Estudo comparativo de mecanismos para conformação de tráfego em redes IEEE 802.16

Geovane Griesang[1], Rafael Kunst[2]

[1]Universidade de Santa Cruz do Sul (UNISC) – Santa Cruz do Sul – RS – Brasil

[2]Departamento de Informática – Universidade de Santa Cruz do Sul (UNISC)
Santa Cruz do Sul – RS – Brasil

geovane.griesang@gmail.com, rkunst@unisc.br

Abstract. *The great diversity and the portable device advancement, together with the need to obtain and exchange information at any time and place, stimulates the increased use of wireless networks, especially in the context of metropolitan networks. This paper presents an approach focused on providing quality of service (QoS) in IEEE 802.16 networks. Thus, studies are techniques for traffic shaping and policing, aiming to ensure the maintenance of the service established for the connection between the source and provider of services. Accordingly, there will be a comparative study between the performance of algorithms for traffic shaping based on techniques of Leaky Bucket and Token Bucket. Results show the rate of acceptance of connections for various scenarios encountered in the context of IEEE 802.16 networks.*

Resumo. *A grande diversidade e o avanço de aparelhos portáteis, aliado à necessidade de obter e trocar informações a qualquer hora e lugar, estimula a crescente utilização das redes sem fio, em especial no contexto das redes metropolitanas. Este trabalho apresenta uma abordagem focada em prover qualidade de serviço em redes IEEE 802.16. Para tanto, estuda-se técnicas de conformação e policiamento de tráfego, com objetivo de garantir a manutenção do contrato de serviço estabelecido durante a conexão entre a fonte e o provedor de serviços. Nesse sentido, realiza-se um estudo comparativo entre o desempenho de algoritmos para conformação de tráfego baseados em técnicas de Token Bucket e Leaky Bucket. Resultados mostram a taxa de aceitação de conexões para diversos cenários encontrados no contexto das redes IEEE 802.16.*

1. Introdução

Atualmente, a necessidade de obter informações a qualquer hora e em qualquer lugar, aliada ao crescente uso de dispositivos móveis, estimula o surgimento de novas tecnologias, cada vez mais sofisticadas e flexíveis, compatíveis com o grau de evolução dos sistemas. A solução dessas necessidades contribui para a inclusão digital de povos distantes das metrópoles, como por exemplo, as pessoas que residem nas zonas rurais.

Por não possuírem uma infra-estrutura adequada, muitos locais não conseguem estabelecer conexão com a Internet. Neste contexto, o cenário atual exige a expansão das redes de computadores e dos serviços de banda larga oferecidos, pois os

mecanismos utilizados, além de serem limitados pela distância geográfica, também possuem um elevado custo para implantação (CHOI e CHOI 2005).

Diante dessas características, as redes de acesso a banda larga sem fio (*Broadband Wireless Access* – WBA) e as redes metropolitanas sem fio (*Wireless Metropolitan Area Network* – WMAN) baseadas no padrão IEEE (*Institute of Electrical and Electronics Engineers*) 802.16, aparecem como uma alternativa aos sistemas de conexão tradicionais (cabo e *Digital Subscriber Line* - DSL) e tornam-se uma solução tecnicamente e financeiramente viável para tais localidades (GHOSH et al. 2005).

O grupo IEEE 802.16 foi criado para padronizar as camadas física e de controle de acesso ao meio das redes metropolitanas sem fio. Sendo assim, a norma IEEE 802.16e (IEEE-802.16 2005) define a interface aérea para sistemas fixos e móveis em redes metropolitanas, como uma solução para acesso sem fio de banda larga. Uma preocupação do grupo, é oferecer garantias para o tráfego de voz, vídeo e dados com QoS (Q*uality of Service*), sem prejudicar as demais SSs (*Subscriber Station*). Este padrão foi projetado com recursos de priorização, controle/garantia de banda e QoS em todos os dispositivos (LIMA et al. 2005).

Portanto, o padrão IEEE 802.16 define cinco classes com diferentes requisitos de serviços (IEEE-802.16 2005, LIMA et al. 2005): Serviço garantido (*Unsolicited Grant Service* – UGS); aplicações de tempo real com taxa variável de bits e supressão de silêncio (*Extended Real Time Polling Service* - ertPS); aplicações de tempo real com taxa variável de bits (*real-time Polling Service* - rtPS); aplicações sem requisitos de tempo real (*non-real time Polling Service* - nrtPS); tráfego de melhor esforço (*Best Effort* - BE).

Apesar dessas especificações, não é definido pela norma um mecanismo de gerenciamento para garantia de QoS. As cinco classes de serviço permitem a distinção entre fluxos de tráfego e a possibilidade de um tratamento diferenciado para cada fluxo. Entretanto, simplesmente classificar os fluxos não garante que eles recebam um serviço com a QoS desejada (BOTH et al. 2006).

Procurando atender essas especificações, este presente trabalho tem como objetivo principal o estudo e a implementação de algoritmos para conformação e policiamento de trafego. Em uma topologia PMP (*Point to Multi-Point*), a BS (*Base Station*) é o nó central que coordena toda a comunicação e as SSs se localizam a diferentes distâncias das BS. A BS pode estar conectada a outra infra-estrutura de rede, como por exemplo, um ISP (*Internet Service Providers*), possibilitando uma extensão dos serviços oferecidos aos usuários (BOTH et al. 2006).

Com isso, a Seção 2 apresenta a conformação e policiamento de tráfego em redes no padrão IEEE 802.16. Por outro lado, a Seção 3 apresenta a modelagem dos algoritmos, enquanto a Seção 4 mostra os resultados obtidos através das simulações. Por fim, a Seção 5 apresenta as considerações finais.

2. Conformação e policiamento de tráfego no padrão IEEE 802.16

Os mecanismos para a conformação e policiamento de tráfego possuem objetivos semelhantes: identificar e reagir a violações de perfis de tráfego. Porém, diferem na maneira como respondem à violação (SANTANA 2006). Com isso, a principal tarefa do policiamento é impedir que a SS viole os perfis de tráfego

estabelecidos durante a conexão com a BS, com o objetivo de impedir abusos que possam prejudicar outras SSs (LI e STOL 2002, LEKCHAROEN e FUNG 2007).

Por outro lado, os mecanismos de conformação de tráfego, fazem uso de filas para armazenar o tráfego excedente (ao invés de descartá-lo como ação principal). O principal objetivo é encaminhar todo o tráfego que chega à interface, porém de forma disciplinada, para que a taxa de transmissão resultante esteja de acordo com o perfil pré-definido (SANTANA 2006).

Os algoritmos formam implementados com base no conformador de tráfego TB de Li e Stol (2002) e no conformador de tráfego LB de Lekcharoen e Fung (2007). Já o policiador de tráfego foi baseado no algoritmo RNC de Li e Stol (2002).

3. Modelagem

Inicialmente, o tráfego é gerado com base em cinco modelos de tráfego: HTTP, FTP, Vídeo clipe, VoIP com supressão de silêncio e VoIP sem supressão de silêncio. Em seguida, esse tráfego é encaminhado para a função de conformação de tráfego, que por sua vez, o classifica e o fornece para a função de policiamento de tráfego.

O funcionamento do conformador TB é demonstrado na Figura 1. Inicialmente, o pacote tem o seu tamanho comparado ao valor do *bucket b*, que indica o número total de oportunidades de transmissão. Se o tamanho do pacote for maior que o valor de *b*, o pacote é marcado como não compatível. Caso contrário, é um pacote compatível.

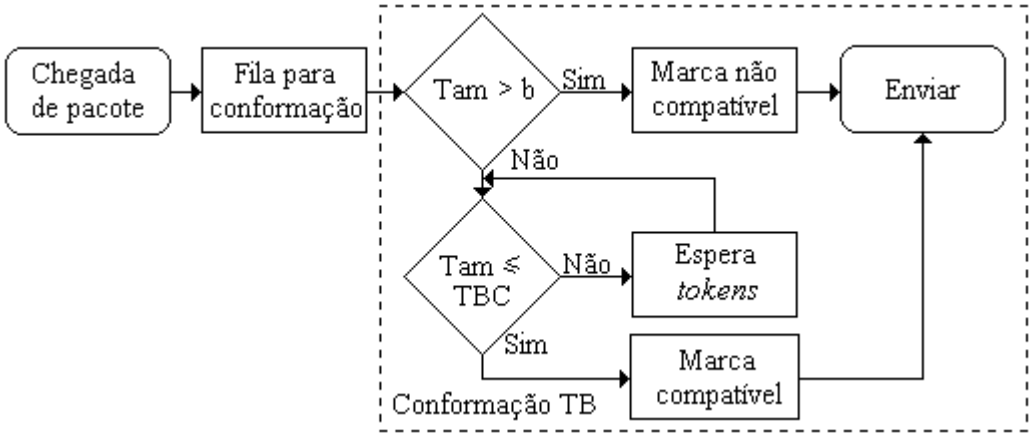

Figura 1 – Funcionamento do conformador de tráfego TB

Também há uma variável interna, chamada de TBC *(Token Bucket Counter)*, usada para registrar a qualquer momento o número restante de *tokens*. Já a taxa r representa a taxa de reposição do *token*. Com isso, se o pacote for maior que o valor de *TBC*, o mesmo deve esperar até que hajam *tokens* suficientes para a transmissão. Isso pode ocorrer após uma ou mais atualizações do valor de *TBC* (*TBC = TBC + r*). Essas atualizações geram um atraso na conformação do pacote, porém, quando esse pacote for menor ou igual ao valor de *TBC*, ele é liberado e marcado como compatível.

Por outro lado, o funcionamento do conformador de tráfego LB implementado é demonstrado na Figura 2. Esse algoritmo possui um *bucket* de tamanho *b* e uma variável interna chamada *LBC* (*Leaky bucket Counter*), que por sua vez, especifica a ocupação do *bucket b*. A primeira tarefa do mecanismo é verificar a variável interna *LT (Last Time)*, responsável por guardar o tempo de chegada do último pacote transmitido. Se o

valor de *LT* for igual a zero, essa variável recebe o tempo de chegada do pacote em conformação, representado por *T* (ALBERTI 2003).

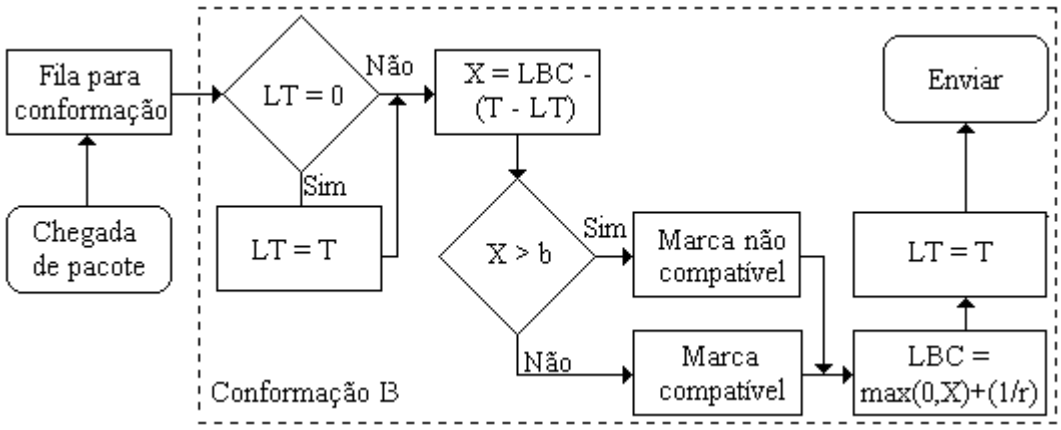

Figura 2 – Funcionamento do conformador de tráfego LB

Uma variável *X* é usada para guardar o valor de *LBC*, subtraído das variáveis *T* e *LT (X = LBC - T - LT)*. Em seguida, a variável *X* é comparada com o valor de *b*. Se *X* for maior que *b*, o pacote é considerado compatível, caso contrário, é considerado não compatível. Após a classificação do pacote, o valor de *LBC* é atualizado por *X*, mais 1/*r*, onde *r* é a taxa de pico dos pacotes desejados para conexão. Por fim, a variável *LT* é atualizada com o valor de *T* (ALBERTI 2003).

Por fim, um policiador RNC foi implementado e o seu funcionamento pode ser observado através da Figura 3. A primeira análise do algoritmo é referente ao congestionamento, ou seja, se a rede não está congestionada no momento em que um pacote chega, o mesmo é aceito. Com isso, tanto os pacotes compatíveis quanto os não compatíveis são aceitos. Porém, quando a rede está congestionada, o algoritmo descarta os pacotes não compatíveis preferencialmente. Nesse caso, se o pacote em questão é não compatível, o mesmo é imediatamente descartado. No entanto, se o pacote é compatível, o algoritmo verifica se há pacotes não compatíveis na fila em policiamento para serem descartados. Havendo um pacote não compatível, ele é descartado. Caso contrário, o pacote compatível é descartado.

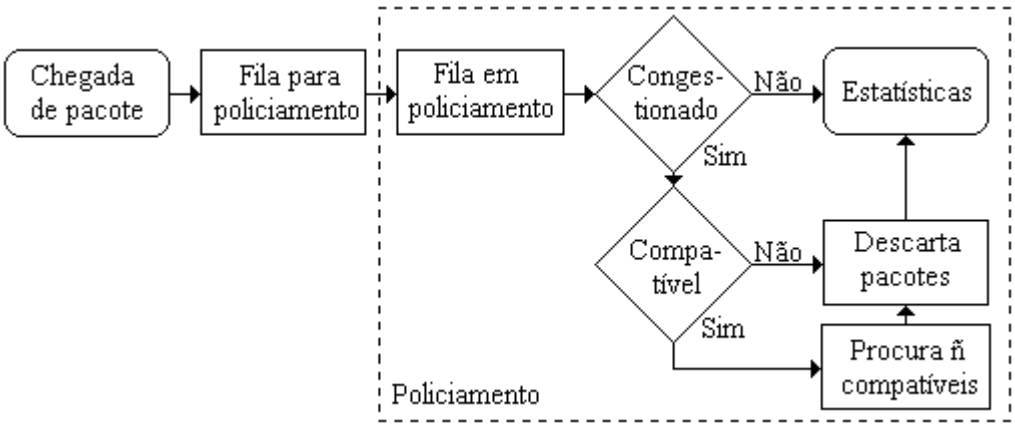

Figura 3 – Funcionamento do policiamento de tráfego

Para a elaboração das simulações foram utilizados dois softwares: LabVIEW (NI 2008) e MATLAB (MATHWORKS 2009). O LabVIEW foi utilizado para a implementação dos algoritmos, enquanto o MATLAB foi usado para na geração dos

modelos de tráfego. Com isso, é possível a execução das simulações e análise dos resultados, conforme apresentado na próxima Seção.

4. Resultados

O fluxo de tráfego para a conformação foi gerado para as cinco classes de serviço especificadas no padrão IEEE 802.16e: VoIP sem supressão de silêncio (UGS); VoIP com supressão de silêncio (ertPS); vídeo clipe (rtPS); FTP (nrtPS); e HTTP (BE). Também foi variada a quantidade de SSs, a taxa r e o tamanho do *bucket*. Para o policiamento de tráfego, foram estabelecidos percentuais de congestionamento e de tamanho para a fila em policiamento. A taxa r também foi utilizada e variada para a execução das simulações. É importante destacar que os dados foram coletados com base em um intervalo de confiança de 95%.

A partir do gráfico apresentado pela Figura 4, é possível verificar o impacto do tamanho do *bucket* sobre os conformadores de tráfego implementados. A Figura 4.A apresenta o conformador de tráfego TB, enquanto a Figura 4.B apresenta o conformador de tráfego LB. É importante destacar que, cada SS possui uma conexão. Nesse caso, 30 SSs possuem 30 conexões. Com isso, para cada análise, apenas um tipo de modelo de tráfego é gerado para cada SS. Ambas simulações foram executadas para 30 SSs e para os tamanhos de *bucket* com 5.000 bits, 8.221 bits, 10.865 bits e 12.000 bits.

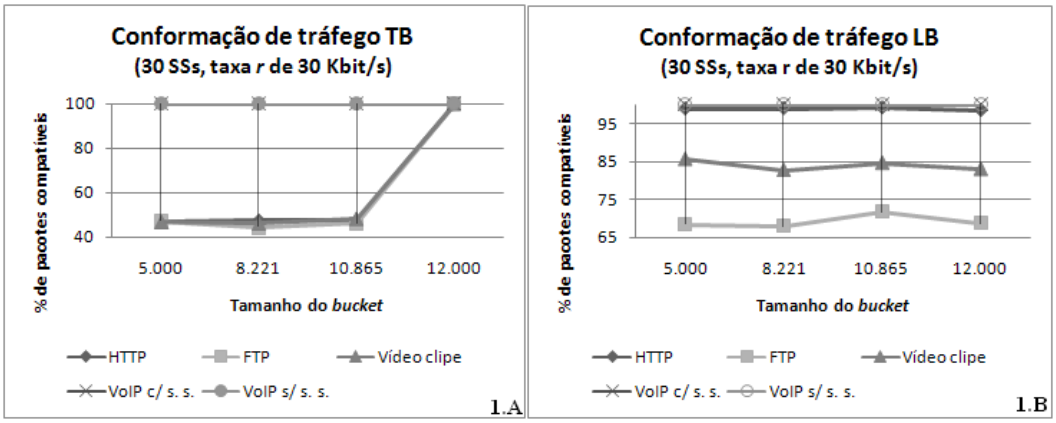

Figura 4 – Gráfico do impacto do tamanho do *bucket* sobre os conformadores

Os resultados da Figura 4 foram gerados com base nos dados apresentados na Tabela 1. Com isso, pode-se concluir que, no conformador de tráfego TB, o tamanho do *bucket* é determinante para que os pacotes possam ser classificados como compatíveis. Isso pode ser justificado pela variação de resultados entre os modelos, onde o modelo de tráfego FTP obteve a maior variação entre os resultados, com 55,8%.

Tabela 1 – Tabela do impacto do tamanho do *bucket* sobre os conformadores

	Conformador TB (%)				Conformador LB (%)			
	5.000	8.221	10.865	12.000	5.000	8.221	10.865	12.000
HTTP	46,65	47,24	47,18	100	98,93	99,02	99,21	98,53
FTP	46,94	44,2	45,82	100	68,34	68,08	71,67	68,79
Vídeo clipe	46,79	46,11	48,33	100	85,62	82,74	84,61	83,02
VoIP c/ s. s.	100	100	100	100	100	100	100	100
VoIP s/ s. s.	100	100	100	100	100	100	100	100

A partir do gráfico apresentado pela Figura 5, é possível verificar o impacto da taxa *r* sobre a conformação de tráfego TB e LB. A Figura 5.A apresenta os resultados para o conformador de tráfego TB, enquanto a Figura 5.B apresenta os resultados para o conformador e tráfego LB. Ambas as simulações foram executadas para 30 SSs e para o tamanho de *bucket* igual a 10.865 bits.

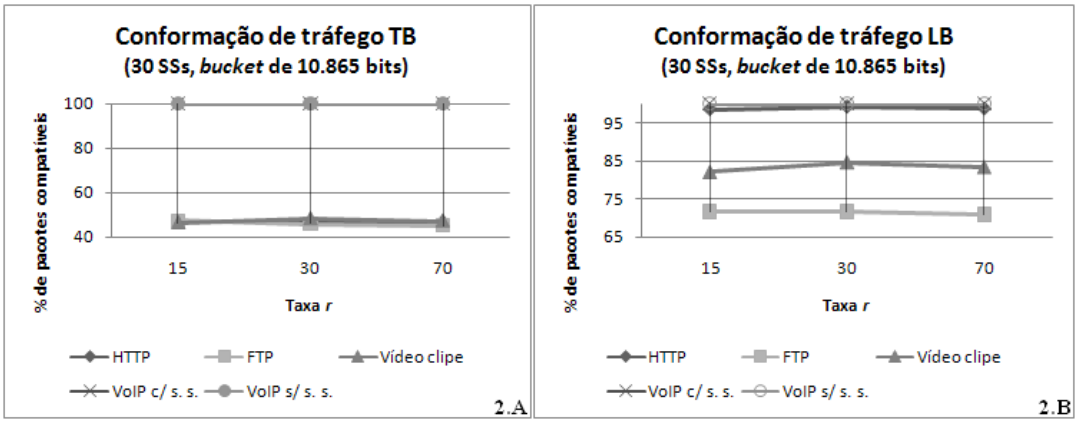

Figura 5 – Gráfico do impacto da taxa r sobre os conformadores

Os resultados da Figura 5 foram gerados com base nos dados apresentados pela Tabela 02. Com isso, pode-se concluir que, a taxa r não é determinante para o número de pacotes compatíveis em um conformador TB. O modelo de tráfego FTP obteve a maior variação de resultados para a taxa r, com uma variação máxima de 2,22% de pacotes compatíveis. Isso pode ser justificado pelas características do conformador de tráfego TB. Esse conformador define um pacote como sendo compatível ou não compatível, apenas através do tamanho do *bucket*. A taxa r para o conformador de tráfego TB é utilizada para reposição de *tokens*.

Tabela 2 – Tabela do impacto da taxa r sobre os conformadores

	Conformador TB			Conformador LB		
	15 Kbis/s	30 Kbis/s	70 Kbis/s	15 Kbis/s	30 Kbis/s	70 Kbis/s
HTTP	46,88	47,18	47,02	98,54	99,21	98,71
FTP	47,38	45,82	45,16	71,56	71,67	70,95
Vídeo clipe	46,44	48,33	47,31	82,02	84,61	83,37
VoIP c/ s. s.	100	100	100	100	100	100
VoIP s/ s. s.	100	100	100	100	100	100

Ainda com base nos resultados apresentados na Tabela 2, pode-se perceber que, mesmo variando a taxa r, os resultados não apresentam uma variação significativa no conformador LB. O modelo de tráfego FTP apresenta a maior variação, em 2,59%. Com isso, é possível observar que, o desempenho do algoritmo LB não depende da taxa r. No entanto, como já visto na análise do impacto do tamanho do *bucket*, o tempo de chegada do pacote é determinante para o número de pacotes compatíveis.

A partir do gráfico apresentado pela Figura 6, é possível verificar a probabilidade de descarte dos pacotes sobre o policiador de tráfego RNC. A Figura 6.A apresenta os resultados para os pacotes compatíveis descartados, enquanto a Figura 6.B apresenta os resultados para os pacotes não compatíveis descartados. Ambas as simulações foram executadas para uma fila em policiamento com tamanho de 40% do

total de pacotes. Os resultados também são apresentados conforme a variação do percentual de congestionamento, que varia em 10%, 20%, 30% e 40%.

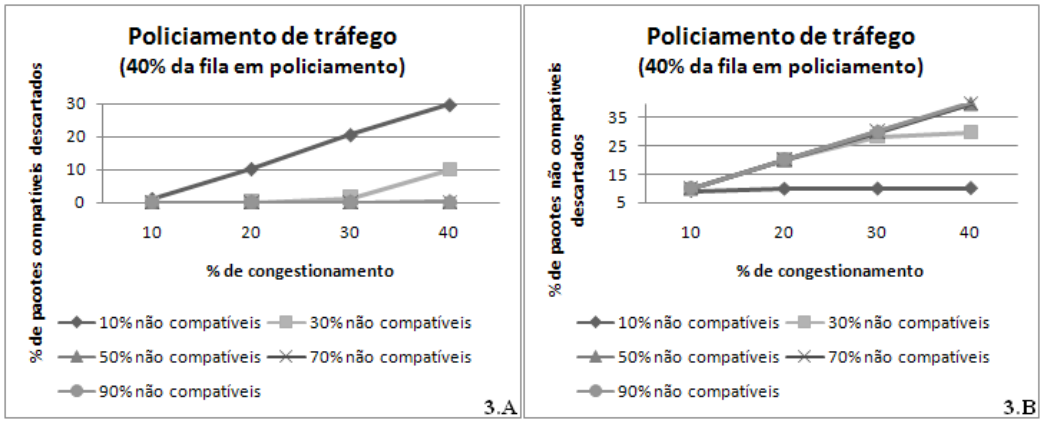

Figura 6 – Gráfico com a análise da probabilidade de descarte dos pacotes

Os resultados da Figura 6 foram gerados com base nos dados da Tabela 3. Com isso, é possível observar que, o percentual de congestionamento é determinante para o descarte de pacotes compatíveis e não compatíveis. Quanto maior o congestionamento, maior o descarte de pacotes. Por outro lado, quanto maior o número de pacotes não compatíveis existentes na rede, maior a probabilidade dos pacotes não compatíveis serem descartados. Tais resultados se justificam, uma vez que, o policiador implementado descarta preferencialmente os pacotes não compatíveis.

Tabela 3 – Tabela com a análise da probabilidade de descarte dos pacotes

	% compatíveis descartados				% não compatíveis descartados			
	10	20	30	40	10	20	30	40
10% ñ c.	1,02	10,15	20,49	29,63	9,07	9,07	9,93	10,1
30% ñ c.	-	0,14	1,45	9,85	9,92	20,03	28,55	29,83
50% ñ c.	-	0,03	0,07	0,19	10,00	20,01	29,97	39,81
70% ñ c.	-	-	-	0,03	10,04	20,06	29,97	39,88
90% ñ c.	-	-	-	-	9,95	20,21	30,00	40,1

Por fim, com base nas simulações e resultados obtidos, pode-se chegar a algumas considerações finais, assim como apresentado na Seção 5.

5. Considerações

Com base nos algoritmos estudados e implementados, é possível a avaliação dos mecanismos de conformação e policiamento de tráfego propostos por Li e Stol (2002) e Lekcharoen e Fung (2007). Através dessas análises, pode-se concluir que, ambos os conformadores de tráfego apresentam um bom desempenho para os modelos de tráfego VoIP com e sem supressão de silêncio, uma vez que, priorizam tais modelos. Também é importante destacar que, para os modelos HTTP, FTP e vídeo clipe, o conformador LB apresenta melhor desempenho do que o conformador TB.

Também é possível concluir que, o policiador de tráfego RNC apresenta um bom desempenho, descartado primeiramente os pacotes não compatíveis. Com isso, o tráfego de compatíveis é priorizado.

Por fim, trabalhos futuros podem ser realizados com base nesse trabalho: estudo do impacto da conformação de tráfego na conformação dos pacotes compatível maiores que o TBC; análise do impacto sofrido pelo policiador de tráfego ao procurar um pacote não compatível na fila em policiamento; e adaptações aos mecanismos desenvolvidos com a finalidade de buscar melhorias no desempenho dos mesmos.

6. Referências

ALBERTI, A. M., "Desenvolvimento de Modelos de Simulação para a Análise de Qualidade de Serviço em Redes ATM", Universidade Federal de Campinas (UNICAMP), Tese de doutorado submetida à Faculdade de Engenharia Elétrica e de Computação, Departamento de comunicações. Campinas/SP, abril de 2003.

BOTH C. B., KUNST R. e ROCHOL J., "Acesso de Banda Larga Sem-fio (WBA) e Redes Metropolitanas Sem-fio (WMAN) baseados no padrão IEEE 802.16 (WiMAX)", IV ERRC (Escola Regional de Redes de Computadores). SBC (Sociedade Brasileira de computação), Passo Fundo/RS, 2006.

CHOI Y. e CHOI S., "*LLC-level FEC scheme in IEEE 802.11 WLAN*". IEEE APWCS'2005, Hokkaido, 2005.

GHOSH, A.,WOLTER, D., ANDREWS, J., e CHEN, R.. "*Broadband wireless access with WiMAX/802.16: Current performance benchmarks and future potential*". IEEE Communications Magazine, 2005, pp. 129-136.

IEEE-802.16. "*IEEE standard for local and metropolitan area networks - part 16: Air interface for fixed and mobile broadband wireless access systems*". IEEE Std. 802.16-2005, 2005.

LEKCHAROEN S. e FUNG, C. C.. "*An Adaptive Fuzzy Control Traffic Shaping Scheme over Wireless Networks*", 2007, pp 177-182.

LIMA, L. DOS SANTOS, SOARES, L. F. G., ENDLER M., "WiMAX: Padrão IEEE 802.16 para Banda Larga Sem Fio". Rio de Janeiro, Pontifícia Universidade Católica do Rio de Janeiro - PUC, 2004.

LI F.Y. e STOL N., "*QoS Provisioning using Traffic Shaping and Policing in 3rd-Generation Wireless Networks*", 2002, pp. 139-143.

MATHWORKS, The MathWorks. Entidade desenvolvedora da ferramenta MATLAB (MATrix LABoratory). Página oficial disponível em http://www.mathworks.com/. Acessado em Junho, 2009.

NI, National Instruments. Entidade desenvolvedora da ferramenta LabVIEW (Laboratory Virtual Instrument Engineering Workbench). Página oficial disponível em http://www.ni.com/labview/. Acessado em Novembro, 2008.

SANTANA, F. L.. Proposta de Referência para Projetos de Qualidade de Serviço (QoS) em Redes Corporativas, Universidade Salvador – UNIFACS, 2006.