limpa sem nenhuma regra de *nat* para não atrapalhar o funcionamento do HA.
echo	echo <texto ou número>	Este comando está sendo utilizado principalmente para sobrepor texto dos arquivos, um exemplo é a liberação da função *gateway* nos servidores APs da seguinte maneira: echo 1 > /proc/sys/net/ipv4/ip_forward

4. AVALIAÇÃO DA PROPOSTA

O método de análise das perdas do protocolo SMIPv4 no ambiente escolhido, leva em consideração a coleta de dados retirados do envio de *datagramas* do protocolo *icmp* durante o processo de *handover*. O algoritmo do programa de coleta é dado da seguinte maneira: - O programa é iniciado; - Dentro dele está pré definido qual o tamanho da amostra; - Ele entra então entra em um laço que só vai parar quando a quantidade de *handovers* programada for feita; - Dentro do laço ele entra primeiro no *handover* de ida para rede visitada; - É dado inicio ao envio de *datagramas* para o CN por meio do programa *ping* três segundos antes do MN solicitar a mudança, os dados estão sendo salvos e um arquivo de *log*; - O status do arquivo de mudança é modificado e então o programa segue, aguarda mais três segundos; - O processo de envio de *datagramas* é concluído; - Mais alguns

ISBN 978-85-62830-10-5

segundos e os dados estatísticos de envio e perda são coletados; - Mais alguns segundos e os dados são acrescentados no final de outro arquivo que estará gerando o *log* final dos testes; - Aguarda mais alguns segundos para que o processo de solicitação de mudança de rede e a coleta de dados levem 15 segundos ao total; - O laço continua e estes passos são repetidos, mas agora para gerar os dados do *handover* de volta para o HA; - Ao fim da quantidade de *handovers* programada no início é encerrado o programa e os dados estão nos arquivos de *log* gerados durante a execução.

A aplicação fará 30 *handovers* de ida e 30 de volta para que sejam gerados os dados da pré amostra e possamos definir qual o tamanho da amostra que possa ter relevância para o levantamento confiável dos dados sobre a perda do protocolo. Os dados coletados nesta primeira amostra são essenciais para a continuidade do trabalho.

O resultado da amostra inicial pode ser visualizado abaixo no Gráfico 1 e na Tabela 4:

Gráfico 1 – Pré amostra de 30 *handovers* para definir o tamanho real da amostra final

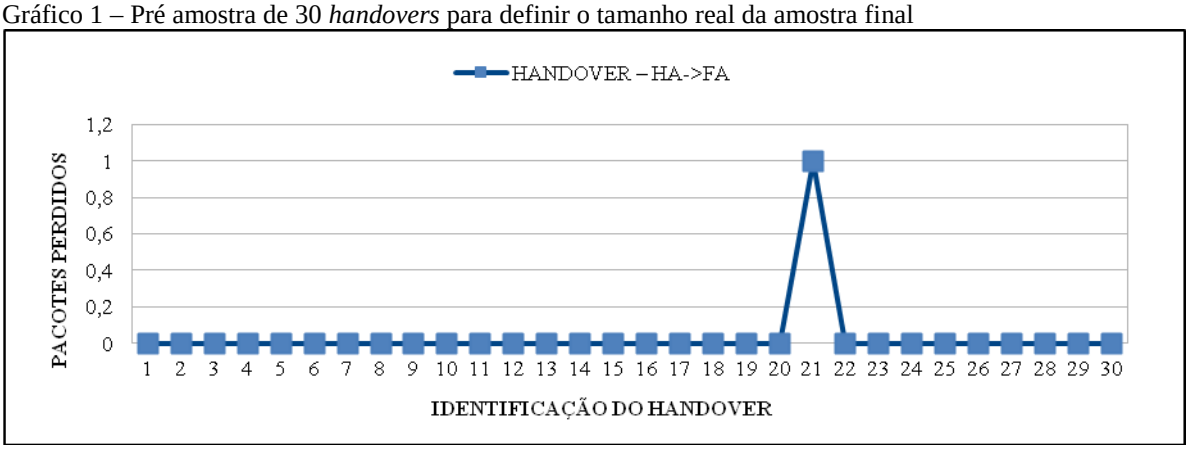

Tabela 4 Coleta de pré amostra feita com 30 *handovers*, a perda (*packet loss*)

MÁXIMO	**1**
MÍNIMO	**0**
MÉDIA	**0,033333333**
DESVIO PADRÃO	**0,182574186**
ERRO	**0,041716283**
TAMANHO DA AMOSTRA	**74**

Podemos observar que no Gráfico 1 a perda foi de um pacote e ocorreu apenas no momento do *handover* 21. Essa pré amostra determinou que o tamanho da amostra final, para que a confiança desejada nos resultados fosse alcançada é de 74 *handovers*. Considerando esse número podemos dizer que se a amostra for maior, a relevância dos resultados aumenta. Portanto que a amostra final seja mais relevante, a quantidade de *handovers* a ser feito deve ser arredondada para 100, a apresentação destes estará na seção de resultados.

5. RESULTADOS

Os resultados finais quanto a perda do protocolo SMIP estão descritos no gráfico e na tabela logo abaixo, a primeira medida que tinha servido como pré – amostra para determinarmos o desvio padrão e então assim podermos calcular o número real de coletas a serem feitas, para que a confiabilidade dos resultados chegasse a 95%, se comparada é possível observar que estão de acordo quanto ao desvio padrão.

A amostra final foi coletada perfazendo um total de 100 *handovers*, para que fosse possível observar melhor a eficiência do protocolo no envio e recebimento de *datagramas icmp*. Os dados

ISBN 978-85-62830-10-5

apresentados no Gráfico 2 e na Tabela 5 logo abaixo, demonstram que a variação da perda é insignificante levando – se em consideração a camada 3 de transporte. Significa que as variáveis de recuperação presentes nas camadas inferiores podem ter sido utilizadas e por este motivo as perdas não foram sentidas na camada três. Ou seja, isto significa que uma aplicação que esteja sendo consumida no momento dos *handovers* pode sim sentir a perda de pacotes de maneira mais significativa, mas para que isso seja comprovado são necessários testes com aplicações para saber qual o impacto dos *handovers* na descontinuidade dos serviços.

Gráfico 2 Gráfico das perdas dentro de uma amostra de 100 *handovers*

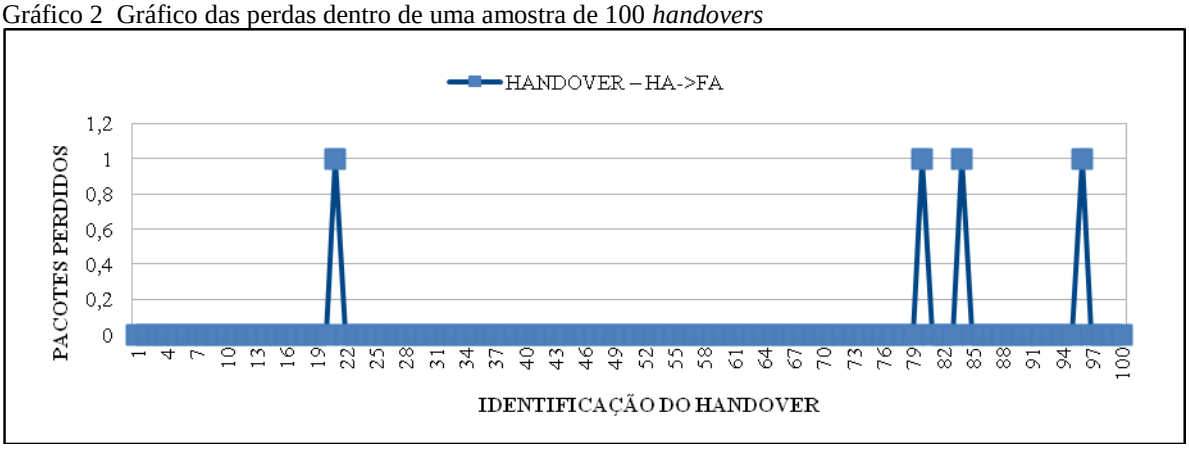

Tabela 5 – Dados de perda dentro de uma amostra de 100 *handovers*

MÁXIMO	**1**
MÍNIMO	**0**
MÉDIA	**0,04**
DESVIO PADRÃO	**0,196946386**
ERRO	**0,041716283**
TAMANHO DA AMOSTRA	**86**

Observadas as tabelas e gráficos de resultados obtidos com os testes finais, podemos constatar que os dados da perda realmente estão dentro de uma perspectiva que torna o protocolo muito eficiente quanto ao envio de *datagramas icmp*. Os dados levantados na pré amostra e na amostra final, foram consistentes e com o tratamento estatístico formado podemos dizer que caso outro pesquisador refaça os testes seguindo o modelo deste trabalho ele terá o mesmo resultado, seja qual for o tamanho das amostras.

6. CONCLUSÃO E TRABALHOS FUTUROS

O funcionamento do SMIPv4 é interessante e abre uma série de possibilidades que podem ser exploradas visto sua condição de ser *opensource e* utilizar *softwares* também *opensource* em sua implementação. As aplicações criadas que se utilizem dos seus conceitos, para propiciarem ao usuário algo melhor do que as propostas existentes na atualidade devem ser melhor aceitas diante de estudos como este, que por métodos estatísticos possam medir sua eficiência. Os dados da perda de pacotes do SMIPv4 levantados neste trabalho, demonstraram uma grande eficiência do protocolo, visto que os testes realizados demonstraram que a perda dos *datagramas icmp* foi imperceptível levando – se em consideração a camada de transporte, o que não quer dizer que o usuário não perceberia caso estivesse consumindo uma aplicação de *streaming* de vídeo como o VLC por exemplo. O que é desejável, do ponto de vista da consolidação do protocolo, é que mais trabalhos sejam realizados evoluindo para testes com aplicações como o VLC, que evidenciem o desempenho do protocolo na percepção do

ISBN 978-85-62830-10-5

usuário enquanto consumidor de aplicações. A conclusão deste estudo é que o protocolo se mostrou eficiente e isso foi comprovado por métodos estatísticos de amostras de diferentes tamanhos.

7. REFERÊNCIAS

IKEDA, André Tadashi Eurico; PAULA, Clelio de; HORTA, Felipe Figueira. **IP Móvel**. Disponível em: < http://www.gta.ufrj.br/grad/09_1/versao-final/ipmovel/index.html > Acesso em: 08 jul. 2012.

JUNIOR, Eduardo C. Gonçalves. **Redes IP Móveis**. Disponível em: < http://www.gta.ufrj.br/grad/06_2/eduardo/index.html > Acesso em: 08 jul. 2012.

LOPES, Danilo Vieira; SANTOS, Jaime Batista. **Análise Estatística da Latência e Perda de Pacotes numa Rede de Computadores.** Disponível em: < http://www.dimap.ufrn.br/~sbmac/ermac2008/Anais/Resumos%Estendidos/Analise%Estatistica_danilo.pdf > Acesso em: 18/07/2012.

MONTEIRO, Claudio de Castro. **Um Ambiente para Apoio à Integração de Redes Sem Fio Heterogêneas.** Tese de Doutorado. Engenharia Elétrica. UnB. 2012.

PEREIRA, Helder Cleber Almeida. **Comparativo entre protocolos de gerenciamento de mobilidade.** In: XI Encontro de Estudantes de Informática do Tocantins, 2009, Palmas. Anais do XI Encontro de Estudantes de Informática do Tocantins. Palmas: Centro Universitário Luterano de Palmas, 2009. p. 103-111. Disponível em: < http://www3.ulbra-to.br/eventos/encoinfo/2009/Anais/Comparativo_entre_protocolos_de_gerenciamento_de_mobilidade.pdf > Acesso em 08/06/2012.

PERKINS, C. **Mobility Support for IPv4.** IETF RFC 3220 (2002). Disponível em: < http://www.faqs.org/rfcs/rfc3220.html > Acesso em: 01 ago. 2012.

ISBN 978-85-62830-10-5