

UNIVERSIDADE FEDERAL DE GOIÁS
ESCOLA DE ENGENHARIA ELÉTRICA E COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

**Algoritmo de Policiamento de Tráfego para Redes OFDM/TDMA
WiMAX Baseado em Modelagem Multifractal e Cálculo de Rede**

Josemar Alves dos Santos Junior

Orientador: Prof. Dr. Flávio Henrique Teles Vieira.

Goiânia
2011

Josemar Alves dos Santos Junior

**Algoritmo de Policiamento de Tráfego para Redes OFDM/TDMA
WiMAX Baseado em Modelagem Multifractal e Cálculo de Rede**

Dissertação apresentada ao Programa de **Pós-Graduação Strictu Sensu** da Escola de Engenharia Elétrica e de Computação da Universidade Federal de Goiás, para obtenção do título de **Mestre em Engenharia Elétrica e de Computação**.

Área de Concentração: Engenharia da Computação

Linha de Pesquisa: Telecomunicações

Orientador: Prof. Dr. Flávio Henrique Teles Vieira.

Dados Internacionais de Catalogação-na-Publicação (CIP)
(GPT/BC/UFG)

Santos Junior, Josemar Alves
Algoritmo de policiamento de tráfego para redes OFDM/TDMA
S237a WiMAX baseado em modelagem multifractal e cálculo de rede
[manuscrito] / Josemar Alves dos Santos Junior. – 2011.
135f. : il.

Orientador: Prof. Dr. Flávio Henrique Teles Vieira
Dissertação (Mestrado) – Universidade Federal de Goiás, Escola
de Engenharia Elétrica e Computação, 2011.

Bibliografia

Inclui lista de figuras, abreviaturas, siglas e tabelas.

Apêndice.

1. Algoritmo de policiamento 2. Análise de rede. 3. Modelagem
Multifractal. 4. Cálculo de rede. I. Título

CDU: 004.021

Josemar Alves dos Santos Junior

**Algoritmo de Policiamento de Tráfego para Redes OFDM/TDMA
WiMAX Baseado em Modelagem Multifractal e Cálculo de Rede**

Dissertação defendida e aprovada em 29 de setembro de 2011, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Flávio Henrique Teles Vieira.
Presidente da Banca

Prof. Dr. Sibelius Lellis Vieira
PUC - Goiás

Prof. Dr. Leonardo da Cunha Brito
UFG

Prof. Dr. Marcos Antônio de Sousa
UFG

AGRADECIMENTOS

Gostaria de expressar meus agradecimentos:

A Deus pela realização de mais um sonho.

Ao professor e orientador Flávio Henrique Teles Vieira pelo apoio, incentivo e dedicação para o cumprimento deste trabalho.

Aos meus pais, Josemar e Vera e irmão Adriano pela dedicação, carinho e suporte valiosos e por sempre apostarem em mim.

À minha esposa Juliana e meus filhos Thales e Luisa, pelo apoio e compreensão dos momentos que faltei com eles.

À minha família e amigos que me incentivaram a chegar até aqui.

Ao Prof. Clodoaldo Valverde e Angélica Fleury por terem apoiado meu ingresso ao Mestrado.

Aos membros da banca pelas sugestões apresentadas.

Aos colegas e amigos do Mestrado que de uma forma ou de outra fizeram parte dessa história, em especial aos dedicados amigos Leonardo Alves e Flávio Rocha, pela força e companheirismo.

“Os que se encantam com a prática sem a ciência são como os timoneiros que entram no navio sem timão nem bússola, nunca tendo certeza do seu destino.”
Leonardo da Vinci

RESUMO

A modelagem multifractal tem se mostrado mais apropriada para descrever algumas características encontradas nos fluxos de tráfego de redes reais que outros modelos, tais como o modelo de Poisson e Markov. Este trabalho investiga o comportamento dos algoritmos de policiamento baseados em modelagem de tráfego (Balde Furado, Balde Furado Fractal, Balde Furado Multifractal Gaussiano) em relação à utilização do *buffer*, eficiência em descrever o tráfego acumulado (processo envelope) e descarte de pacotes e perda de dados (*bytes*). Primeiramente, compara-se o processo envelope dos algoritmos de policiamento considerados e do algoritmo proposto neste trabalho, o MAPM (*Multifractal Arrival Policing Mechanism*), com o tráfego sem policiamento. Em seguida, a taxa de perda em um enlace simples com *buffer* finito com e sem algoritmo de policiamento é calculada. Utilizando o Cálculo de Rede Determinístico, estima-se o tamanho da fila (*backlog*) e retardo (*delay*) de *bytes*, conforme o conceito da álgebra Min-Plus. O algoritmo de policiamento proposto foi aplicado em um sistema de transmissão OFDM (*Orthogonal Frequency - Division Multiplexing*) / TDMA (*Time Division Multiplexing Access*) baseado no sistema WiMAX simplificado, onde se avaliou o desempenho da rede com os algoritmos de policiamento considerados. Realizam-se simulações com séries reais de tráfego de redes sem fio (Wi-Fi) e de redes com fio a fim de demonstrar a eficiência do algoritmo proposto em relação aos algoritmos de policiamento encontrados na literatura. As simulações realizadas evidenciam a eficiência do algoritmo MAPM em policiar séries reais de tráfego de redes com fio e redes sem fio. Propôs-se também, a utilização do Cálculo de Rede Determinístico associado ao processo envelope multifractal para se analisar o comportamento do tráfego em termos de retardo e *backlog* após a aplicação dos algoritmos de policiamento de rede. Por fim, são apresentados os resultados de retardo, *backlog*, utilização média do *buffer* e utilização do enlace para um sistema WiMAX onde o algoritmo de policiamento MAPM que apresentou em geral, acréscimo no retardo e *backlog* do tráfego em relação aos outros algoritmos e baixa utilização do enlace.

Palavras-chave: Modelagem Multifractal, Algoritmo de Policiamento, Cálculo de Rede, Tráfego de Rede, WiMAX, Qualidade de Serviço, Retardo, *Backlog*.

ABSTRACT

The multifractal modeling is more appropriate in describing some features finding in traffic flows in real networks than other models. This work investigates the behavior of the traffic modeling based policing algorithms found in the literature (Leaky Bucket, Fractal Leaky Bucket, Gaussian Multifractal Leaky Bucket) regarding the buffer utilization, the efficiency for the use of buffer efficiency in describing the accumulated traffic (envelope process), packet dropping and data loss (bytes). First, we compare the envelope process of the considered policing algorithms and the proposed algorithm MAPM (Multifractal Arrival Policing Mechanism), with traffic without policing. Next, it was calculated the system loss rate for a finity buffer system with and without policing algorithm. Using the deterministic Network Calculus, it is also estimated the average queue length (backlog) and delay of bytes by applying the concept of the Min-Plus algebra that presents some differences against the conventional algebra. The proposed policing algorithm was applied to a transmission system based on OFDM (Orthogonal Frequency - Division Multiplexing) / TDMA (Time Division Multiplexing Access) system, where it was evaluated the network performance of the considered policing algorithms. Simulations were carried out with real wireless network trace (Wi-Fi) and wired network trace in order to demonstrate the efficiency of the algorithm proposed in relation to policing algorithms in the literature. The simulations shown the efficiency of the MAPM policing algorithm with traces from wired and wireless networks. We also propose the use of deterministic Network Calculus associated to multifractal envelope process to analyze the traffic behavior in terms of delay and backlog before policing algorithms application in the network. Finally we present the results of buffer utilization, link utilization, delay and backlog to a WiMAX system where the policing algorithm MAPM in general shown delay and backlog increasing in the traffic compared with others algorithms and low link utilization.

Keywords: Multifractal Modeling, Policing Algorithm, Network Calculus, Network Traffic, WiMAX, Quality of Service, Delay, Backlog.

LISTA DE FIGURAS

Figura 2.1 - Modo de operação infraestrutura.....	28
Figura 2.2 - Modo de operação <i>Ad-Hoc</i>	29
Figura 2.3 - Valores esperados para taxas de dados em diferentes distâncias do Ponto de Acesso para os padrões 802.11a, 802.11b e 802.11g.....	33
Figura 2.4 - Padrão IEEE 802.16 como solução para diversos segmentos de acesso à banda larga (INTEL, 2003).....	36
Figura 3.1 - Densidade de probabilidade para diferentes valores de λ	48
Figura 3.2 - Polígono composto de cópias repetidas de um pentagrama (LAUWERIER, 1991)	51
Figura 3.3 - Processo de construção da cascata binomial (VIEIRA; LING, 2008).....	55
Figura 3.4 - Cascata formada pelos coeficientes de escala $U_{j,k}$ (CROUSE et al., 2000).	56
Figura 4.1- Valores das séries de tráfego com fio (a) lbl-pkt-5 e (b) dec-pkt-3.....	61
Figura 4.2 - Valores das séries de tráfego sem fio (a) USC_06spring e (b) USC_2005summer	61
Figura 4.3 - Função densidade de probabilidade dos tráfegos com fio (a) lbl-pkt-5, (b) dec-pkt-3	62
Figura 4.4 - Função densidade de probabilidade dos tráfegos sem fio (a) USC_06spring e (b) USC_2005summer	63
Figura 4.5 - Processo Envelope para séries de tráfego com fio (a) lbl-pkt-5 e (b) dec-pkt-3 ..	64
Figura 4.6 - Processo Envelope para séries de tráfego sem fio (a) USC_06spring e (b) USC_2005summer	64
Figura 4.7 - Série de tráfego sintética Poisson: (a) série de tráfego e (b) processo envelope ..	65
Figura 4.8 - Série de tráfego sintética MWM: (a) série de tráfego e (b) processo envelope ...	65
Figura 4.9 - Processo envelope MFBAP para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring.....	67
Figura 4.10 - Comparativo dos processos envelopes de séries de tráfego USC_06spring e sintéticas	67
Figura 4.11 - Comparativo dos processos envelopes de séries de tráfego lbl-pkt-5 e sintéticas	68
Figura 4.12 - Balde Furado (TANENBAUM, 2003).....	69

Figura 4.13 - Processo envelope para o algoritmo Balde Furado para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring	70
Figura 4.14 - Pacotes descartados ou marcados como baixa prioridade para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento LB	71
Figura 4.15 - P_b versus Tamanho do <i>buffer</i> para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento LB	73
Figura 4.16 - Processo envelope Balde Furado Fractal para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring	73
Figura 4.17 - Pacotes descartados ou marcados como baixa prioridade para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento FLB	74
Figura 4.18 - P_b versus Tamanho do <i>buffer</i> para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento FLB	76
Figura 4.19 - Processo envelope Balde Furado Multifractal Gaussiano para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring	77
Figura 4.20 - Pacotes descartados ou marcados como baixa prioridade para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento GMLB	78
Figura 4.21 - P_b versus tamanho do <i>buffer</i> para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento GMLB	79
Figura 4.22 - Processo envelope MAPM para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring	80
Figura 4.23 - Pacotes descartados ou marcados como baixa prioridade para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento MAPM	81
Figura 4.24 - P_b versus tamanho do <i>buffer</i> para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento MAPM	82
Figura 4.25 - Processo Envelope MAPM, GMLB, FLB e LB para tráfegos (a) lbl-pkt-5 e (b) USC_06spring	83
Figura 4.26 - P_b para os algoritmos MAPM, GMLB, FLB e LB para a série de tráfego lbl-pkt-5	84
Figura 4.27 - P_b para os algoritmos MAPM, GMLB, FLB e LB para a série de tráfego USC_06spring	85
Figura 5.1 - A resposta ao impulso da concatenação de dois circuitos lineares é (a) a convolução da resposta ao impulso individual, a curva de formação da concatenação de dois reguladores é (b) a convolução das curvas individuais modeladas (LE BOUDEC;	

THIRAN, 2004)	88
Figura 5.2 - Exemplos de funções de entradas e saídas (LE BOUDEC; THIRAN, 2004)	89
Figura 5.3 - Limitantes para <i>backlog</i> para a série de tráfego com fio lbl-pkt-5	93
Figura 5.4 - Limitantes para <i>backlog</i> para a série de tráfego com fio dec-pkt-3	93
Figura 5.5 - Limitantes para <i>backlog</i> para a série de tráfego sem fio USC_06spring	94
Figura 5.6 - Limitantes para <i>backlog</i> para a série de tráfego sem fio USC_2005summer	94
Figura 5.7 - Limitantes para retardo para a série de tráfego com fio lbl-pkt-5	95
Figura 5.8 - Limitantes para retardo para a série de tráfego com fio dec-pkt-3	96
Figura 5.9 - Limitantes para retardo para a série de tráfego sem fio USC_06spring	96
Figura 5.10 - Limitantes para retardo para a série de tráfego sem fio USC_2005summer	97
Figura 5.11 - Sistema de enlace simples e <i>buffer</i> finito	98
Figura 5.12 - Utilização média do <i>buffer</i> para séries de tráfego com fio (a) lbl-pkt-5 e (b) dec-pkt-3	98
Figura 5.13 - Utilização média do <i>buffer</i> para séries de tráfego sem fio (a) USC_06spring e (b) USC_2005summer	99
Figura 5.14 - Utilização do enlace para séries de tráfego com fio (a) lbl-pkt-5 e (b) dec-pkt-3	100
Figura 5.15 - Utilização do enlace para séries de tráfego sem fio (a) USC_06spring e (b) USC_2005summer	100
Figura 6.1 - Modelo OFDM/TDMA com escalonamento <i>Round Robin</i> (ROCHA; VIEIRA; SANTOS JR., 2010)	103
Figura 6.2 - Sistema WiMAX com algoritmo de policiamento	105
Figura 6.3 - Probabilidade de descarte de pacotes <i>versus</i> tamanho do <i>buffer</i> para série de tráfego lbl-pkt-5	106
Figura 6.4 - Probabilidade de descarte de pacotes <i>versus</i> tamanho do <i>buffer</i> para série de tráfego dec-pkt-3	106
Figura 6.5 - Probabilidade de descarte de pacotes <i>versus</i> tamanho do <i>buffer</i> para série de tráfego USC_06spring	107
Figura 6.6 - Probabilidade de perda de pacotes <i>versus</i> tamanho do <i>buffer</i> para série de tráfego dec-pkt-2	107
Figura 6.7 - Taxa de perda <i>versus</i> capacidade do <i>buffer</i> para série de tráfego lbl-pkt-5	108
Figura 6.8 - Taxa de perda <i>versus</i> capacidade do <i>buffer</i> para série de tráfego dec-pkt-3	108

Figura 6.9 - Taxa de perda <i>versus</i> capacidade do <i>buffer</i> para série de tráfego USC_06spring	109
Figura 6.10 - Taxa de perda <i>versus</i> capacidade do <i>buffer</i> para série de tráfego dec-pkt-2....	110
Figura 6.11 - Utilização média do <i>buffer versus</i> tamanho do <i>buffer</i> para a série de tráfego lbl-pkt-5	111
Figura 6.12 - Utilização média do <i>buffer versus</i> tamanho do <i>buffer</i> para a série de tráfego USC_06spring.....	111
Figura 6.13 – Utilização do enlace para a série de tráfego lbl-pkt-5.....	112
Figura 6.14 – Utilização do enlace para a série de tráfego USC_06spring.....	113
Figura 6.15 - Limitante para <i>Backlog</i> para a série de tráfego dec-pkt-3 no sistema WiMAX	114
Figura 6.16 - Limitante para <i>Backlog</i> para a série de tráfego USC_06spring no sistema WiMAX.....	115
Figura 6.17 - Limitante para retardo para a série de tráfego dec-pkt-3 para um sistema WiMAX simplificado.....	116
Figura 6.18 - Limitante para retardo para a série de tráfego USC_06spring para um sistema WiMAX simplificado.....	117

LISTA DE TABELAS

Tabela 2.1 - Taxa de transmissão e modulação 802.11 (AMODEI, 2003).....	30
Tabela 2.2 - Taxa de transmissão e modulação 802.11a (AMODEI, 2003).....	31
Tabela 2.3 - Taxa de transmissão e modulação 802.11b (AMODEI, 2003).....	31
Tabela 2.4 - Taxa de transmissão e modulação 802.11g (AMODEI, 2003).....	32
Tabela 2.5 - Requisitos IEEE 802.16m (LEE; CHOI, 2008).....	41
Tabela 2.6 - Taxa de transmissão de dados e comprimento máximo por material (DIAS; ALVES JR., 2002).....	42
Tabela 4.1 - Características básicas das séries de tráfego.....	60
Tabela 4.2 - Comparativo entre as séries de tráfego sem policiamento e com o algoritmo de policiamento LB.....	72
Tabela 4.3 - Comparativo entre as séries de tráfego sem policiamento e com o algoritmo de policiamento FLB.....	75
Tabela 4.4 - Comparativo entre tráfego sem policiamento e com o algoritmo de policiamento GMLB.....	78
Tabela 4.5 - Comparativo entre tráfego sem policiamento e com o algoritmo de policiamento MAPM.....	81
Tabela 4.6 - Erro quadrático entre os processos envelopes dos algoritmos LB, FLB, GMLB, MAPM com o Real.....	84
Tabela 4.7 – Somatório de J_n e P_b dos algoritmos de policiamento analisados para as séries de tráfego reais.....	85
Tabela 6.1 - Erro quadrático entre os limitantes para <i>backlog</i> dos algoritmos LB, FLB, GMLB, MAPM e Real.....	115
Tabela 6.2 - Erro quadrático entre os limitantes para retardo dos algoritmos LB, FLB, GMLB, MAPM e Real.....	117

LISTA DE SIGLAS E ABREVIATURAS

AAS	- Advanced Antenna Systems / Sistemas avançados de antena
AES	- Advanced Encryption Standard / Padrão avançado de criptografia
AMC	- Adaptive Modulation and Coding / Modulação e codificação adaptativa
ANATEL	- Agência Nacional de Telecomunicações
AP	- Access Point / Ponto de acesso
ASK	- Amplitude Shift Keying / Chaveamento por mudança de amplitude
ATM	- Asynchronous Transfer Mode / Modo de transferência assíncrono
AWMM	- Adaptive Wavelet based Multifractal Model / Wavelet adaptativa baseada em modelo multifractal
b_{\max}	- Backlog bound / Limitante de tamanho de fila
$B(t)$	- Backlog no tempo t
BER	- Bit Error Rate / Taxa de erro de bit
BPSK	- Binary Phase Shift Keying / Chaveamento por mudança de fase binária
BSS	- Basic Service Set / Conjunto básico de serviço
C	- Capacidade de transmissão
$c_{m,n}$	- Número Máximo de Bits por Símbolo (Hz)
CCK	- Complementary Code Keying / Chaveamento por código complementar
CGMD	- Cascade with Generalized Multiplier Distributions / Cascata com distribuição multiplicativa generalizada
DBPSK	- Differential Binary Phase Shift Keying Chaveamento por mudança de fase binária diferencial
DCF	- Distributed Coordination Function / Função de coordenação distribuída
DiffServ	- Differentiated Services / Serviços diferenciados
DQPSK	- Differential Quadrature Phase-Shift Keying / Chaveamento por mudança de fase com quadratura diferencial
d_{\max}	- Delay bound / Limitante para retardo
DSL	- Digital Subscriber Line / Linha de assinante digital
DSSS	- Direct Sequence Spread Spectrum / Espalhamento espectral em sequência direta
DWT	- Discrete Wavelet Transform / Transformada de wavelet discreta
E1	- Canal de 2.028 Mbit/s (Padrão Europeu)

EM	- Estação Móvel
ERB	- Estação Rádio Base
fBm	- Fractional Brownian motion / Movimento Browniano fractal
fBt	- Fractional Brownian traffic / Tráfego Browniano fractal
FCC	- Federal Communications Commission / Comissão Federal de Comunicações
FDD	- Frequency-division duplexing / Duplicação por divisão de frequência
FFT	- Fast Fourier Transform / Transformada rápida de Fourier
FHSS	- Frequency Hopping Spread Spectrum / Espalhamento espectral de saltos em frequência
FLB	- Fractal Leaky Bucket / Balde Furado Fractal
GMLB	- Gaussian Multifractal Leaky Bucket / Balde Furado Multifractal Gaussiano
H	- Parâmetro de Hurst
H(.)	- Expoente de Hölder
HiperMAN	- High Performance Radio MAN / Rádio de alto desempenho MAN
IEEE	- Institute of Electrical and Electronics Engineers / Instituto de Engenheiros Eletricistas e Eletrônicos
i.d.d	- Independente e identicamente distribuídos
IntServ	- Integrated Services / Serviços integrados
IP	- Internet Protocol / Protocolo de internet
$k\nu_{T,\tau}$	- Curva de Chegada
LAN	- Local Area Network / Rede de área local
LB	- Leaky Bucket / Balde Furado
LRD	- Long Range Dependency / Dependência de longa duração
LOS	- Line of sight / Linha de visada
LSP	- Label Switching Paths / Rótulos de caminhos de chaveamento
LTE	- Long Term Evolution / Evolução de longo prazo
MAC	- Media Access Control / Controle de acesso ao meio
MAN	- Metropolitan Area Network / Rede de área Metropolitana
MAPM	- Multifractal Arrival Policing Mechanism / Mecanismo de Policiamento de Chegadas Multifractais
mBm	- Multifractal Brownian Motion / Movimento Browniano multifractal
MIMO	- Multiple Input – Multiple Output / Múltiplas entradas – Múltiplas saídas
MIT	- Massachusetts Institute of Technology / Instituto de tecnologia de Massachusetts

MPLS	- Multiprotocol Label Switching / Rótulo de chaveamento de multiprotocolos
MWM	- Multifractal Wavelet Model / Modelo wavelet multifractal
\mathbb{N}	- Conjunto dos números naturais
NLOS	- Non line of sight / Sem linha de visada
OFDM	- Orthogonal Frequency-Division Multiplexing / Multiplexação por divisão de frequência ortogonal
ρ	- Média de tráfego de pacotes
$\rho(k)$	- Função de autocorrelação
PA	- Ponto de Acesso
P_b	- Taxa de Perda do Sistema
P_d	- Taxa de Tráfego Marcado com Baixa Prioridade ou Descartado
PDA	- Personal Digital Assistants / Assistente pessoal digital
PE	- Processo Envelope
PHY	- Camada Física
PSK	- Phase-Shift Keying / Chaveamento por mudança de fase
Q_r	- Buffer
QAM	- Quadrature Amplitude Modulation / Modulação por amplitude e quadratura
QoS	- Quality of Service / Qualidade de serviço
QPSK	- Quadrature Phase-Shift Keying / Chaveamento por mudança de fase e quadratura
\mathbb{R}	- Conjunto dos números Reais
$R(.)$	- Função de entrada de fluxo
SELFIS	- Self-similarity analysis Software / Software de análise de autossimilaridade
SLA	- Service Level Agreements / Acordo de nível de serviço
SOFDMA	- Scalable Orthogonal Frequency Division Multiplexing Access / Multiplexação de acesso por divisão de frequência escalável
SoHo	- Small Office/ Home Office – Escritórios pequenos / Escritórios em casa
$S(n)$	- Modelo de tempo discreto
SNR	- Signal-to-Noise Ratio / Taxa de sinal ruído
σ	- Desvio padrão
τ	- Tolerância
Δ	- Intervalo de tempo
t	- Tempo

T1	- Canal de 1.544 Mbit/s (Padrão Americano)
TCP	- Transmission Control Protocol / Protocolo de controle de transmissão
TDD	- Time-division duplexing / Duplicação por divisão de tempo
TKIP	- Temporal Key Integrity Protocol / Protocolo de integridade de chave temporal
TXOP	- Transmission Opportunity / Oportunidade de transmissão
u_b	- Utilização do buffer
u_e	- Utilização do enlace
USC	- University of Southern California / Universidade do Sul da Califórnia
VBR	- Variable Bit Rate / Taxa de bit variável
VoIP	- Voice over IP / Voz sobre IP
$v_{T,\tau}$	- Função Degrau
$X(.)_n$	- Variável aleatória / Tráfego de entrada
$W(t)_n$	- Retardo no tempo t
WAN	- Wide Area Network / Rede de longa distância
WECA	- Wireless Ethernet Compatibility Alliance
WEP	- Wired Equivalent Protocol / Protocolo equivalente à rede com fio
Wi-Fi	- Wireless Fidelity / Fidelidade sem fio
WiMAX	- Worldwide Interoperability for Microwave Access / Interoperabilidade Mundial para Acesso de Micro-ondas
WLAN	- Wireless Local Area Network / Rede local sem fio
\mathbb{Z}	- Conjunto dos números inteiros

TRABALHOS SUBMETIDOS E PUBLICADOS

1. J. A. Santos Jr., F. G. C. Rocha e F. H. T. Vieira. –A Traffic Policing Mechanism for WiMAX Systems Based on Multifractal Modeling”. The 7th International Telecommunications Symposium (ITS 2010), Manaus - AM, 06 - 09 de setembro, 2010;
2. J. A. Santos Jr., F. H. T. Vieira e F. G. C. Rocha. –A Policing Algorithm for WiMAX Systems Considering Multifractal Traffic Characteristics”. The 13th International Symposium on Wireless Personal Multimedia Communications (WPMC 2010), Recife, 11 - 14 de outubro, 2010;
3. J. A. Santos Jr., F. H. T. Vieira, F. G. C. Rocha e M. A. DeSousa. –Análise de Desempenho de Algoritmos de Controle para Tráfego Multifractal de Redes”. XVIII Congresso Brasileiro de Automática, Bonito - MS, 12 - 16 de setembro, 2010;
4. F. G. C. Rocha, F. H. T. Vieira e J. A. Santos Jr. –A multifractal based approach for loss probability estimation for OFDM/TDMA based wireless systems”. The 13th International Symposium on Wireless Personal Multimedia Communications (WPMC 2010), Recife, 11 - 14 de outubro, 2010;
5. J. A. Santos Jr., F. H. T. Vieira. –Análise de desempenho de algoritmos de policiamento em redes sem fio considerando tráfego multifractal”. Conpeex (Congresso de Pesquisa, Ensino e Extensão) 2010, Goiânia, 18 - 22 de outubro, 2010.
6. F. H. T. Vieira, F. G. C. Rocha, J. A. Santos Jr., –Loss probability estimation and control for OFDM/TDMA wireless systems considering multifractal traffic characteristics”, Computer Communications, Elsevier;

SUMÁRIO

RESUMO.....	VII
ABSTRACT.....	VIII
LISTA DE FIGURAS	IX
LISTA DE TABELAS.....	XIII
LISTA DE SIGLAS E ABREVIATURAS	XIV
TRABALHOS SUBMETIDOS E PUBLICADOS.....	XVIII
CAPÍTULO 1 INTRODUÇÃO	22
CAPÍTULO 2 PADRÕES DE REDES SEM FIO.....	27
2.1 REDES SEM FIO PADRÃO IEEE 802.11 (Wi-Fi / WLAN).....	28
2.1.1 <i>Padrão IEEE 802.11a</i>	30
2.1.2 <i>Padrão IEEE 802.11b</i>	31
2.1.3 <i>Padrão IEEE 802.11g</i>	32
2.1.4 <i>Padrão IEEE 802.11n</i>	34
2.2 REDES SEM FIO PADRÃO IEEE 802.16 (WiMAX / WMAN)	35
2.2.1 <i>Padrão IEEE 802.16a</i>	37
2.2.2 <i>Padrão IEEE 802.16c</i>	37
2.2.3 <i>Padrão IEEE 802.16d</i>	38
2.2.4 <i>Padrão IEEE 802.16e</i>	39
2.2.5 <i>Padrão IEEE 802.16m</i>	41
2.3 REDES COM FIO PADRÃO IEEE 802.3 (<i>ETHERNET</i>).....	42
2.4 RESUMO DO CAPÍTULO.....	43
CAPÍTULO 3 MODELAGEM E ESTIMAÇÃO DE PARÂMETROS DE FLUXOS DE TRÁFEGO DE REDES	44
3.1 MODELAGEM DE TRÁFEGO.....	45
3.2 MODELO DE POISSON.....	47
3.3 MODELO MOVIMENTO BROWNIANO FRACTAL (FBM).....	48
3.3.1 <i>Parâmetro de Hurst</i>	51
3.3.2 <i>Função de Autocorrelação</i>	51
3.4 PROCESSOS MULTIFRACTAIS	52

3.5	MODELO MOVIMENTO BROWNIANO MULTIFRACTAL (MBM).....	53
3.6	MODELO CASCATAS MULTIPLICATIVAS.....	54
3.7	MODELO MWM (<i>MULTIFRACTAL WAVELET MODEL</i>).....	56
3.8	MODELO AWMM (<i>ADAPTIVE WAVELET BASED MULTIFRACTAL MODEL</i>).....	57
3.9	MODELO CGMD (<i>CASCADE WITH GENERALIZED MULTIPLIER DISTRIBUTIONS</i>)....	57
3.10	RESUMO DO CAPÍTULO.....	58
CAPÍTULO 4 POLICIAMENTO BASEADO EM MODELAGEM DE TRÁFEGO..		59
4.1	SÉRIES DE TRÁFEGO UTILIZADAS	60
4.2	PROCESSO ENVELOPE (PE).....	63
4.3	PROCESSO DE CHEGADA COM LIMITANTE MULTIFRACTAL (<i>MULTIFRACTAL BOUNDED ARRIVAL PROCESS – MFBAP</i>)	65
4.4	POLICIAMENTO DE REDES BASEADO EM MODELAGEM DE TRÁFEGO.....	68
4.4.1	<i>Balde Furado (Leaky Bucket - LB)</i>	69
4.4.2	<i>Balde Furado Fractal (Fractal Leaky Bucket - FLB)</i>	73
4.4.3	<i>Balde Furado Multifractal Gaussiano (Gaussian Multifractal Leaky Bucket – GMLB)</i>	76
4.5	MECANISMO DE POLICIAMENTO DE CHEGADA MULTIFRACTAL (<i>MULTIFRACTAL ARRIVAL POLICING MECHANISM – MAPM</i>)	79
4.6	COMPARAÇÕES ENTRE OS PROCESSOS ENVELOPES DOS ALGORITMOS DE POLICIAMENTO	82
4.7	RESUMO DO CAPÍTULO.....	86
CAPÍTULO 5 CÁLCULO DE REDE DETERMINÍSTICO: ESTIMAÇÃO DE BACKLOG E RETARDO		87
5.1	INTRODUÇÃO AO CÁLCULO DE REDE	87
5.2	LIMITANTES PARA <i>BACKLOG</i> E RETARDO	89
5.3	DEFINIÇÃO DE CURVA DE CHEGADA.....	90
5.4	DEFINIÇÃO DE CURVAS DE SERVIÇO	90
5.5	CÁLCULO DO TAMANHO MÉDIO DA FILA (<i>BACKLOG</i>) E DO RETARDO (<i>DELAY</i>)...	92
5.6	ANÁLISE DA UTILIZAÇÃO MÉDIA DO <i>BUFFER</i> E DO ENLACE.....	97
5.7	RESUMO DO CAPÍTULO.....	101
CAPÍTULO 6 POLICIAMENTO DE TRÁFEGO EM REDES WIMAX BASEADO EM MODELAGEM MULTIFRACTAL		102
6.1	SISTEMA DE TRANSMISSÃO OFDM/TDMA BASEADO EM REDES WIMAX.....	103

6.2	APLICAÇÃO DE ALGORITMOS DE POLICIAMENTO EM REDES OFDM/TDMA WIMAX: SIMULAÇÕES E RESULTADOS	104
6.2.1	<i>Comparações entre as perdas de bytes dos algoritmos de policiamento de tráfego de rede</i>	104
6.3	CÁLCULO DE <i>BACKLOG</i> E DE RETARDO EM REDE WIMAX UTILIZANDO CÁLCULO DE REDE	113
6.4	RESUMO DO CAPÍTULO.....	118
CAPÍTULO 7 CONCLUSÕES.....		119
REFERÊNCIAS.....		122
APÊNDICE A.....		130

CAPÍTULO 1

INTRODUÇÃO

Em redes de computadores, uma conexão (fluxo de pacotes entrantes na rede) que é admitida deve ser policiada a fim de obrigar que a sequência de pacotes gerados nesta conexão fique em conformidade com o perfil de tráfego requerido. O algoritmo de policiamento destina-se a regular a entrada de pacotes na rede de forma a tornar o fluxo de tráfego de acordo com as características estipuladas no contrato de serviço (SLA – *Service Level Agreement*) (ITU-T, 1996). Caso contrário, os pacotes devem ser descartados ou marcados como sendo de baixa prioridade.

Atualmente, grande parte das redes de computadores utiliza somente serviços de melhor-esforço (*best effort*), os quais não são apropriados para certas aplicações de transmissão de dados em tempo real ou sensíveis ao retardo. A fim de ampliar o suporte a serviços com restrições temporais e com taxas de transmissão variáveis, o conceito de qualidade de serviço (QoS – *Quality of Service*) deve ser incorporado ou implementado nestas redes IP.

A primeira arquitetura proposta para QoS levando em consideração parâmetros de qualidade de serviço foi o *IntServ* (*Integrated Service* – Serviços Integrados) (PARTRIDGE, 1992), no qual se propõe a realizar reservas de recursos ao longo dos caminhos de transmissão da rede (BRADEN; CLARK; SHENKER, 1994). Devido a falta de escalabilidade, este modelo de serviço para QoS não é aplicado satisfatoriamente nos pontos da Internet onde o número de fluxos é alto.

Em resposta às dificuldades da falta de escalabilidade pela agregação de fluxos de dados que surgiram com o *IntServ*, surgiu a arquitetura *DiffServ* (*Differentiated Services* – Serviços Diferenciados) (HUSTON, 2000; CHEN; QIAO; YU, 2004). Em vez de se ter tratamento individualizado para cada fluxo de tráfego, os pacotes de dados são designados às classes que possuem parâmetros de QoS distintos.

Vieira (2006) assim como Dias e Willrich (2001) afirmam que o *Diffserv* pode ser implementado através da arquitetura MPLS (*Multiprotocol Label Switching*). Esta arquitetura apresenta várias facilidades à engenharia de tráfego de rede, criando rotas através do estabelecimento de LSPs (*Label Switching Paths*) e usando FECs (*Forwarding Equivalent Class*) que dividem o tráfego em diferentes fluxos agregados de acordo com o modelo de serviço adotado. Com isso, mecanismos de policiamento são ferramentas importantes em arquitetura de redes, já que o controle do tráfego de rede consiste na integração de funções como controle de acesso, gerenciamento de rede e policiamento de tráfego. Destaca-se também, que o policiamento de tráfego é exigido devido a natureza estatística e a possibilidade de haver tráfego mal comportado (fora dos padrões acordados pelo SLA) para algumas séries de tráfego de rede (VIEIRA, 2006).

Observa-se que os fluxos de tráfego de redes que violam o acordo de conexão (SLA) podem ter seus pacotes descartados para evitar congestionamento na rede ou impacto adverso nos parâmetros de QoS dos outros fluxos de tráfego na rede, bem como marcados como sendo de prioridade baixa e permitir ou não a entrada destes na rede. Segundo Rathgeb (1991), a utilização de mecanismos de policiamento de tráfego para estes casos é proposta desde o surgimento da tecnologia de redes.

O algoritmo de Balde Furado (*Leaky Bucket* – LB) é o mecanismo de policiamento de tráfego mais comum presente na literatura (TANENBAUM, 2003). Contudo, o algoritmo de Balde Furado (LB) não apresenta uma resposta muito eficiente quando polícia tráfegos com pacotes em rajadas, devido a esse tipo de tráfego encher o balde (*buffer*) rapidamente (SOHRABY; SIDI, 1994; SILVESTERL, 1996).

Em decorrência disso, o transbordo do balde faz o algoritmo descartar pacotes bem comportados (que estão de acordo com o SLA). Este tipo de situação pode ser observada quando são considerados os modelos de tráfego entrante monofractais e multifractais, uma vez que uma característica comum aos dois modelos é o fluxo de tráfego de pacotes ter um número considerável de rajadas. Em outras palavras, o algoritmo Balde Furado (LB) descarta ou marca como mal comportado parte do tráfego em rajadas até quando suas características estão de acordo com a descrição de serviço (SLA), porque o algoritmo não é capaz de reconhecer o tráfego real como adequadamente comportado.

Em Pereira, Fonseca e Arantes (2001), um regulador de tráfego chamado Balde Furado Fractal (*Fractal Leaky Bucket* – FLB) foi introduzido para lidar com o tráfego monofractal. O FLB provou ser um mecanismo eficiente para policiar fontes de tráfego

monofractais. Em contrapartida, o Balde Furado Multifractal Gaussiano (*Gaussian Multifractal Leaky Bucket* – GMLB) descrito por Takada e Anzaloni (2006) foi utilizado para lidar com tráfego multifractal.

Constata-se que até no ano 2000, os usuários de Internet (principalmente as universidades com conexões *dial-up*, empresas e instalações do governo com *links* dedicados) acessavam o seu conteúdo geralmente através de fios, ou seja, por meio de sistemas de infraestrutura fixa (redes *Ethernet* e Internet) (VALE; COSTA; ALVES JR, 2001). Porém, a tecnologia evoluiu de tal forma que um número significativo de usuários de serviços de acesso à Internet atualmente é sem fio. Esta evolução do acesso ocorreu em conjunto com o aumento da utilização de computadores portáteis e pequenos aparelhos móveis sem fio, como telefones celulares e outros dispositivos.

Percebe-se que a arquitetura sem fio para Internet emergente continua evoluindo e apoiando um crescente número de acesso de usuários com altas taxas de dados, de tal forma que a experiência do usuário é semelhante à experiência de uma conexão de alta velocidade com fio. Com isso, uma variedade de tecnologias sem fio tem sido propostas tais como *Bluetooth*, *Zig-bee*, Wi-Fi e WiMAX, tanto em organizações de padronização quanto pelos consórcios de indústrias, para permitir o acesso à rede sem fio (LABIOD; AFIFI; SANTIS, 2007).

O aumento do tráfego na rede com a utilização de serviços de transmissão de voz e vídeo, além dos dados convencionais, desencadeou uma queda na qualidade dos serviços da rede devido aos diferentes tipos de dados (pacotes) transmitidos. Segundo Dias e Alves Jr. (2002), para melhorar a qualidade, seria necessário o aumento da largura de banda (capacidade do enlace) ou um controle de tráfego mais eficiente. Por sua vez, Fraga e Paiva (2007) afirmam que os diferentes tipos de serviços presentes na rede podem causar um fluxo de pacotes em rajadas além de outros fatores, como as características multifractais, até então pouco consideradas nos algoritmos de policiamento existentes na literatura.

Considera-se que os modelos multifractais apresentam várias características presentes em outros modelos e descrevem de forma mais precisa e abrangente o comportamento do tráfego de redes atual. Com uma caracterização mais detalhada do tráfego, espera-se obter melhores estimativas, por exemplo, para a probabilidade de perda de pacotes para fluxos de tráfego e para o processo envelope (PE) dos fluxos de tráfegos (VIEIRA, 2006).

Neste trabalho, apresenta-se uma proposta de algoritmo de policiamento do tipo

Balde Furado baseado nas propriedades multifractais do tráfego de redes chamado MAPM (Mecanismo de Policiamento de Chegadas Multifractais), mais abrangente e preciso (mais próximo do processo envelope) que a abordagem fractal (FLB) e mais adequado (matematicamente mais simples) para o tráfego de rede real (atual) que a abordagem multifractal Gaussiana (GMLB).

Utiliza-se a teoria de redes conhecida como Cálculo de Rede (*Network Calculus*) para estimação do tamanho da fila (*backlog*) e retardo (*delay*) dos pacotes para algumas séries de tráfego em um enlace simples, assim como para cada algoritmo de policiamento apresentado (LE BOUDEC; THIRAN, 2004). O Cálculo de Rede é aplicado para um sistema de fila simples (*buffer* finito) e para um sistema de transmissão OFDM / TDMA baseado em WiMAX simplificado.

Por fim, apresentam-se os resultados do algoritmo de policiamento de tráfego de rede proposto, que leva em consideração o processo envelope de um modelo multifractal e da proposta de utilização do Cálculo de Rede para estimação de retardo e tamanho de fila (*backlog*) para fluxos reais de tráfego de rede fixa (Internet) e sem fio (Wi-Fi).

Após o capítulo introdutório, a dissertação está organizada da seguinte maneira:

Capítulo 2 – Padrões de redes sem fio, onde se apresentam as tecnologias de redes sem fio mais utilizadas na atualidade, como o Wi-Fi (IEEE 802.11) e WiMAX (IEEE 802.11), bem como suas versões e atualizações mais importantes.

Capítulo 3 - Modelagem e estimação de parâmetros de fluxos de tráfegos de redes, onde se descreve a modelagem de tráfego de rede e estimação de parâmetros, apresentando os modelos mais comuns para fluxos de tráfego de redes como o modelo de Poisson e o Movimento Browniano Fractal (fBm). Neste capítulo, trata-se também da definição do parâmetro de Hurst, Processos Multifractais como o Movimento Browniano Multifractal (mBm) e expoente de Hölder, Cascatas Multiplicativas, Multifractal *Wavelet Model* (MWM), *Adaptative Wavelet Based Multifractal Model* (AWMM) e *Cascade with Generalized Multiplier Distributions* (CGMD).

Capítulo 4 - Policiamento baseado em modelagem de tráfego, apresenta-se as séries de tráfego utilizadas e seus principais parâmetros como média, variância e parâmetro de Hurst. Ainda neste capítulo, trata-se sobre o conceito de: processo envelope determinístico e o processo envelope do Processo de Chegada com Limitante Multifractal (MFBAP – *Multifractal Bounded Arrival Process*); dos algoritmos de policiamento de tráfego de redes baseado em modelagem de rede, como o Balde Furado (LB – *Leaky Bucket*), Balde Furado

Fractal (FLB – *Fractal Leaky Bucket*) e Balde Furado Multifractal Gaussiano (GMLB – *Gaussian Multifractal Leaky Bucket*), onde o estudo dos algoritmos de policiamento apresentados motivou à proposição de um novo algoritmo de policiamento que também se apresenta neste capítulo, chamado de Mecanismo de Policiamento de Chegadas Multifractais (MAPM – *Multifractal Arrival Policing Mechanism*).

Capítulo 5 - Cálculo de rede determinístico: estimação de backlog e retardo, onde se dá ênfase ao Cálculo de Rede Determinístico (*Deterministic Network Calculus*) aplicado na estimação do tamanho médio da fila (*backlog*) e retardo (*delay*) dos fluxos de tráfegos de rede analisados, além do processo envelope determinístico também baseado em Cálculo de Redes.

Capítulo 6 - Policiamento de tráfego em redes wimax baseado em modelagem multifractal, apresenta-se um sistema OFDM/TDMA baseado em WiMAX simplificado, onde se aplica neste sistema, o algoritmo de policiamento de tráfego de redes proposto, chamado de Mecanismo de Policiamento de Chegada Multifractal (MAPM) e compara os outros algoritmos de policiamento. Neste capítulo são apresentados os resultados das simulações realizadas, considerando o sistema OFDM/TDMA WiMAX simplificado.

Capítulo 7 - Conclusões, onde são apresentadas as conclusões obtidas com as análises das séries de tráfego de rede analisadas, dos algoritmos de policiamento utilizados, além dos resultados de retardo e *backlog* obtidos através do Cálculo de Rede Determinístico para um sistema OFDM/TDMA baseado em WiMAX.

CAPÍTULO 2

PADRÕES DE REDES SEM FIO

As tecnologias de rede sem fio estão em ascensão no mercado atual. Este tipo de rede possui categorias com características derivadas do padrão *Ethernet* (TANENBAUM, 2003) tais como: Redes locais sem fio ou WLAN (*Wireless Local Area Network*), Redes metropolitanas sem fio ou WMAN (*Wireless Metropolitan Area Network*), Redes de longa distância sem fio ou WWAN (*Wireless Wide Area Network*), redes de loop local ou WLL (*Wireless Local Loop*) e as Redes pessoais sem fio ou WPAN (*Wireless Personal Area Network*) (SILVA, 1998).

Mesmo com o surgimento do LTE (*Long Term Evolution*) (ERICSSON, 2009; MARTÍN-SACRISTÁN et al., 2009) como mais uma alternativa ao padrão IEEE 802.16, são apresentadas apenas os padrões 802.11 e 802.16, pois estão envolvidos diretamente neste trabalho com as séries de tráfego utilizadas (Wi-Fi) e o sistema de transmissão sem fio (WiMAX), respectivamente.

Na seção 2.1 se apresenta o padrão de rede sem fio IEEE 802.11, também conhecido com Wi-Fi e suas subseções mostram os padrões mais populares adotados para esta tecnologia, bem como o alcance máximo do sinal e suas taxas de transmissão de dados. Na seção 2.2, apresenta-se o padrão IEEE 802.16, ou popularmente chamado de WiMAX, que surge como uma melhoria de algumas limitações do padrão Wi-Fi como taxa de transmissão e tamanho da área de cobertura do sinal. Na seção 2.3, apresenta-se o resumo do capítulo.

Neste trabalho utiliza-se séries de tráfegos provenientes de redes Wi-Fi padrão 802.11g para demonstração dos resultados dos algoritmos de policiamento de tráfego aplicados ao tráfego de rede sem fio. Considera-se o padrão 802.16d (WiMAX Nomádico) para as análises da eficiência dos algoritmos de policiamento em um sistema de transmissão sem fio (OFDM / TDMA).

2.1 Redes Sem Fio Padrão IEEE 802.11 (Wi-Fi / WLAN)

O padrão de rede sem fio IEEE 802.11, também conhecido com Wi-Fi, constitui-se uma das maiores inovações tecnológicas dos últimos anos. Há quem diga que atualmente, é o padrão de fato com conectividade sem fio para redes locais. Prova disso é o crescente número de *Hotspots*¹ (encontrados geralmente em locais públicos como cafês, restaurantes, hotéis e aeroportos) e do fato da maioria dos computadores portáteis novos já saírem de fábrica equipados com interfaces IEEE 802.11.

As redes sem fio padrão 802.11 podem operar em duas configurações distintas: Infraestrutura e *Ad-Hoc* (TANENBAUM, 2003).

No modo infraestrutura existe um equipamento para concentrar todo o tráfego da rede, conhecido como AP (*Access Point* ou Ponto de Acesso) conforme ilustrado na Figura 2.1 (KHAN; KHWAJA, 2003). Este modo possui alguns aspectos positivos, como por exemplo, a configuração da rede é feita somente no concentrador e as estações clientes são configuradas de modo automático.



Figura 2.1 - Modo de operação infraestrutura.

Segundo Andrade e Colli (2003), no modo *Ad-Hoc* não existe um equipamento concentrador (ponto de acesso) conforme ilustra a Figura 2.2, ou seja, os equipamentos se conectam diretamente uns aos outros sem necessidade de equipamentos adicionais. Em uma

¹ *Hotspot* (do inglês *hot*, quente e *spot*, ponto) – nome dado ao local onde a tecnologia Wi-Fi está disponível.

rede de computadores *Ad-Hoc*, todos os terminais funcionam como roteadores, encaminhando os pacotes de tráfego para terminais vizinhos até chegarem no terminal de destino (KHAN; KHWAJA, 2003).

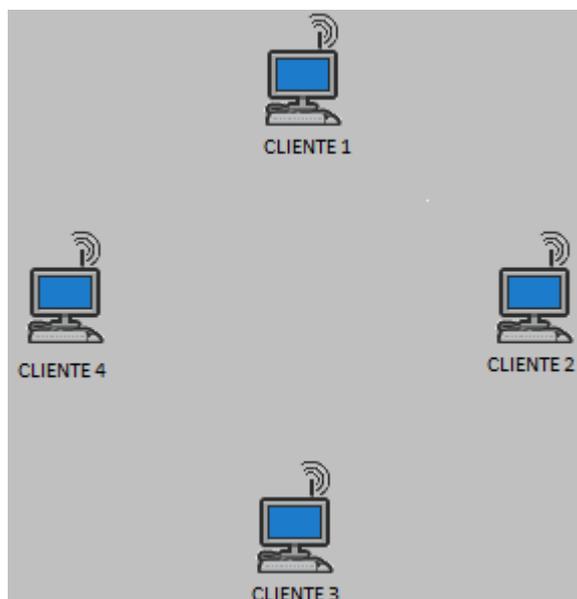


Figura 2.2 - Modo de operação *Ad-Hoc*

Outras características distintas das redes *Ad-Hoc* incluem o modo de operação distribuído ponto a ponto, roteamento *multi-hop* e mudanças relativamente frequentes na rota do tráfego dos pacotes de dados na rede.

Para evitar o problema de conectividade entre os diferentes fabricantes de tecnologias de redes sem fio, a Sociedade de Computação do IEEE (*Institute of Electrical and Electronics Engineers*) instaurou um comitê para definir um padrão. Após sete anos de pesquisa e desenvolvimento, em junho de 1997, aprovou-se o padrão IEEE 802.11 (IEEE Std. 802.11, 1999).

As duas técnicas de espalhamento espectral especificadas foram a *Frequency Hopping* (FHSS – *Frequency Hopping Spread Spectrum*, Espalhamento espectral por saltos em frequência), e a *Direct Sequence* (DSSS – *Direct Sequence Spread Spectrum*, Espalhamento espectral por sequência direta) (KHAN; KHWAJA, 2003), que utilizam a faixa de frequência de 2,4 GHz com taxas e modulações digitais BPSK (*Binary Phase Shift Keying*, Chaveamento por mudança de fase binária) e QPSK (*Quadrature Phase-Shift Keying*, Chaveamento por mudança de fase e quadratura) conforme Tabela 2.1.

Taxa de Transmissão (Mbps)	Modulação	Alcance (m)	
		<i>Indoor</i>	<i>Outdoor</i>
1	BPSK	20	100
2	QPSK		

Tabela 2.1 - Taxa de transmissão e modulação 802.11 (AMODEI, 2003)

O termo Wi-Fi é uma marca registrada pertencente à WECA (*Wireless Ethernet Compatibility Alliance*) (Wi-Fi Alliance, 2011). A WECA é uma organização sem fins lucrativos formada em 1999 e tem como missão certificar a interoperabilidade entre produtos que utilizam o padrão 802.11. Após a realização de diversos testes, os produtos que atendem ao padrão recebem o logotipo Wi-Fi (Wi-Fi Alliance, 2011).

A Wi-Fi Alliance foi o novo nome utilizado para WECA a partir de 2000. Com programas de desenvolvimento tecnológico, construção de mercado e de regulamentação, a Wi-Fi Alliance tem permitido a adoção generalizada de Wi-Fi em todo o mundo. O programa Wi-Fi CERTIFIED™ lançado em março de 2000 fornece uma designação amplamente reconhecida de interoperabilidade e de qualidade, que ajuda a garantir que os produtos Wi-Fi ofereçam uma melhor qualidade de serviço ao usuário (Wi-Fi Alliance, 2011).

O padrão IEEE 802.11 divide-se em várias partes, nas quais cada subdivisão trata de aspectos diferentes no desenvolvimento e desempenho das redes Wi-Fi.

2.1.1 Padrão IEEE 802.11a

O padrão IEEE 802.11a alcança taxas de 54 Mbps segundo a norma do IEEE criada em 1999 e de 72 até 108 Mbps para taxas proprietárias (taxas não padronizadas pelo IEEE e que diferem de acordo com cada fabricante). Este padrão utiliza a modulação OFDM com 52 subportadoras, sendo 48 delas para dados e 4 são subportadoras piloto² (GASPARINI, 2007). Este padrão de rede opera na frequência de 5 GHz e suporta 64 usuários por AP (ou ponto de acesso – PA, em português) (IEEE 802.11a, 1999), as taxas de transmissão padronizadas e suas respectivas modulações encontram-se na Tabela 2.2.

As diferentes taxas de transmissão que utilizam modulações iguais, apresentadas na Tabela 2.2, são possíveis devido a diferentes taxas de códigos convolucionais, dadas pela fração k/n , onde para cada k bits de informação útil o código gera n bits de dados onde $n - k$ são os bits redundantes. Por isso, o código de convolução utilizado é um dos fatores

² Subportadoras piloto – são subportadoras utilizadas para o transporte de sinalização do equipamento (equalização da magnitude e fase, por exemplo).

determinantes na estimação da taxa de transmissão de dados.

Taxa de Transmissão (Mbps)	Modulação	Taxa de código	Alcance (m)	
			<i>Indoor</i>	<i>Outdoor</i>
6	BPSK	1/2		
9	BPSK	3/4		
12	QPSK	1/2		
18	QPSK	3/4	35	120
24	16-QAM	1/2		
36	16-QAM	3/4		
48	64-QAM	2/3		
54	64-QAM	3/4		
72 / 108	Modo proprietário	--	--	--

Tabela 2.2 - Taxa de transmissão e modulação 802.11a (AMODEI, 2003)

As principais características do padrão 802.11a são a taxa de transmissão (maior que para o padrão 802.11 inicial que era de 2 Mbps) e a utilização de frequência não-licenciada de 5 GHz com baixo nível de interferências. A maior desvantagem do padrão IEEE 802.11a é a incompatibilidade com os padrões 802.11b e 802.11g no que diz respeito aos pontos de acesso (concentradores) e estações clientes.

2.1.2 Padrão IEEE 802.11b

Este padrão alcança taxas de até 11 Mbps conforme determinação do IEEE (em 1999), com subtaxas apresentadas na Tabela 2.3 e taxa máxima de 22 Mbps oferecida por alguns fabricantes (não-padronizados). Este padrão opera na frequência de 2,4 GHz e suporta 32 usuários por ponto de acesso (AP) (IEEE 802.11b, 1999). As diferentes taxas de transmissão de dados também são possíveis utilizando-se diferentes taxas de *bits* por símbolo em conjunto com a técnica de modulação CCK (*Complementary Code Keying*) (PEARSON, 2000; HALFORD et al., 1999).

Taxa de Transmissão (Mbps)	Modulação	<i>Bits/símbolo</i>	Alcance (m)	
			<i>Indoor</i>	<i>Outdoor</i>
1	BPSK	1		
2	QPSK	2	38	140
5,5	CCK-QPSK	4		
11	CCK-QPSK	8		
22	Modo proprietário	--	--	--

Tabela 2.3 - Taxa de transmissão e modulação 802.11b (AMODEI, 2003)

Um ponto negativo neste padrão é a alta interferência tanto na transmissão como na recepção de sinais, por funcionar em 2,4 GHz, equivalente aos telefones celulares, fornos de micro-ondas e dispositivos *Bluetooth*. Os aspectos positivos são o baixo preço dos dispositivos e espectro de frequência livre mundialmente.

O padrão IEEE 802.11b foi a primeira norma que tornou as WLANs utilizáveis de forma global, fornecendo um desempenho robusto e confiável com 11 Mbps, cinco vezes mais rápido que o padrão original/inicial (o padrão IEEE 802.11). Este padrão também forneceu aos clientes WLAN a liberdade de escolha de fabricante de modo flexível e interoperável. A solução de interoperabilidade de múltiplos fornecedores certificados garantiu a aceitação de usuários e preços mais acessíveis com soluções às altas taxas sem fio (de 2 Mbps para 11 Mbps). Esse padrão abriu novas oportunidades para se expandir o potencial da computação em rede e serviu de base de estudos para padrões que surgiram posteriormente com maiores taxas de transmissão de dados e alcance do sinal (AMODEI, 2003).

2.1.3 Padrão IEEE 802.11g

Este padrão baseia-se na compatibilidade com os dispositivos 802.11b (LUTHER, 2005) e oferece taxas de até 54 Mbps (pela norma IEEE 802.11g de 2003, conforme Tabela 2.4) e 108 Mbps com padrões proprietários (incompatível entre fabricantes) e opera na frequência de 2,4 GHz.

Taxa de Transmissão (Mbps)	Modulação	Taxa de código	Alcance (m)	
			<i>Indoor</i>	<i>Outdoor</i>
6	BPSK	1/2		
9	BPSK	3/4		
12	QPSK	1/2		
18	QPSK	3/4	35	120
24	16-QAM	1/2		
36	16-QAM	3/4		
48	64-QAM	2/3		
54	64-QAM	3/4		
72 / 108	Modo proprietário	--	--	--

Tabela 2.4 - Taxa de transmissão e modulação 802.11g (AMODEI, 2003)

Para as novas taxas de transmissão de dados (conforme apresentadas na Tabela 2.4) especificadas pelo padrão IEEE 802.11g, utiliza-se a modulação OFDM e para as taxas equivalentes aos padrões anteriores, utilizam-se as modulações do padrão IEEE 802.11b.

Com o 802.11g tem-se os mesmos inconvenientes do padrão 802.11b quanto a utilização da frequência, além da presença de um dispositivo 802.11b numa rede 802.11g reduzir consideravelmente a taxa de dados geral da rede (GASPARINI, 2007). Isso ocorre porque ao manter a compatibilidade com dispositivos 802.11b, os equipamentos operam com métodos diferentes de codificação de dados e *overhead* (cabeçalho) de gerência dos dispositivos, que para uma rede mista 802.11b/g pode-se obter transmissões de dados mais lentas (ENGST; FLEISHMAN, 2005).

Os valores das taxas de transmissão com a mesma modulação, apresentadas na Tabela 2.4 são obtidos com diferentes taxas de código. O padrão prevê a obtenção dos diferentes valores de taxas de transmissão de dados de acordo com a qualidade do sinal e distância entre a estação cliente e o ponto de acesso.

A Figura 2.3 apresenta um comparativo entre os padrões 802.11a, 802.11b e 802.11g em relação à taxa de transmissão de dados e alcance do sinal, que são inversamente proporcionais.

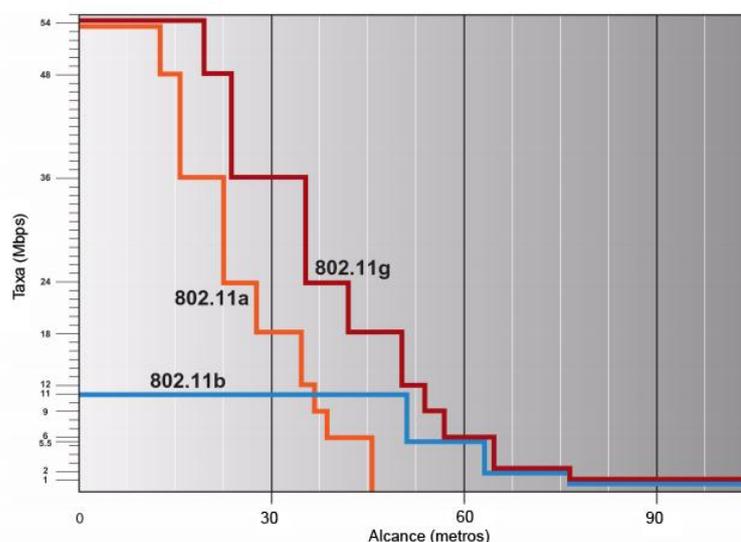


Figura 2.3 - Valores esperados para taxas de dados em diferentes distâncias do Ponto de Acesso para os padrões 802.11a, 802.11b e 802.11g

A vantagem do padrão 802.11g é a transmissão de dados com taxas semelhantes ao padrão 802.11a, pois é possível taxas superiores a 11 Mbps (superando o padrão IEEE 802.11b) na frequência de 2,4 GHz. Na parte de segurança da rede, utiliza-se autenticação WEP (*Wired Equivalent Privacy*) estática e aceita outros tipos de autenticação como WPA (*Wireless Protect Access*) com criptografia dinâmica (método de criptografia TKIP – *Temporal Key Integrity Protocol* e AES – *Advanced Encryption Standard*) (AMODEI, 2003).

Os dispositivos IEEE 802.11g tornam-se por vezes difíceis de configurar como *Home Gateway*³, devido a sua frequência de rádio e outros sinais que podem interferir na transmissão da rede sem fio.

Outra diferença do padrão 802.11g em relação ao 802.11b está no tratamento mais apropriado da reflexão dos sinais de rádio que colidem com diferentes tipos de materiais (plantas, construções, água, etc) com velocidades e angulações diferentes. Neste caso, as reflexões diferentes de um mesmo sinal, ao chegarem no mesmo conjunto de dados em intervalos diferentes são reorganizadas pelo receptor. O 802.11g (assim como no 802.11a) divide o espectro para que os receptores possam tratar estas reflexões de modo mais simples e mais efetivo que no 802.11b (KHAN; KHWAJA, 2003).

Mesmo com melhor tratamento do sinal, o 802.11g sofre as mesmas interferências do padrão 802.11b, devido a ocupação da faixa de 2,4 GHz. Interferências e problemas relacionados à frequência de 2,4 GHz têm se tornado a maior preocupação e frustração por parte dos usuários. Assim como ocorre com o 802.11b, o 802.11g suporta 14 (quatorze) canais, sendo somente 3 (três) não sobrepostos nos países de FCC (*Federal Communications Commission*) e 4 (quatro) nas nações europeias. Comparado ao padrão IEEE 802.11a, que tem 8 (oito) canais não sobrepostos internos, observa-se que o padrão 802.11g não deve ser a tecnologia mais adequada para locais com grande número de usuários e dispositivos sem fio, ou seja, altamente compartilhado (GASPARINI, 2007).

2.1.4 Padrão IEEE 802.11n

O IEEE aprovou oficialmente a versão final do padrão para redes sem fio 802.11n em setembro de 2009 (IEEE Std. 802.11n). Vários produtos surgiram no mercado antes do padrão IEEE 802.11n ser oficialmente lançado, no qual foram projetados (estes produtos) com base em um rascunho (*draft*) deste padrão. Há a possibilidade de equipamentos IEEE 802.11n que chegaram ao mercado antes do lançamento do padrão oficial serem incompatíveis com a sua versão final. Basicamente todos os equipamentos projetados com base no pré-projeto (*draft 2.0*) são compatíveis com a versão final do padrão IEEE 802.11n (DeBEASI, 2008). Porém, estes equipamentos possivelmente precisarão de um *upgrade de firmware* para serem 100% compatíveis com o padrão final (CRUZ et al., 2009).

³ *Home Gateways* – são *gateways* ou dispositivos domésticos que fazem a mediação entre as fronteiras da rede do operador e dos clientes (CRUZ et al., 2009).

O padrão IEEE 802.11n promete ser o padrão sem fio para distribuição multimídia, pois oferecerá, através de MIMO (*Multiple Input, Multiple Output* – Múltiplas Entradas e Múltiplas Saídas), taxas mais altas de transmissão de dados (até 600 Mbps) (LEE; CHOI, 2008), maior eficiência na propagação do sinal (com uma área de cobertura de até 400 metros *outdoor*) e ampla compatibilidade com demais protocolos 802.11. O 802.11n atende tanto as necessidades de transmissão sem fio para o padrão HDTV (*High-Definition Television*, TV de alta definição), como de um ambiente altamente compartilhado (empresas e residências) (BARTHOLD, 2008).

Para o padrão 802.11n utiliza-se de transmissão *multi-streams* para aumentar consideravelmente a taxa de transmissão de dados sem fio. *Streams* são fluxos de dados transmitidos por cadeias de rádio simultaneamente. Com isso, a tecnologia 802.11n tem de suportar por padrão no mínimo 2 *streams* (para taxa máxima de 300 Mbps), ou seja, ter a capacidade de transmitir ao menos em dois fluxos de dados simultaneamente no mesmo canal e no máximo 4 *streams* (capacidade máxima de transmitir 4 fluxos de dados simultaneamente). Com a transmissão de 4 fluxos simultâneos o padrão prevê uma taxa de transmissão máxima de 600 Mbps (Wi-Fi Alliance, 2009).

2.2 Redes Sem Fio Padrão IEEE 802.16 (WiMAX / WMAN)

O padrão 802.16 foi aprovado em 2002 e também é conhecido como WiMAX (*Worldwide Interoperability for Microwave Access* - Interoperabilidade Mundial para Acesso de Micro-ondas). É semelhante ao 802.11 no aspecto de oferecer comunicação sem fio de banda larga, mas difere na distância de alcance do sinal e tipo de usuário final, que na concepção do padrão era apenas para clientes fixos (torres e edifícios) e atualmente vêm sendo desenvolvidos padrões para usuários móveis também (*laptops* e celulares) (ROH; YANOVER, 2009).

O padrão sem fio 802.16 está a caminho de revolucionar a indústria de acesso de Banda Larga sem fio e também é conhecido como a interface aérea da IEEE para *Wireless Metropolitan Area Network* (WMAN), ou seja, rede metropolitana sem fios.

Esta tecnologia foi especificada pelo grupo do IEEE que trata de acessos de banda larga para última milha (*last mile*) em áreas metropolitanas, com padrões de desempenho equivalentes às das redes de transmissão tradicionais, tais como DSL (Digital Subscriber Line), Cable modem ou E1/T1. A Figura 2.4 mostra utilização do padrão 802.16 capaz de

substituir as tecnologias a cabo para acesso a Internet em diversas aplicações (INTEL, 2003).

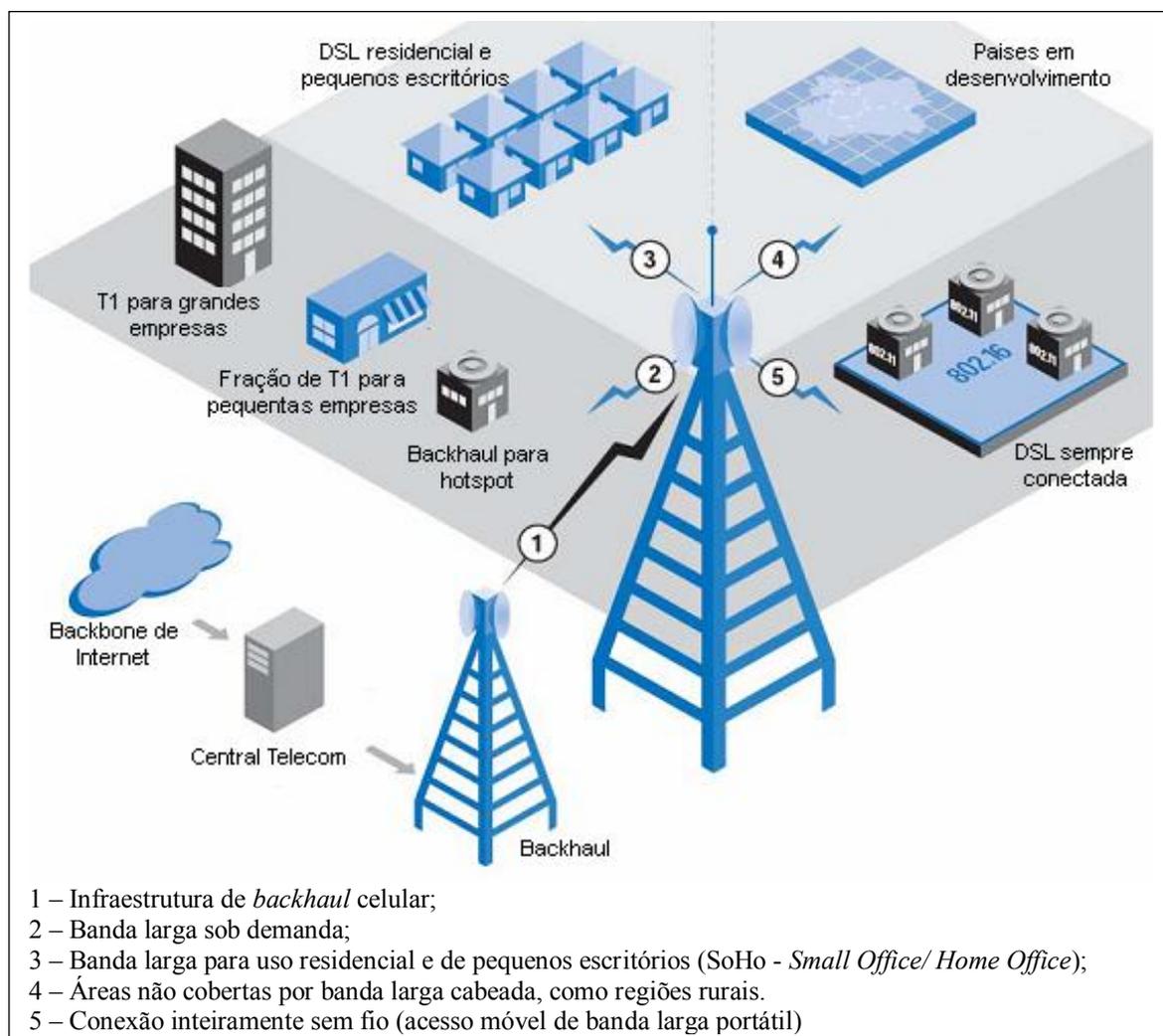


Figura 2.4 - Padrão IEEE 802.16 como solução para diversos segmentos de acesso à banda larga (INTEL, 2003).

Inicialmente, o padrão IEEE 802.16 definido em dezembro de 2001 previa uma faixa de operação entre 10 e 66 GHz, com linha de visada, taxa de transmissão de 32 a 134 Mbps e largura de faixa de 28 MHz (WiMAX Forum, 2008).

Em conjunto com essa tecnologia, surgiu também o WiMAX Fórum, uma organização sem fins lucrativos, formada por empresas fabricantes de equipamentos e de componentes com o objetivo de promover em larga escala a utilização de redes ponto-multiponto, operando em frequências entre 2 e 11 GHz, alavancando a padronização IEEE 802.16 e garantindo a compatibilidade e interoperabilidade dos equipamentos que operem com este padrão.

O WiMAX Fórum é o equivalente ao Wi-Fi *Alliance*, responsável pelo grande

desenvolvimento e sucesso do Wi-Fi em todo o mundo (INTEL, 2003). O WiMAX Fórum tem por objetivo criar um mercado de acesso Banda Larga mais competitivo, através de um conjunto mínimo de especificações de desempenho da interface de rádio entre os produtos de diversos fabricantes, certificando os produtos que atendem a estas especificações. A seguir, são descritos os pontos principais dos padrões mais conhecidos para as redes WiMAX.

2.2.1 Padrão IEEE 802.16a

Definido em janeiro de 2003, o padrão IEEE 802.16a prevê operação nas faixas entre 2 e 11 GHz, sem linha de visada (NLOS - *Non Line Of Sight*), taxa de transmissão máxima de 75 Mbps e largura de faixa de 20 MHz (diferenciando do padrão inicial que previa 134 Mbps de taxa de transmissão de dados e 28 MHz de largura de faixa) (IEEE 802.16a Std).

Este padrão apresenta a tecnologia apropriada para transmissão sem fios com obstáculos como árvores e edifícios. As estações podem ser montadas em residências ou edifícios, ao invés de torres. O 802.16a também fornece tecnologia de baixa latência para serviços sensíveis ao retardo, tais como circuitos de tráfego de voz com comutação ou voz sobre IP (VoIP), o transporte otimizado para vídeo e priorização de tráfego de dados. Isto é especialmente importante para as empresas que necessitam transportar dados de voz, além de serviços de dados comuns de seu provedor de serviços de banda larga (RAICHURA, 2003).

2.2.2 Padrão IEEE 802.16c

O padrão IEEE 802.16c surgiu em janeiro de 2003, com o intuito de padronizar a interoperabilidade da tecnologia WiMAX entre os diversos fabricantes de equipamentos (FIGUEIREDO, 2011), resultado do trabalho da IEEE *Task Group C* (TGc) iniciado em dezembro de 2002. A documentação foi desenvolvida para redes sem fio que operam em bandas de rádio frequência (RF) licenciadas⁴ e não licenciadas⁵ entre 2 e 10 GHz. A norma define detalhadamente o perfil do sistema, a forma de avaliação de desempenho e testes, porém a cobertura máxima não é superior a 5 km (ALI; HASSANEIN, 2007).

Este padrão (IEEE 802.16c) também melhorou a qualidade de serviço (QoS) e a camada de controle de acesso ao meio (MAC), juntamente com a adição de suporte para a norma europeia *HiperMAN* (*High Performance Radio Metropolitan Area Network*) para as

⁴ As frequências **licenciadas** no Brasil são de 3,5 GHz e 10,5 GHz [Prado, 2004].

⁵ As frequências **não licenciadas** no Brasil são de 2,4 GHz e 5,8 GHz [Prado, 2004].

redes WiMAX (HOYMANN; PÜTTNER; FORKEL, 2003). Acrescentou-se também ao padrão 802.16 o número de camadas físicas (PHY) e protocolos de transporte suportados, tais como IP, *Ethernet* e ATM (ALI; HASSANEIN, 2007).

2.2.3 Padrão IEEE 802.16d

Criado no primeiro trimestre de 2004, o padrão IEEE 802.16d trouxe algumas modificações no padrão 802.16a e melhorias na interoperabilidade (IEEE 802.16c) entre os fabricantes de equipamentos. Ratificado em junho de 2004, é o resultado do aprimoramento de padrões anteriores, tornando-os obsoletos. Entre as alterações, destaca-se o suporte para antenas MIMO (*Multiple Input – Multiple Output*) que aumenta a confiabilidade do alcance através de múltiplos percursos (WALKE; MANGOLD; BERLEMANN, 2006).

O padrão IEEE 802.16d, também conhecido por WiMAX Nomádico (ou fixo), teve seus primeiros equipamentos homologados em janeiro de 2006 pelo laboratório espanhol Cetecom. Seu funcionamento é semelhante ao IEEE 802.16a, nas frequências entre 2 e 11 GHz, porém o IEEE 802.16d não é capaz de efetuar *handoff*⁶ rápido entre as Estações Rádio Base (ERBs), ou seja, não é possível mudar de ERB quando os usuários em movimento, estão transferindo dados em altas taxas de *bytes*, sem interromper a conexão. Sua taxa de transmissão também fica em torno dos 75 Mbps e utiliza canais de 20 MHz. Quanto ao alcance deste padrão, estima-se que seja de 8 a 12 km com cobertura NLOS (sem visada) e entre 30 e 40 km com cobertura LOS (*Line Of Sight*, com visada direta) (ALI; HASSANEIN, 2007).

Utiliza-se a modulação OFDM (*Orthogonal Frequency Division Multiplexing*) por apresentar as características fundamentais para que o padrão 802.16d seja capaz de suportar operação sem linha de visada. O OFDM é uma técnica de multiplexação de informações que utiliza conjuntos de subcanais modulados por subportadoras de banda estreita e ortogonais entre si, o que proporciona um alto desempenho nas taxas de transmissão (FIGUEIREDO, 2011).

Nesta modulação (OFDM), uma sequência de *bits* transmitida com taxa de R *bits/s* é multiplexada em N subcanais, tem-se na transmissão R/N *bits/s* para cada subportadora. As subportadoras ortogonais entre si possibilitam a utilização de equalizadores

⁶ *Handoff* – processo de mudança do canal (frequência, horário, código de espalhamento, estação rádio base, ou a combinação deles) associado com a conexão atual, para uma chamada em curso (ZENG; AGRAWAL, 2002).

mais simples nos receptores, pois o canal de rádio distorce uniformemente cada subcanal, e para equalizá-los é preciso somente uma amplificação do sinal recebido, ao contrário de um sinal transmitido por um sistema de portadora única, pois o equalizador necessita de características mais complexas para a recomposição do sinal original.

No Brasil o WiMAX está regulamentado pela Anatel (Agência Nacional de Telecomunicações - órgão cujas principais atribuições são a implementação e fiscalização da política nacional de telecomunicações) para operar nas frequências de 2,6 GHz (Resolução 429 de 13 de fevereiro de 2006), 3,5 GHz (Resolução 416 de 14 de outubro de 2005) e 5 GHz (Resolução 506 de 1º de julho de 2008).

A empresa Intel executou em Minas Gerais (nas cidades de Belo Horizonte e Ouro Preto em 2005), testes com equipamentos WiMAX a fim de se observar o comportamento desta tecnologia com relevos montanhosos como os dessas cidades. O teste foi considerado um sucesso, utilizando-se equipamentos que operavam na frequência de 3,5 GHz e sem visada direta (NLOS) (LADOCICCO, 2007).

A empresa Embratel, anunciou em 18 de março de 2008, a primeira fase de um projeto WiMAX que atenderia 12 cidades (Belém, Belo Horizonte, Brasília, Curitiba, Fortaleza, Goiânia, Porto Alegre, Recife, Rio de Janeiro, Salvador, São Luís e São Paulo) com um volume de investimentos da ordem de R\$ 175 milhões (EMBRATEL, 2008). Porém pouco se sabe sobre este teste, pois a empresa não divulgou os fabricantes dos equipamentos utilizados e os resultados obtidos.

O futuro do WiMAX, segundo um estudo chamado *“WiMAX Network Equipment and Subscribers Market Outlook”* desenvolvido pela *Infonetics Research* (empresa de consultoria e pesquisa internacional), onde se avaliou as regiões alvo e os países no mundo que têm forte potencial para mercados de WiMAX fixo e móvel, o número de assinantes de WiMAX no Brasil crescerá 940%, partindo de menos de mil usuários (assinantes) em 2007, para 3,6 milhões em 2011. Esta avaliação leva em consideração tanto o alto índice populacional, quanto a demanda por banda larga que não é atendida pelas tecnologias existentes.

2.2.4 Padrão IEEE 802.16e

Ratificado em dezembro de 2005, o 802.16e (também conhecido como WiMAX Móvel) é capaz de efetuar *handoff* entre as ERBs e estações móveis em alta velocidade, para

até 150 km/h. Porém, sua taxa de transmissão é inferior ao dos padrões 802.16a e 802.16d. Com canais de 5 MHz, consegue-se taxas próximas a 15 Mbps (ALI; HASSANEIN, 2007).

Utiliza-se SOFDMA (*Scalable Orthogonal Frequency Division Multiplexing Access*), uma técnica de modulação multiportadora que usa subcanalização (PRASAD; VELEZ, 2010). Operou inicialmente nas frequências de 2,3 GHz, 2,5 GHz, 3,3 GHz e 3,5 GHz com canais de 5, 7, 8, 10 e 75 MHz. Posteriormente, o WiMAX Fórum decidiu incluir também a frequência de 700 MHz (WiMAX FORUM, 2008).

O SOFDMA (ou S-OFDMA) adiciona escalabilidade para OFDMA, dimensionando o tamanho da FFT (*Fast Fourier Transform* - Transformada Rápida de Fourier) para a largura do canal, mantendo constante o espaçamento da frequência por subportadora através de diferentes canais em larguras de banda. O tamanho da FFT equivale ao número de subportadoras, ou seja, um sistema OFDM / OFDMA com 256 subportadoras, o tamanho da FFT é 256. Quanto menor o tamanho dado ao canal FFT, menor o canal da largura de banda, enquanto maior o tamanho da FFT, maior o canal da largura de banda. Ao fazer o espaçamento de frequência por subportadora constante, o SOFDMA reduz a complexidade do sistema de canais menores e melhora o desempenho dos canais maiores (YAGHOUBI, 2004).

Para o WiMAX, tem-se também a IFFT (*Inverse Fast Fourier Transform*, Transformada Rápida Inversa de Fourier), que se utiliza no transmissor para criar uma forma de onda de fluxos OFDM modulados de dados, enquanto que a FFT é usada no receptor WiMAX para demodular os fluxos de dados (CHEN; LIN; LEE, 2006).

O padrão 802.16e acrescenta uma modulação OFDMA 2K-FFT, 512-FFT e uma capacidade de 128 FFT. A subcanalização é utilizada para configuração da distância de alcance do concentrador, proporcionando às operadoras a capacidade de dinamicamente reduzir o número de canais enquanto aumenta o ganho do sinal para cada canal a fim de atingir os clientes mais distantes. O inverso também é possível, ou seja, à medida que um usuário se aproxima de uma célula (ERB), o número de canais aumenta e a modulação também muda para aumentar a largura de banda (ROH; YANOVER, 2009; JHA; PRASAD, 2007).

A versão de WiMAX 802.16e também incorpora suporte para antenas MIMO, bem como *Beamforming* (técnica de processamento de sinal) e AAS (*Advanced Antenna Systems* – Sistema Avançado de Antena), que são tecnologias inteligentes que melhoram significativamente o ganho da antena e a vazão (*throughput*) em sistemas WiMAX (ALI;

HASSANEIN, 2007).

Utiliza-se o padrão 802.16e é utilizado principalmente em frequências licenciadas para aplicações puramente móveis. Muitas empresas optaram por desenvolver o padrão 802.16e, exclusivamente para as versões fixa e móvel. A versão de WiMAX IEEE 802.16e é a tecnologia de rede móvel mais próxima do padrão Wi-Fi (PRASAD; VELEZ,2010).

2.2.5 Padrão IEEE 802.16m

A crescente demanda por Internet móvel e aplicativos de multimídia sem fio tem estimulado o desenvolvimento de tecnologias de banda larga de acesso sem fio nos últimos anos. O IEEE 802.16m se mostrou apropriado para este campo, com implantações mistas para a utilização de Estações Móveis (EM) e Estações Rádio Base (ERB). O recurso de compatibilidade com versões anteriores permite mudanças suaves para o atualizações e migrações de sistemas, além de permitir conexões em *roaming* através da utilização de métodos adequados de interoperabilidade entre fabricantes (AHMADI, 2009).

Item	Requisito
Largura de banda de operação <i>Duplex</i>	Largura de banda escalável entre 5 e 20 MHz <i>Full-duplex FDD, Half-duplex FDD, TDD</i>
Pico de taxa de dados normalizado	<i>Downlink: >8,0 bps/Hz, Uplink: >2,8 bps/Hz</i>
Tempo de interrupção de <i>handover</i>	Intra-frequência: Máx. 30 ms, Inter-frequência: Máx. 100 ms
<i>Throughput</i> usuário	<i>Downlink: >2 x 802.16e,</i> <i>Uplink: > 2 x 802.16e</i>
Mobilidade	Máxima de 350 km/h

Tabela 2.5 - Requisitos IEEE 802.16m (LEE; CHOI, 2008)

O WiMAX Fórum também definiu um roteiro de evolução do WiMAX móvel, e em conformidade com a normalização 802.16m (ver Tabela 2.5), planeja desenvolver o perfil do sistema WiMAX móvel 2.0. Além deste perfil, algumas especificações de rede WiMAX desenvolvidas pelo WiMAX Fórum serão a base da certificação do WiMAX versão 2.0 (LEE; CHOI, 2008).

2.3 Redes Com Fio Padrão IEEE 802.3 (*Ethernet*)

A Internet foi criada para redes geograficamente distribuídas, porém muitas universidades e organizações possuíam grande número de computadores que deveriam estar conectados. Para resolver essa questão, surgiu em 1972 nos laboratórios da Xerox com Robert Metcalfe o padrão *Ethernet*. No início todas as estações compartilhavam o mesmo meio de transmissão (cabo coaxial) e a configuração de conexão foi a de barramento com taxa de transmissão de 2,94 Mbps (TANENBAUM, 2003; DIAS; ALVES JR., 2002).

O modo de transmissão é uma característica importante e pode ser um dos três apresentados abaixo (DIAS; ALVES JR., 2002):

- *Simplex*: durante todo o tempo apenas uma estação transmite, a transmissão é feita unilateralmente;
- *Half-duplex*: cada estação transmite ou recebe informações, não acontecendo transmissão simultânea;
- *Full-duplex*: cada estação transmite e/ou recebe, podendo ocorrer transmissões simultâneas.

A estrutura física apresenta três topologias de rede distintas, conforme se apresenta abaixo:

- Barramento: utiliza cabo coaxial fino ou grosso;
- Estrela: utiliza cabo de par trançado;
- Árvore: misto entre barramento e estrela;

A distância máxima da rede e taxa máxima de dados de uma rede com fio depende do material utilizado na construção do cabo. Com o passar dos anos o meio físico também sofreu alterações, com materiais novos e maior alcance dos cabos. A Tabela 2.6 mostra a evolução das distâncias permitidas com cada taxa de transmissão máxima.

Tipo de cabo	10 Mbps	100 Mbps	1 Gbps	10 Gbps
Fibra monomodo	25 km	20 km	3 km	40 km
Fibra multimodo	2 km	3 km	500 m	300 m
Coaxial	500 m	100 m	25 m	-
Par trançado (categoria 5)	100 m	100 m	100 m	-

Tabela 2.6 - Taxa de transmissão de dados e comprimento máximo por material (DIAS; ALVES JR., 2002)

As séries de tráfego utilizadas neste trabalho provenientes de redes com fio serão

descritas com maiores detalhes no Capítulo 4.

2.4 Resumo do Capítulo

Neste capítulo, apresentou-se os principais padrões desenvolvidos para as tecnologias de redes sem fio Wi-Fi (IEEE 802.11) e WiMAX (IEEE 802.16), responsáveis pelo aumento significativo no número de usuários para o mercado de telecomunicações. Estas redes possuem peculiaridades em relação às redes cabeadas e até mesmo entre os diferentes padrões de rede sem fio, como taxa de transmissão de dados e cobertura do sinal.

Também foram apresentadas as principais técnicas de modulação, protocolos, vantagens e desvantagens, além das distâncias de cobertura do sinal e taxas de transmissão de dados para os padrões IEEE 802.11 a/b/g/n e IEEE 802.16 a/c/d/e/m.

Apresenta-se também uma breve explicação a respeito das redes com fio padrão 802.3 e suas principais taxas de transmissão e tipos de cabos utilizados para cada taxa.

CAPÍTULO 3

MODELAGEM E ESTIMAÇÃO DE PARÂMETROS DE FLUXOS DE TRÁFEGO DE REDES

Neste capítulo aborda-se a modelagem de tráfego de rede e os principais modelos baseados em teoria de fractais encontrados na literatura. A modelagem de tráfego é uma técnica utilizada para caracterizar fluxos de tráfegos de rede. O modelo de tráfego ideal deve apresentar características semelhantes às do tráfego de rede modelado. Estes modelos têm por objetivo facilitar o entendimento das características do tráfego modelado, parametrização das variáveis obtidas e possibilidade de simulações do comportamento do tráfego.

Na estimação de parâmetros de tráfegos de redes, estuda-se o comportamento dos pacotes na rede e assim classifica-se o modelo mais apropriado (a natureza do tráfego) para descrever o tráfego real. A modelagem de tráfego de rede ajuda no desenvolvimento de equipamentos, serviços e protocolos de rede, além de ter grande importância nas análises de desempenho e simulações de redes.

Este capítulo está organizado da seguinte forma: na seção 3.1, discute-se sobre modelagem de tráfego de rede. Na seção 3.2, apresenta-se o modelo de Poisson, que é um dos modelos de tráfego mais conhecidos na literatura. Na seção 3.3, apresenta-se o modelo fBm (*fractal Brownian motion*) que leva em conta as características monofractais do tráfego de rede, como o parâmetro de Hurst (seção 3.3.1) que define o grau de autossimilaridade da série. Apresenta-se também, o conceito de função de autocorrelação (seção 3.3.2) e suas particularidades. Na seção 3.4, descreve-se os processos multifractais e seus conceitos básicos. Na seção 3.5, apresenta-se o modelo mBm (*multifractal Brownian motion*), em conjunto com o expoente de Hölder, que é o parâmetro utilizado para definir o grau de regularidade local do tráfego (seção 3.5.1). Na seção 3.6, discursa-se sobre o modelo de

Cascatas Multiplicativas que leva em consideração as características multifractais do tráfego. Trata-se na seção 3.7 sobre o modelo MWM (*Multifractal Wavelet Model*) que é baseado em *wavelets* (RIEDI et al., 1999). Na seção 3.8, apresenta-se o modelo AWMM (*Adaptive Wavelet Based Multifractal Model*) baseado em modelos *wavelet* multifractais e na seção 3.9 apresenta-se o modelo CGMD (*Cascade with Generalized Multiplier Distributions*) que é baseado em cascatas multiplicativas. Por fim, na seção 3.10, apresenta-se o resumo sobre o capítulo.

3.1 Modelagem de Tráfego

Na década de 20 o modelo clássico de tráfego de Poisson foi proposto para análise de sistemas de telefonia e posteriormente ajustado para a análise de filas em redes de dados (KLEINROCK, 1975). Este modelo tem como vantagem o fato de ser analiticamente tratável, permitindo que expressões matemáticas sejam diretamente derivadas para caracterização do desempenho de fila nos *buffers*. Mas com a chegada das redes com suporte a vários serviços, a natureza do tráfego mudou drasticamente, exibindo características bem diferentes das sugeridas por modelos como o de Poisson e o de Markov, como por exemplo, o comportamento fractal (VIEIRA, 2006).

Leland et al. (1994) constataram experimentalmente que o tráfego coletado na rede *Ethernet* do *Bellcore Morristown Research and Engineering Center* exibia características fractais tais como autossimilaridade. A dependência de longa duração ou longa-dependência para uma série de tráfego é uma característica que implica em uma estrutura de correlação que decai mais lentamente do que uma exponencial (LELAND et al., 1994). Este decaimento da função de autocorrelação, relacionado também à autossimilaridade, foi observado no tráfego de redes de longa distância (WAN - *Wide Area Networks*), metropolitanas (MAN - *Metropolitan Area Network*) (PAXSON; FLOYD, 1995), tráfego Internet (CROVELLA; BESTAVROS, 1996), dentre outros. Constatou-se que estas propriedades, principalmente a dependência de longa duração, influenciam fortemente no projeto de redes e seu desempenho (PARK; WILLINGER, 2000), por isso não são coerentemente modeladas por processos estocásticos Markovianos (VIEIRA; GARCEZ, 2011).

Em estudos realizados com alta taxa de variação do tráfego Internet observaram-se rajadas variando em uma gama de escalas de tempo, contrariando a suposição de que rajadas de tráfego só existem em escalas curtas de tempo (PAXSON; FLOYD, 1995).

Mostrou-se nestes estudos que estas incidências de rajadas multiescalas têm um impacto significativo no desempenho das redes (ERRAMILI; NARAYAN; WILLINGER, 1996). Nos resultados apresentados por Erramilli, Narayan e Willinger (1996), observa-se que a aplicação do conhecimento das características do tráfego em múltiplas escalas consegue melhorar a eficiência dos mecanismos de controle de tráfego (VIEIRA, 2006).

Propôs-se em diversas referências, modelos de tráfego com o objetivo de representar as características autossimilares encontradas nas séries de tráfego de redes. Um modelo que pode apresentar de maneira simples e que abrange matematicamente as características autossimilares observadas no tráfego é o modelo de tráfego Browniano fracionário (*fractional Brownian traffic*, fBt). Contudo, verificou-se que em escalas de tempo da ordem acima de poucos segundos ou maiores, o comportamento do tráfego seria melhor representado por modelos autossimilares, mas em escalas de tempo menores, inferiores à ordem de poucos segundos, as características de tais modelos afastavam-se das apresentadas pelo tráfego real analisado (VIEIRA, 2006; BIANCHI, 2005).

Outras propriedades mais complexas do tráfego de redes que os modelos monofractais foram descobertas, como as características multifractais. Os resultados indicam que o desempenho das filas depende tanto da taxa de variação do tráfego em certas escalas de tempo, quanto do valor do parâmetro de Hurst H , que mede o grau de autossimilaridade de um processo (ERRAMILI; NARAYAN; WILLINGER, 1996). A origem dessas propriedades consideradas presentes em pequenas escalas de tempo é atribuída à ação dos protocolos predominantes nas redes e dos mecanismos de controle de congestionamento ponto a ponto existentes na Internet, que determinam o comportamento do fluxo de informações entre diferentes camadas na hierarquia de protocolos TCP/IP (FELDMANN; GILBERT; WILLINGER, 1998).

Investigações envolvendo tráfego WAN TCP/IP constataram que essas diferentes propriedades e comportamentos do tráfego podem ser convenientemente descritos utilizando-se a análise multifractal (RIEDI; VÉHEL, 1997). Para muitos processos de tráfego de rede, seus gráficos de energia em escala dos coeficientes *wavelet* ou os de variância-tempo normalmente não têm comportamento linear. Muitos destes processos apresentam uma combinação de comportamentos fractais, com o parâmetro de Hurst variando em pequenas e diferentes escalas de tempo, ou seja, características multifractais. De fato, o desempenho de fila depende intensamente das irregularidades do tráfego em escalas de tempo pequenas devido à dinâmica complexa das redes de dados. Pesquisadores discutem que esta combinação

de comportamentos em escala é melhor representada por processos multifractais (FELDMANN; GILBERT; WILLINGER, 1998).

Conhecendo as características principais do tráfego, pode-se selecionar o modelo de rede que melhor representará a série de tráfego de rede, sendo possível incorporar às simulações, métodos analíticos e características semelhantes às reais. Em simulações de rede, deseja-se conhecer valores relacionados às variáveis aleatórias cuja obtenção direta seria muito difícil ou impossível. Geralmente utiliza-se dois tipos de estimação:

- Estimação pontual: quando se deseja estimar um único valor correspondente à quantidade de interesse;
- Estimação de intervalo: quando se deseja conhecer um intervalo no qual o parâmetro estimado esteja com nível de confiança dado.

As técnicas de estimação são utilizadas também para determinar parâmetros das distribuições dos dados de entrada obtidos experimentalmente.

Para se gerenciar o tráfego de redes é preciso uma forma de detectar a existência de erros de transmissão (erro de *bit*). A detecção de congestionamento pode ser dificultada pelos erros de transmissão, ou seja, ao invés do pacote ter sido descartado por causa de congestionamentos na rede, o motivo pode ter sido erro de transmissão, fazendo com que o pacote seja perdido e depois retransmitido. Atualmente, a perda de pacotes devido a erros de transmissão é pouco frequente, porque a maioria dos troncos de longa distância é de boa qualidade como, por exemplo, de fibra óptica (embora também existam enlaces de redes sem fios ou fios de cobre). Como consequência, a maior parte dos erros de transmissão na Internet se deve aos congestionamentos de dados (TANENBAUM, 2003).

3.2 Modelo de Poisson

O processo de Poisson é empregado na modelagem de processos físicos e desempenha um papel central na teoria de filas clássica. A razão para seu uso está no fato de que o modelo de Poisson possui uma série de propriedades que dão origem a resultados confiáveis de estimativa de filas. Em segundo lugar, também é considerado um bom modelo para um processo que envolve a chegada de um grande número de usuários similares e independentes (HOCK; HEE, 2008).

Mais precisamente, um processo de Poisson é um processo de contagem do número de eventos que ocorrem de forma aleatória dos pontos observados em um

determinado intervalo de tempo $(0, t)$. Também se pode considerar como sendo um caso de limite de colocação em pontos aleatórios k para o intervalo de tempo de $(0, t)$. Se a variável aleatória $X(t)$ contendo o número de eventos em um intervalo de tempo distribuído de acordo com a distribuição de Poisson, então esse processo é um processo de Poisson (HOCK; HEE, 2008). A probabilidade de $X(t)$ ser igual a k segundo o modelo de Poisson é dada por:

$$P\{X(t) = k\} = \frac{e^{-\lambda t} (\lambda t)^k}{k!} \quad (3.1)$$

onde k é o número inteiro não negativo que representa o número de ocorrências, λ é a taxa de ocorrência destes eventos pontuais e λt é a média de uma variável aleatória de Poisson, que fisicamente representa o número médio de ocorrências do evento em um intervalo de tempo t .

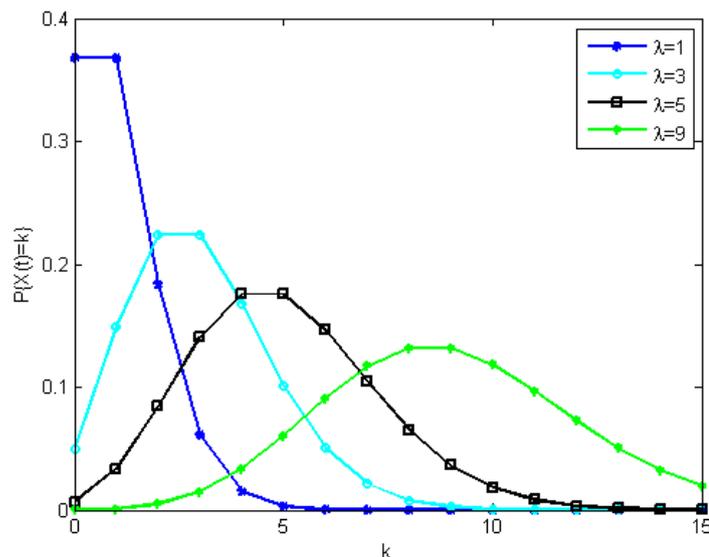


Figura 3.1 - Densidade de probabilidade para diferentes valores de λ

A Figura 3.1 apresenta a Função Densidade de Probabilidade (PDF– *Probability Density Function*) obtida pela equação (3.1) para diferentes taxas de ocorrência (λ).

3.3 Modelo Movimento Browniano Fractal (fBm)

No verão de 1827, Robert Brown, botânico e médico escocês, observou ao microscópio minúsculos grãos de pólen de plantas suspensas em um fluido e notou incrementos altamente irregulares. Verificou-se que partículas mais finas moviam-se mais rapidamente, e que o movimento era estimulado pelo calor e pela diminuição da viscosidade

do líquido. Suas investigações foram publicadas em *—A Brief Account of Microscopical Observations Made in the Months of June, July and August 1827—* (Um breve relato de observações microscópicas feitas nos meses de junho, julho e agosto de 1827). Ainda naquele século, foi postulado que o movimento irregular era causado por um grande número de colisões entre os grãos de pólen e as moléculas do líquido (que são microscopicamente pequenos em relação ao pólen). Os impactos ocorrem com muita frequência mesmo em pequenos intervalos de tempo, independentemente umas das outras, e o efeito de um acerto particular é considerado pequeno se comparado ao efeito total (WIERSEMA, 2008).

Por volta de 1900, Louis Bachelier, um estudante de doutorado em matemática na Sorbonne (Universidade de Paris), foi estudar o comportamento dos preços das ações na bolsa de Paris e observou incrementos altamente irregulares. Ele desenvolveu a primeira especificação matemática do processo de incrementos relatado por Brown, que foi usado como um modelo para o incremento dos preços das ações. Na década de 1920, Norbert Wiener, um físico matemático do MIT (*Massachusetts Institute of Technology*), desenvolveu a estrutura matemática totalmente probabilística para este modelo. Este tipo de incremento passou a ser chamado de movimento Browniano ou processo de Wiener. A proposição do processo é comumente denotada por B ou movimento Browniano W (WIERSEMA, 2008).

O nome movimento Browniano fractal veio com os pesquisadores Mandelbrot e Van Ness. Eles o definiram como uma integral estocástica relacionada ao movimento Browniano padrão (MANDELBROT; NESS, 1966; SOTTINEN; VALKEILA, 2001):

$$Z_t = \int_{-\infty}^t k(t,s)dW_s \quad (3.2)$$

para um dado *kernel* determinístico k dependente de H (parâmetro de Hurst), onde W representa um processo de Wiener (movimento Browniano padrão) definido em $(-\infty, \infty)$, e t e s são dois instantes de tempo (intervalos de tempo).

Além da representação pela integral de Mandelbrot e Van Ness do movimento Browniano fractal, utiliza-se também representação semelhante onde a integração assume um intervalo finito $[0, t]$ (SOTTINEN; VALKEILA, 2001; WIERSEMA, 2008):

$$Z_t = \int_0^t z(t,s)dW_s \quad (3.3)$$

onde:

$$z(t, s) = c_1 \left[\left(\frac{t}{s} \right)^{H-\frac{1}{2}} (t-s)^{H-\frac{1}{2}} - \left(H - \frac{1}{2} \right) s^{\frac{1}{2}-H} \int_s^t u^{H-\frac{3}{2}} (u-s)^{H-\frac{1}{2}} du \right] \quad (3.4)$$

onde c_1 é a constante normalizada do grau de certeza de H (parâmetro de Hurst) e t e s são dois instantes de tempo (intervalos de tempo).

Um movimento Browniano fractal (fBm), é um processo Gaussiano de tempo contínuo $B_H(t)$ em $[0, T]$, que começa em zero, tem média zero em $[0, T]$, apresentando a seguinte função de covariância (PRAKASA, 2010):

$$E[B_H(t)B_H(s)] = \frac{1}{2} \left(|t|^{2H} + |s|^{2H} - |t-s|^{2H} \right) \quad (3.5)$$

onde H é o parâmetro de Hurst (um número real entre 0 e 1), e seu valor determina algumas características importantes para o processo fBm.

Para $H = 1/2$, os incrementos são independentes, para $H > 1/2$ os incrementos são positivamente correlacionados (o processo é dito como sendo autossimilar) e para $H < 1/2$ os incrementos são negativamente correlacionados (não existe autocorrelação) (MISHURA, 2008; CLEGG, 2005).

A integral estocástica para $t \geq 0$ definida por Mandelbrot e Van Ness também pode ser definida pela equação (PELTIER; VÉHEL, 1995):

$$B_H(t) = \frac{1}{\Gamma(H+1/2)} \left\{ \int_{-\infty}^0 [(t-s)^{H-1/2} - (-s)^{H-1/2}] dW(s) + \int_0^t (t-s)^{H-1/2} dW(s) \right\} \quad (3.6)$$

onde W representa um processo de Wiener definido em $(-\infty, \infty)$.

Os fractais são estruturas complexas caracterizadas por três aspectos sempre presentes. O primeiro é quanto à classificação dos fractais, por meio do conceito de dimensão fractal, que representa uma ruptura com a geometria e as topologias tradicionais, pois permite que um objeto tenha como dimensão um valor não inteiro. A segunda característica dos fractais é a autossimilaridade, onde um fractal é invariante por mudança de escalas, ou seja, se uma parte do fractal for ampliada, tem-se uma figura similar a figura que se tinha antes. A terceira característica diz respeito à maneira como os fractais são construídos. Na construção de um fractal, um determinado procedimento se repete indefinidamente (WILLINGER et al., 1995). A Figura 3.2 mostra um exemplo de fractal.



Figura 3.2 - Polígono composto de cópias repetidas de um pentagrama (LAUWERIER, 1991)

3.3.1 Parâmetro de Hurst

O parâmetro de Hurst é utilizado em várias áreas da matemática aplicada, incluindo os fractais e a Teoria do Caos (OLIVEIRA; MENDES, 2006). Utiliza-se também para caracterizar processos de memória longa e na análise espectral. A estimativa do parâmetro de Hurst foi originalmente desenvolvida em hidrologia e tem sido aplicado em áreas que vão desde a biofísica até redes de computadores. Porém, as modernas técnicas para estimação do parâmetro de Hurst vêm da matemática fractal (OLIVEIRA; MENDES, 2006).

Embora o parâmetro de Hurst seja bem definido matematicamente, a sua estimação é problemática. Todos os estimadores são vulneráveis às tendências dos dados, a periodicidade e outras fontes de erros. Muitos estimadores assumem formas específicas para cada aplicação. Neste trabalho, utilizou-se o *software* SELFIS para estimação do parâmetro de Hurst. O SELFIS (*Self-similarity analysis*, análise de autossimilaridade) é um *software* baseado em Java para a estimação de autossimilaridade e análise de tráfego LRD (*Long Range Dependency*, Longa dependência). Este *software* é distribuído gratuitamente à comunidade (disponível em <http://alumni.cs.ucr.edu/~tkarag>) e atualmente, integra várias metodologias de estimação de LRD (KARAGIANNIS, 2010).

3.3.2 Função de Autocorrelação

A função de autocorrelação representa o grau de correlação de uma variável, em um instante de tempo, com ela mesma e em um instante de tempo posterior. Esta função

permite que se analise o grau de irregularidade de um sinal (SILVA FILHO; LIMA, 2008).

A função de autocorrelação $\rho(k)$ para uma série estacionária $\{X_t : t \in N\}$ é dada pela equação (CLEGG, 2005):

$$\rho(k) = \frac{E[(X_t - \mu)(X_{t+k} - \mu)]}{\sigma^2} \quad (3.7)$$

onde $E[\cdot]$ representa o operador esperança matemática, μ e σ^2 são respectivamente, a média e a variância de X_t . As séries de tempo X_t são ditas de longa dependência se $\sum_{k=-\infty}^{\infty} \rho(k)$ divergir. Muitas vezes, a forma da função de autocorrelação pode ser especificada por (CLEGG, 2005):

$$\rho(k) \approx C_\rho k^{-\alpha} \quad (3.8)$$

onde a constante de autocorrelação é $C_\rho > 0$ e $\alpha \in (0,1)$ e o símbolo \approx significa assintoticamente igual, para $f(x) \approx g(x) \rightarrow \frac{f(x)}{g(x)} = 1$ com $x \rightarrow 0$ (CLEGG, 2005). O parâmetro α é relacionado ao parâmetro de Hurst e dado pela equação (BATISTA, 2006):

$$\alpha = 2 - 2H \quad (3.9)$$

3.4 Processos Multifractais

A teoria multifractal foi apresentada por Mandelbrot no contexto de turbulência nos anos 70. A partir de então a teoria multifractal passou a ser usada em vários campos como o processamento de imagem, geofísica, etc. Para o tráfego de redes ser considerado multifractal, é preciso uma estrutura de forte dependência inerente, com incidência de rajadas em várias escalas (PARK; WILLINGER, 2000). Quando encontradas essas características, o desempenho da rede é pior que o considerado por modelos Gaussianos e de curta-dependência. O conceito de multifractalidade se estende facilmente aos processos estocásticos (VIEIRA; LING, 2008).

Para um processo estocástico $X(t)$ ser multifractal é necessário que se satisfaça a equação (VIEIRA; LING, 2007):

$$E\left(|X(t)|^q\right) = c(q)t^{\tau(q)+1} \quad (3.10)$$

onde t e q são intervalos da reta real, $\tau(q)$ e $c(q)$ são funções no domínio Q . Além disso, supõe-se que T e Q possuem comprimentos positivos, e que $0 \in T, [0,1] \subseteq Q$.

A multifractalidade pode ser descrita em termos de momentos em que $\tau(q)$ é a função de escala e $c(q)$ é o fator de momento de um processo multifractal. Se $\tau(q)$ é linear em q , o processo é monofractal, senão é multifractal. Para processos autossimilares com parâmetro de Hurst H , pode-se mostrar que $\tau(q) = qH - 1$ e $c(q) = E(|X(1)|^q)$.

3.5 Modelo Movimento Browniano Multifractal (mBm)

O modelo mBm (movimento Browniano multifractal) introduzido em Peltier e Vêhel (1995) é uma generalização do modelo de movimento Browniano fractal (fBm). Esta generalização ocorre com a troca do parâmetro de Hurst (H) por uma função denominada expoente de Hölder $H(t)$, introduzindo uma dependência entre a regularidade local e o instante de tempo t . Ou seja, enquanto a regularidade local num processo fBm é a mesma (constante), em um processo mBm, ela varia ao longo do tempo, sendo também definida pelo valor do expoente de Hölder $H(t)$.

O expoente de Hölder é capaz de descrever o grau de singularidade local de um processo, o que é interessante para a caracterização das rajadas de dados em séries de tráfego de redes (GUÉVEL; VÉHEL, 2010).

Sejam (X, d_X) e (Y, d_Y) espaços métricos. Uma função $f: X \rightarrow Y$ é dita uma função de Hölder com expoente $\beta > 0$, se para cada $x, y \in X$ com $d_X(x, y) < 1$ tem-se:

$$d_Y(f(x), f(y)) \leq c \cdot d_X(x, y)^\beta \quad (3.11)$$

para qualquer constante $c > 0$.

O modelo mBm, apesar de ser uma generalização do processo fBm, possui algumas propriedades diferentes das encontradas no fBm. Um exemplo disso é a não estacionaridade dos incrementos do processo mBm. As propriedades do processo mBm são:

- Dada uma função de Hölder $H(t)$, o processo mBm $W(t)$ com $H(t)$ associada é contínuo;
- O processo mBm $W(t)$ com função de Hölder $H(t)$ associada apresenta autossimilaridade local (*local assintotic self-similar*) (MELO; FONSECA,

2004), ou seja :

$$\lim_{\rho \rightarrow 0^+} \left\{ \frac{W(t + \rho u) - W(t)}{\rho^{H(t)}} \right\}_{u \in \mathbb{R}^+} = \{B_{H(t)}(u)\}_{u \in \mathbb{R}^+} \quad (3.12)$$

onde $B_{H(t)}(u)$ é um processo fBm com parâmetro de Hurst $H = H(t)$, o valor da função $H(t)$ no instante de tempo t .

Seja $H : (0, \infty) \rightarrow (0, 1)$ uma função de Hölder com expoente $\beta > 0$. O movimento Browniano multifractal é um processo Gaussiano definido em $(0, \infty)$ e descrito por Peltier e Véhel (1995):

$$W_{H(t)} = \frac{1}{\Gamma(H(t) + 1/2)} \left\{ \int_{-\infty}^0 \left[(t-s)^{H(t)-1/2} - (-s)^{H(t)-1/2} \right] dB(s) + \int_0^t (t-s)^{H(t)-1/2} dB(s) \right\} \quad (3.13)$$

onde $B(s)$ representa o movimento Browniano.

3.6 Modelo Cascatas Multiplicativas

Um dos modelos que possuem características capazes de modelar as propriedades de um processo multifractal são as cascatas multiplicativas. A construção de uma cascata multiplicativa é baseada na criação iterativa do processo em escalas mais finas, a partir de escalas mais amplas, de forma multiplicativa.

O modelo de cascatas multiplicativas originou-se do modelo conhecido como cascata binomial. Este modelo (cascatas multiplicativas) é um método para se obter um processo multifractal, que consiste de um procedimento iterativo no intervalo compacto $[0, 1]$ e para m_0 e m_1 (multiplicadores da cascata) dois números positivos cuja soma é 1. No estágio inicial $k = 0$ da cascata, se obtém a medida inicial μ_0 do processo com distribuição de probabilidade uniforme em $[0, 1]$. No próximo estágio $k = 1$, a medida μ_1 distribui massa utilizando a distribuição uniforme, sendo m_0 no subintervalo $[0, 1/2]$ e massa igual a m_0 em $[1/2, 1]$. Em $k = 2$, o intervalo $[0, 1/2]$ é subdividido em $[0, 1/4]$ e $[1/4, 1/2]$ e o mesmo acontece com intervalo $[1/2, 1]$, assim (VIEIRA; LING, 2008):

$$\begin{aligned} \mu_2[0, 1/4] &= m_0 m_0 & \mu_2[1/4, 1/2] &= m_0 m_1 \\ \mu_2[1/2, 3/4] &= m_1 m_0 & \mu_2[3/4, 1] &= m_1 m_1 \end{aligned}$$

Considere o intervalo diádico $[t; t + 2^{-k}]$ em que $t = 0.\eta_1 \dots \eta_k = \sum_{i=1}^k \eta_i 2^{-i}$.

Sejam φ_0 e φ_1 as frequências relativas de 0's e 1's no desenvolvimento da cascata. A medida μ no intervalo diádico é dada por:

$$\mu[t, t + 2^{-k}] = m_0^{k\varphi_0} m_1^{k\varphi_1} \quad (3.14)$$

Este processo preserva a massa dos intervalos diádicos em cada estágio e por isso é chamado de cascata conservativa ou microcanônica. Em cada estágio da cascata os intervalos podem ser divididos em intervalos de $b \geq 2$ com tamanho igual. Este processo é definido como cascata multinomial. Se os multiplicadores usados tiverem valor fixo para m_0 e $b=2$, então a cascata multiplicativa é binomial determinística de função com escala: $\tau(q) = -\log_2(m_0^q + m_1^q) + 1$ (VIEIRA; LING, 2008).

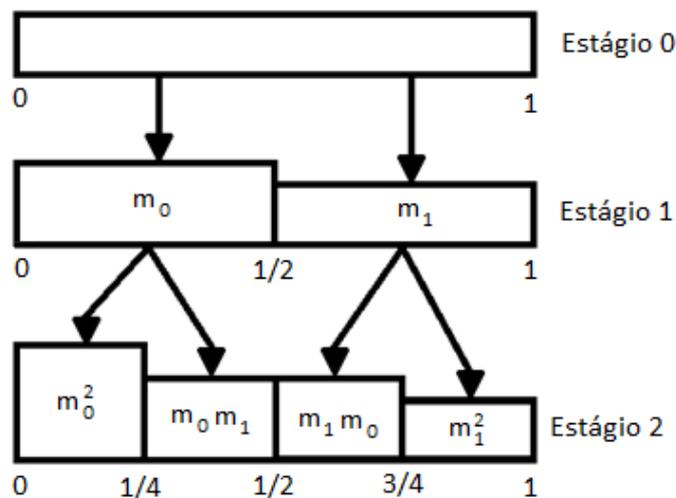


Figura 3.3 - Processo de construção da cascata binomial (VIEIRA; LING, 2008)

Ao se permitir que os multiplicadores da cascata r sejam variáveis aleatórias independentes em $[0, 1]$, com densidade de probabilidade $f_R(x)$, obtém-se uma estrutura mais geral que a determinística, onde os multiplicadores são valores fixos, conforme mostra a Figura 3.3. Desta forma, o processo multifractal obtido $\{\mu(\Delta t_k)\}_{k=1}^{2^N}$ terá no estágio k da cascata um intervalo diádico de comprimento $\Delta t_k = 2^{-k}$, que começa em $t = 0.\eta_1 \dots \eta_k = \sum_{i=1}^k \eta_i 2^{-i}$, a medida μ :

$$\mu(\Delta t_k) = R(\eta_1).R(\eta_1, \eta_2), \dots, R(\eta_1, \dots, \eta_k) \quad (3.15)$$

onde $R(\eta_1, \dots, \eta_i)$ é o multiplicador no estágio k da cascata. Uma vez que os multiplicadores r são independentes e identicamente distribuídos (i.i.d), pode-se demonstrar que a medida μ satisfaz a seguinte relação de escala:

$$E(\mu(\Delta t_k)^q) = (E(R)^q)^k = \Delta t_k^{-\log_2 E(R^q)} \quad (3.16)$$

Esta relação define um processo multifractal com função de escala $\tau(q) = -\log_2(E(R^q))$.

3.7 Modelo MWM (*Multifractal Wavelet Model*)

O modelo multifractal MWM (*Multifractal Wavelet Model*) proposto por Riedi et al. (1999) é baseado na *wavelet* (função utilizada para decompor e descrever processos) de Haar para caracterização de tráfego de redes cuja restrição de estrutura é construída por multiplicadores $W_{j,k}$ de cascata no domínio, dados por (RIEDI et al., 1999):

$$W_{j,k} = A_{j,k} U_{j,k} \quad (3.17)$$

onde $A_{j,k}$ é a variável aleatória suportada no intervalo $[-1,1]$, e $U_{j,k}$ representa uma aproximação de $X(t)$ para resolução de 2^j , conforme ilustrado na Figura 3.4, uma cascata MWM no domínio *wavelet*.

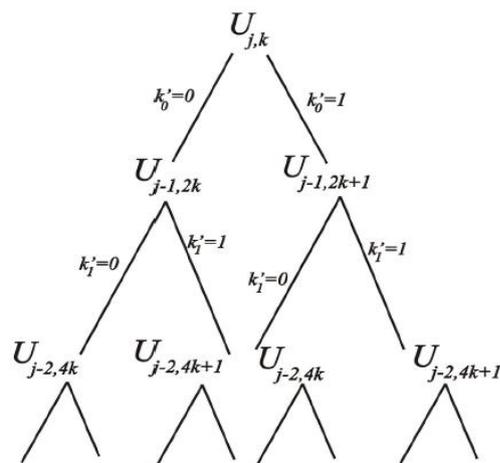


Figura 3.4 - Cascata formada pelos coeficientes de escala $U_{j,k}$ (CROUSE et al., 2000).

O MWM é uma cascata multiplicativa no domínio *wavelet*. A transformada *wavelet* discreta (DWT - *Discrete Wavelet Transform*) é usada neste modelo devido a sua capacidade de representação multi-escala de sinais.

Na obtenção de um processo segundo o modelo MWM é preciso aplicar a transformada *wavelet* discreta ao tráfego de rede, calcular os momentos de segunda ordem dos coeficientes *wavelet* em cada escala, a média e a variância dos coeficientes na escala de maior resolução e calcular p_j , variável usada para capturar o decaimento de energia dos coeficientes *wavelet* em escala (RIBEIRO et al., 2000).

O MWM aproxima com eficiência as propriedades do fluxo de tráfego original em relação à distribuição marginal (produz distribuição aproximadamente lognormal) e sua estrutura de correlação, tendo grande destaque na modelagem de tráfego (VIEIRA; LING, 2008; RIEDI et al., 1999).

3.8 Modelo AWMM (*Adaptive Wavelet Based Multifractal Model*)

O AWMM ou Modelo Adaptativo Multifractal Baseado em *Wavelet* proposto por Vieira e Lee (2009) é um modelo desenvolvido baseado em algumas propriedades da *wavelet* de Haar e em cascatas multiplicativas. Este modelo multifractal possui algumas vantagens sobre os modelos multifractais existentes em termos de poucos parâmetros de entrada e capacidade de atualização *online*.

O AWMM consiste em estimar o coeficiente de segunda ordem do momento da *wavelet* de Haar do produto par a par de amostras de uma cascata e amostras independentes e identicamente distribuídas (i.i.d.) de uma variável aleatória positiva e em seguida, obter os valores dos multiplicadores $A_{j,k}$ a fim de capturar a relação de energia *wavelet* $E(W_{j,k}^2)$. Ou seja, este modelo é capaz de capturar simultaneamente as funções $\tau(q)$ e $c(q)$ de processos multifractais e também o coeficiente de queda de energia *wavelet* (VIEIRA; LEE, 2009).

Para comparar as características autossimilares e as características multifractais estatística do modelo AWMM para aquelas do tráfego real, bem como às do modelo MWM, alguns testes foram realizados com dados estatísticos, tais como função de autocorrelação e espectro multifractal, conforme pode ser observado em Vieira e Lee (2006).

3.9 Modelo CGMD (*Cascade with Generalized Multiplier Distributions*)

O modelo CGMD (Cascata com Multiplicador com Distribuição Generalizada) introduzido por Vieira e Lee (2006) apresenta multiplicadores determinados através de suas densidades de probabilidade estimadas a partir dos fluxos reais de tráfego de rede usando o

método de *Kernel* e o método de Aceitação / Rejeição para obtenção de amostras segundo a PDF obtida (VIEIRA; LEE, 2006).

A função densidade de probabilidade estimada pode ser paramétrica ou não paramétrica, assumindo ou não que os dados são extraídos de uma distribuição conhecida, respectivamente. Em Vieira e Lee (2006) os autores seguiram a abordagem não-paramétrica para estimar os multiplicadores da cascata com base em dados observados.

O estimador de *Kernel* tem ampla aplicabilidade, especialmente no caso univariado. O estimador *Kernel* é provavelmente o estimador de densidade não paramétrico mais comumente utilizados e bastante estudado matematicamente depois do método baseado em histogramas.

O método de síntese CGMD consiste em um processo de cascata multiplicativa assumindo diferentes distribuições de multiplicadores em cada cascata. O procedimento envolve o processo de valor agregado obtido na escala mais grosseira da cascata, a densidade de probabilidade dos multiplicadores estimados pelo método de *Kernel* e os multiplicadores obtidos em cada fase, pelo método de Aceitação/Rejeição. Na verdade, utiliza-se uma mistura Gaussiana para modelar a densidade de probabilidade real dos multiplicadores (VIEIRA; LEE, 2006).

3.10 Resumo do Capítulo

Neste capítulo foram abordados os principais modelos de tráfego de redes existentes na literatura como o Poisson (HOCK; HEE, 2008), fBm (WIERSEMA, 2008), mBm (PELTIER; VÉHEL, 1995), e modelos baseados em cascatas multiplicativas (VIEIRA; LING, 2008) como o CGMD (VIEIRA; LEE, 2006) e modelos baseados em *wavelets* (RIEDI et al., 1999), tais como o MWM (RIEDI et al., 1999) e AWMM (VIEIRA; LEE, 2009). Também verificou-se as peculiaridades dos processos monofractais e multifractais, além dos parâmetros de Hurst (OLIVEIRA; MENDES, 2006) e expoente de Hölder (GUÉVEL; VÉHEL, 2010), utilizados para a determinação do grau de autossimilaridade e regularidade local do tráfego de rede, respectivamente.

A modelagem de tráfego apresentada é utilizada para se observar o comportamento dos algoritmos de policiamento apresentados no próximo capítulo, em relação às diferentes características de séries de tráfego.

CAPÍTULO 4

POLICIAMENTO BASEADO EM MODELAGEM DE TRÁFEGO

Neste capítulo são apresentadas as séries de tráfego de rede utilizadas nas análises dos processos envelopes de tráfego e do desempenho dos algoritmos de policiamento. São abordados também alguns dos algoritmos de policiamento baseados em modelagem de tráfego mais conhecidos da literatura.

É apresentada também uma proposta de algoritmo de policiamento baseado em modelagem multifractal que utiliza o conceito de balde furado para a regulação (policiamento) de séries de tráfego, denominado de Mecanismo de Policiamento de Chegadas Multifractais (MAPM – *Multifractal Arrival Policing Mechanism*).

Os algoritmos de policiamento de rede são alguns dos mecanismos responsáveis pela garantia da qualidade de serviço (QoS) na rede, pois permitem a passagem apenas do tráfego de pacotes conforme o acordo de prestação de serviço (SLA). Utilizando séries reais de tráfego de rede, apresenta-se através de simulações computacionais os resultados da utilização dos seguintes algoritmos de policiamento: Balde Furado, Balde Furado Fractal e Balde Furado Multifractal Gaussiano. Confrontam-se os processos envelopes dos algoritmos de policiamento com o processo envelope do algoritmo de policiamento proposto MAPM .

O capítulo está organizado da seguinte maneira: na seção 4.1 apresenta-se sobre as séries de tráfego utilizadas neste trabalho, na seção 4.2 apresenta-se a definição de processo envelope (PE), na seção 4.3 se apresenta o Processo de Chegada com Limitante Multifractal, na seção 4.4 discursa-se sobre algoritmos de policiamento de tráfego de rede baseados em modelagem, como o Balde Furado Fractal e o Balde Furado Multifractal Gaussiano. Na seção 4.5, apresenta-se a proposta de algoritmo de policiamento chamada de Mecanismo de Policiamento de Chegadas Multifractais (MAPM) e em seguida compara-se os processos envelopes dos algoritmos de policiamento apresentados com o algoritmo proposto (MAPM)

na seção 4.6. Por fim, a seção 4.8 apresenta o resumo deste capítulo.

4.1 Séries de Tráfego Utilizadas

As séries (*traces*) de tráfego utilizadas nas análises desta dissertação estão disponíveis no site *Internet Traffic Archive*⁷, no site da Universidade do Sul da Califórnia⁸ e no site *Universita' degli Studi di Napoli "Federico II"*⁹ (Itália). As séries de tráfego de rede utilizadas foram: o *lbl-pkt-5*, *dec-pkt-2* e *dec-pkt-3* para simulações com pacotes de rede com fio (ITA, 2008) e o *USC_06spring_trace*, *USC_2005summer* (USC, 2006) e *Clean_Unina* (UNINA, 2004), que são séries de tráfego coletadas de rede sem fio. As principais características estatísticas dos *traces* utilizados são apresentadas na Tabela 4.1.

Série de tráfego	Valor mínimo (X_{\min}) (bytes)	Valor médio (\bar{X}) (bytes)	Valor máximo (X_{\max}) (bytes)	Variância (σ^2) (bytes)	Parâmetro de Hurst (H)
lbl-pkt-5	18	1,33x10 ⁴	1,47x10 ⁵	1,27x10 ⁸	0,718
dec-pkt-3	1,10 x10 ³	1,99x10 ⁴	7,06x10 ⁴	5,54x10 ⁷	0,766
dec-pkt-2	20	2,57x10 ³	6,19x10 ⁴	3,02x10 ⁷	0,581
USC_06spring	1	0,80x10 ³	6,52x10 ⁴	7,88x10 ⁶	0,546
USC_2005summer	1	8,44x10 ³	7,69x10 ⁶	1,00x10 ¹⁰	0,596
Clean_Unina	2,31x10 ³	7,85x10 ³	1,71x10 ⁴	3,32x10 ⁶	0,895
Poisson*	9,61x10 ³	9,99x10 ³	1,04x10 ⁴	1,02x10 ⁴	0,588
MWM*	2,72x10 ²	1,18x10 ⁴	1,38x10 ⁵	1,13x10 ⁸	0,796
mBm*	0	8,92x10 ²	4,86x10 ³	6,47x10 ⁵	0,986
fBm*	0	5,83x10 ²	8,04x10 ²	4,23x10 ⁴	0,800

Tabela 4.1 - Características básicas das séries de tráfego

O *trace* *lbl-pkt-5* [Figura 4.1 (a)] representa dados (*bytes*) recolhidos no *gateway* de Internet do Laboratório Lawrence Berkeley (LBL). O *trace* capturado tem duração de uma hora (PAXSON; FLOYD, 1995).

A Figura 4.1 (b) apresenta um gráfico da quantidade de *bytes* a cada 512 ms do *trace* *dec-pkt-3* coletados no principal ponto de acesso à Internet da *Digital Equipment Corporation* (DEC). O ponto de acesso é operado pelo grupo de pesquisa Palo Alto da DEC e os dados foram coletados pelo Laboratório de pesquisa ocidental da DEC. Esses dados de tráfego completos contêm o valor de uma hora de todo o tráfego de longa distância entre a

⁷ Disponível em <http://ita.ee.lbl.gov/html/traces.html>

⁸ Disponível em http://nile.cise.ufl.edu/MobiLib/USC_trace/

⁹ Disponível em <http://www.grid.unina.it/Traffic/Traces/>

* Série de tráfego sintética

Digital Equipment Corporation e o resto do mundo (PAXSON; FLOYD, 1995).

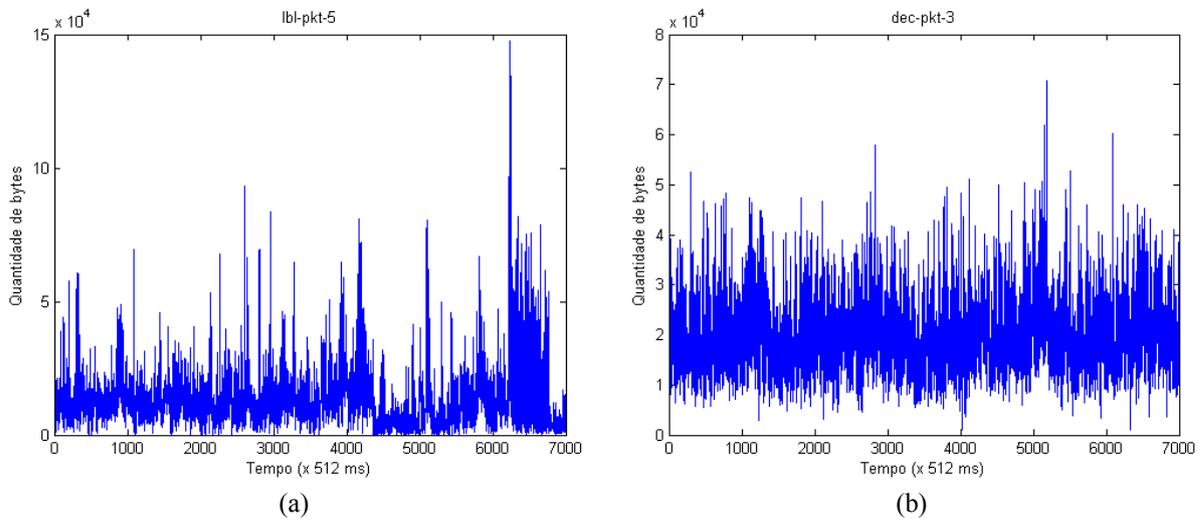


Figura 4.1- Valores das séries de tráfego com fio (a) lbl-pkt-5 e (b) dec-pkt-3

O *trace* USC_06spring [Figura 4.2 (a)] é um conjunto de dados relacionado a 25.481 usuários da rede no período de 25 de janeiro a 28 abril de 2006, no qual utilizou-se o arquivo 0_4_23_4d_47_4 (que se refere a um usuário) e 7.000 (sete mil) amostras com tempo de amostragem de 512 ms. Durante esse período, havia 137 concentradores locais (pontos de acesso) para coleta de dados. Cada local corresponde aproximadamente a um prédio no campus (da Universidade do Sul da Califórnia - USC) codificado no formato de IP_port (a porta do *switch* real que controla o tráfego de (origem) / para (destino) neste local) (HSU, 2006).

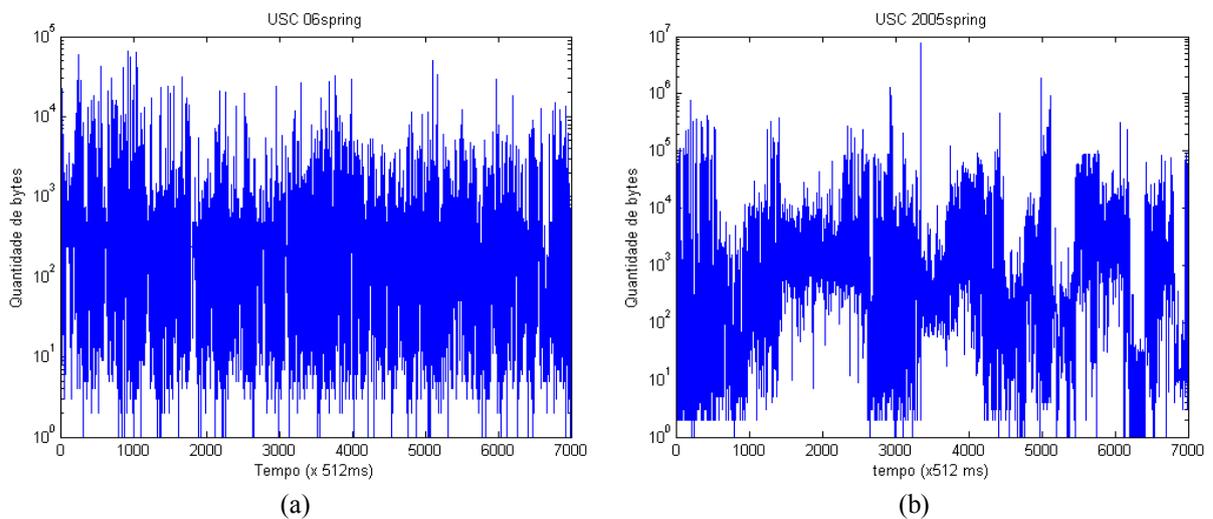


Figura 4.2 - Valores das séries de tráfego sem fio (a) USC_06spring e (b) USC_2005summer

No *trace* USC_2005summer [Figura 4.2 (b)] os dados foram coletados entre 19 de abril e 8 de agosto de 2005, e trata-se de pacotes que trafegavam pela rede sem fio do campus da USC e o roteador de saída para a Internet, onde a identificação do usuário trata de cada porta do *switch* referente a um prédio do campus.

O *trace* Clean_Unina representa três séries de tráfego diferentes, e utilizou-se as duas primeiras. Os *traces* foram coletados em 2004 na rede UNINA, com taxa de amostragem de 2 segundos com a duração de 2 horas cada.

A Figura 4.3 mostra a Função Densidade de Probabilidade (PDF) dos valores de intensidade de tráfego dos *traces* Internet (a) lbl-pkt-5, (b) dec-pkt-3 e a Figura 4.4 para os *traces* sem fio (a) USC_06spring e (b) USC_2005summer. Estas figuras traduzem a distribuição de probabilidade $f(x)$ de uma variável contínua, onde $F_X(x)$ é a função de distribuição acumulada para x em um intervalo $[a,b]$ e definida pela equação (PAPOULIS, 1991):

$$F_X(x) = P[a \leq X \leq b] = \int_a^b f(x)dx \quad (4.1)$$

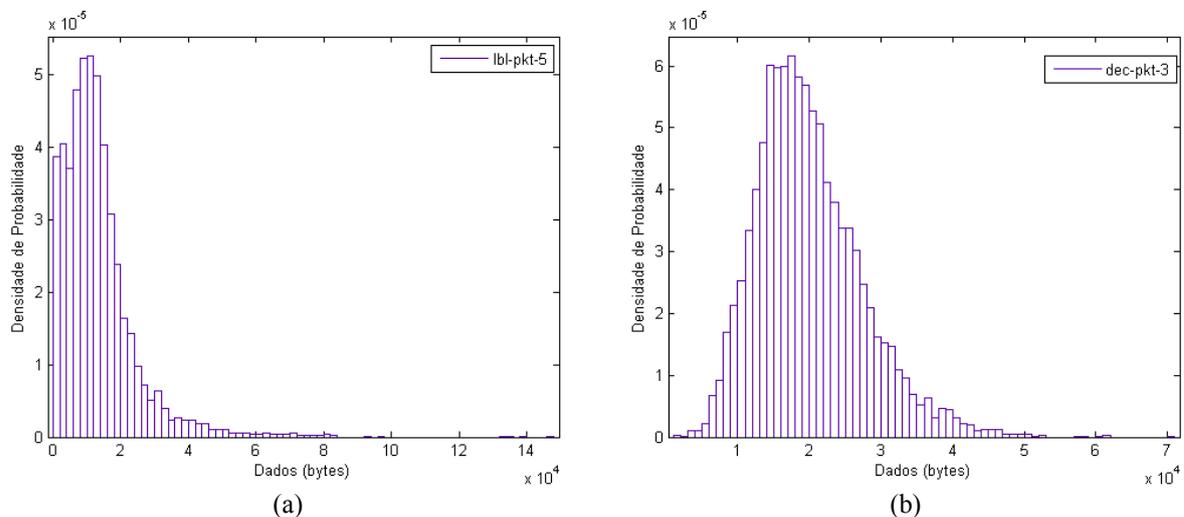


Figura 4.3 - Função densidade de probabilidade dos tráfegos com fio (a) lbl-pkt-5, (b) dec-pkt-3

Para as funções densidade de probabilidade, observa-se que a densidade de probabilidade da série de tráfego lbl-pkt-5 [Figura 4.3 (a)] tende a uma densidade de probabilidade lognormal. Já a densidade de probabilidade para a série dec-pkt-3 [Figura 4.3 (b)] está mais próxima da densidade de probabilidade Gaussiana. Pode-se notar que as PDFs das séries USC_06spring e USC_2005summer [Figura 4.4 (a) e (b), respectivamente] não tendem a uma função Gaussiana.

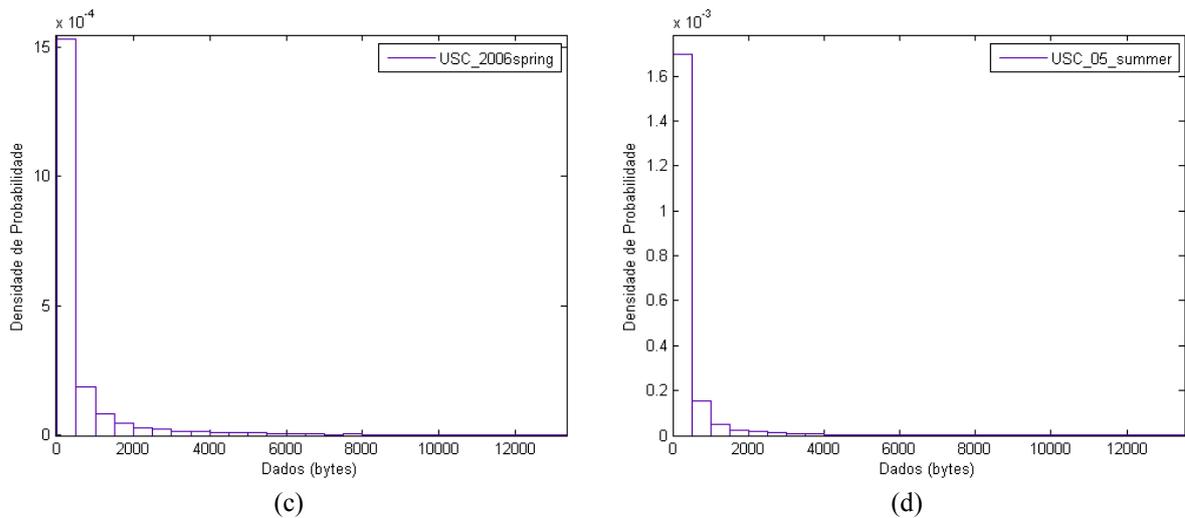


Figura 4.4 - Função densidade de probabilidade dos tráfegos sem fio (a) USC_06spring e (b) USC_2005summer

4.2 Processo Envelope (PE)

O processo envelope (PE) para o tráfego de chegada de pacotes é um limitante superior para o processo real de tráfego de pacotes acumulados. Para um processo envelope determinístico, a função limitante $\hat{A}(t)$ é definida pela equação (MELO; FONSECA, 2004; LE BOUDEC; THIRAN, 2004):

$$\hat{A}(t) = \sup_{s \geq 0} A[s, s+t] \quad (4.2)$$

Esta equação corresponde ao valor máximo de um fluxo $A(t)$ no intervalo de tempo $[s, s+t]$. O processo envelope para as séries de tráfego analisadas é dada por:

$$A(n) = \sum_{i=1}^n X(i) \quad (4.3)$$

A Figura 4.5 apresenta os processos envelopes para as séries de tráfego de rede com fio lbl-pkt-5 e dec-pkt-3. Pode-se afirmar que através dos processos envelopes das séries de tráfego, que quanto mais suave a curva, mais homogêneo é o número de pacotes por intervalo de tempo (rajadas de pacotes com menor intensidade e constantes).

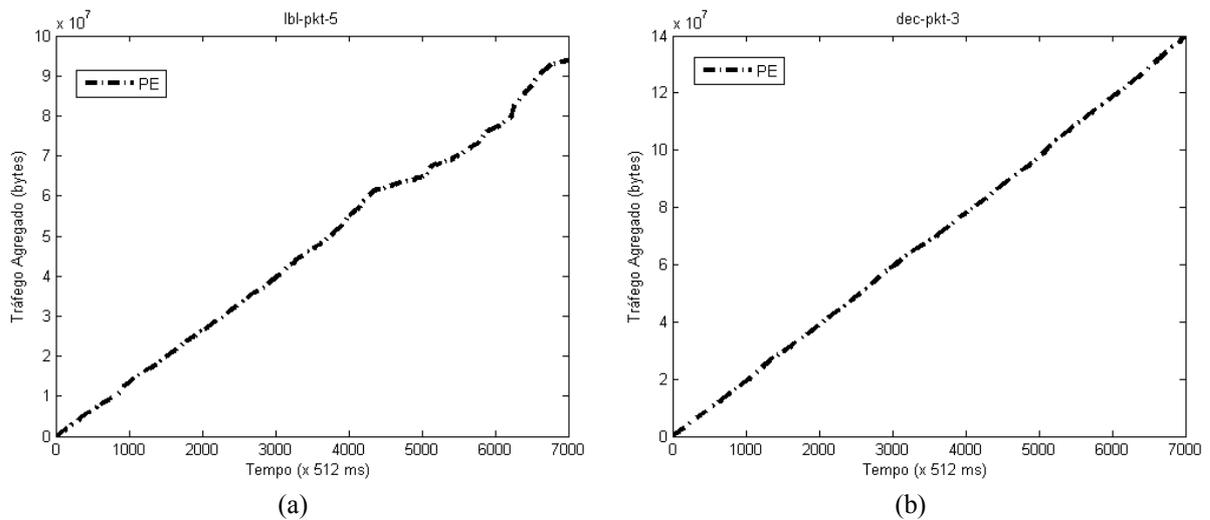


Figura 4.5 - Processo Envelope para séries de tráfego com fio (a) lbl-pkt-5 e (b) dec-pkt-3

Na Figura 4.6 apresenta-se os processos envelopes para as séries de tráfego de rede sem fio (a) USC_06spring e (b) USC_2005summer. Observa-se nestas figuras que as curvas apresentadas são menos lineares, ou seja, estas séries apresentam variações de pacotes por rajadas mais acentuadas se comparadas às séries com fio lbl-pkt-5 e dec-pkt-3.

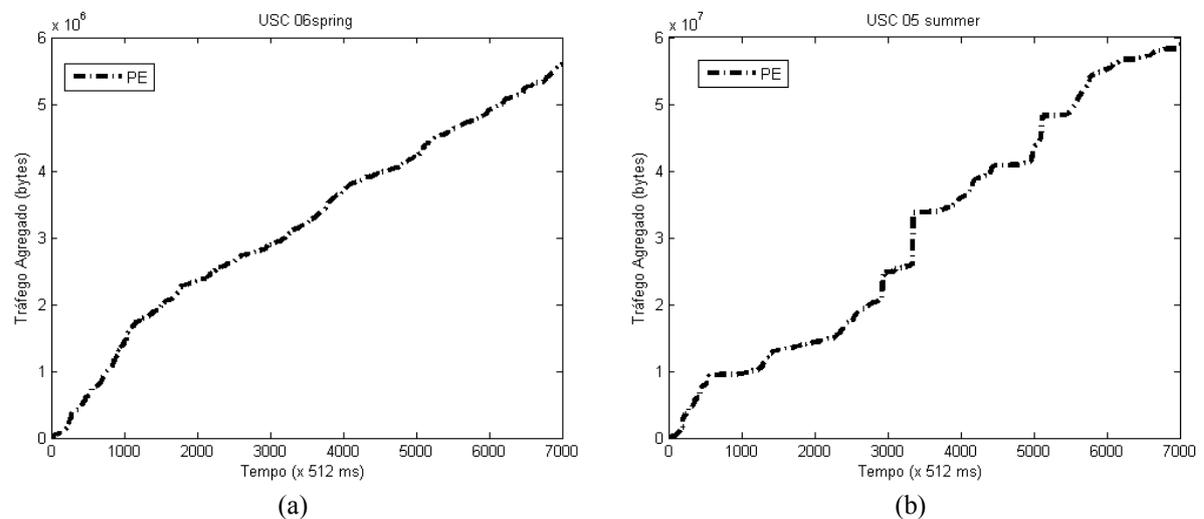


Figura 4.6 - Processo Envelope para séries de tráfego sem fio (a) USC_06spring e (b) USC_2005summer

A Figura 4.7 mostra uma série de tráfego sintética gerada pelo *software* Matlab (MATHWORKS, 2011) segundo o modelo de Poisson (com média igual ao tráfego real) e o seu processo envelope. Verifica-se que para uma série Poissoniana, o processo envelope representa uma reta, pois os pacotes apresentam valores próximos do valor médio do fluxo.

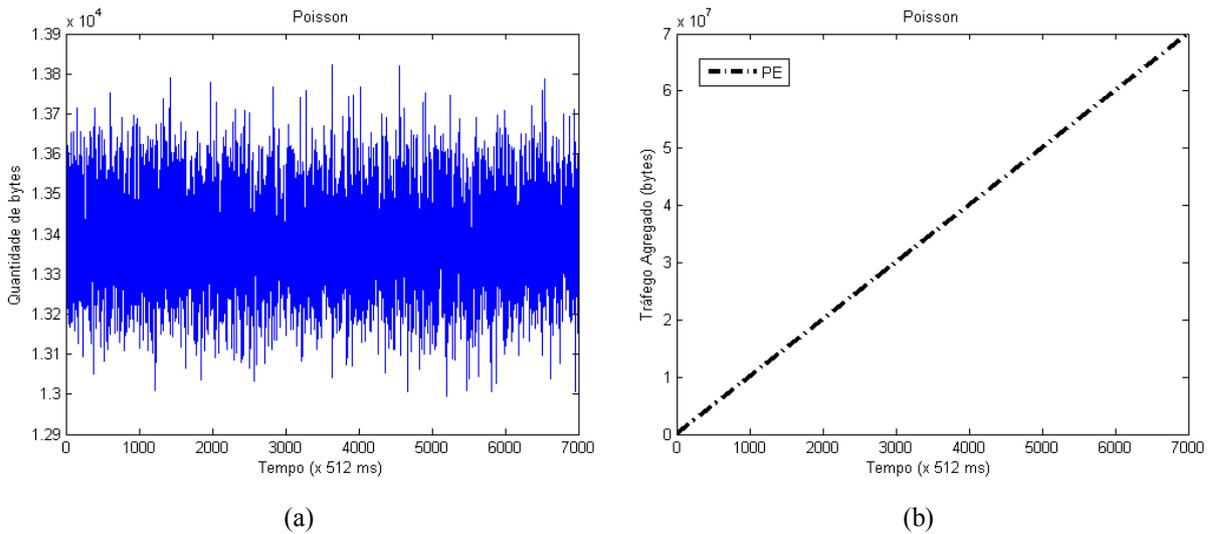


Figura 4.7 - Série de tráfego sintética Poisson: (a) série de tráfego e (b) processo envelope

Para a Figura 4.8, observa-se: (a) a série sintética gerada segundo o modelo MWM também pelo *software* Matlab (com média igual ao tráfego real) e (b) o seu processo envelope. Pode-se observar que para os modelos que levam em consideração as características multifractais do tráfego de rede, a curva apresentada não representa uma reta perfeita devido às imperfeições decorrentes das diferentes quantidades de pacotes em rajadas que ocorre no fluxo do tráfego analisado.

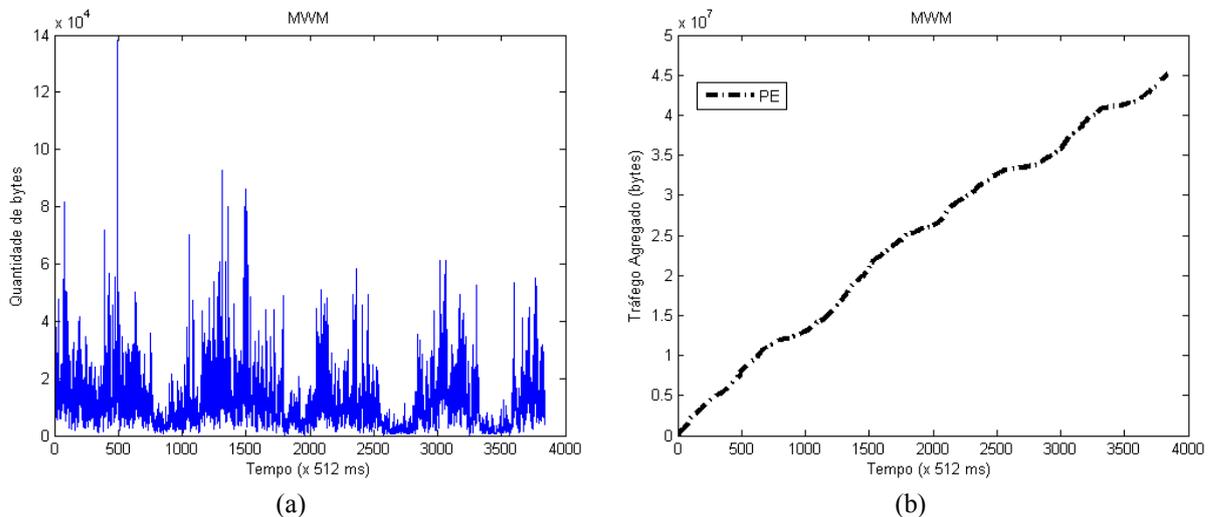


Figura 4.8 - Série de tráfego sintética MWM: (a) série de tráfego e (b) processo envelope

4.3 Processo de Chegada com Limitante Multifractal (*Multifractal Bounded Arrival Process – MFBAP*)

O Processo de Chegada com Limitante Multifractal (MFBAP) é uma alternativa

determinística de se obter o processo envelope que limita o volume do tráfego em um dado intervalo de tempo. Caso o processo envelope seja relacionado ao volume de tráfego até um dado instante, este é chamado processo envelope acumulativo e incremental, caso se limite ao volume de *bytes* em um intervalo de tempo qualquer (PEREIRA, 2006).

O processo envelope MFBAP é dado pela equação (PEREIRA; FONSECA; ARANTES, 2006):

$$\hat{L}_{MFBAP}(t) = \bar{a}t + \kappa\sigma\hat{C}(t) \quad (4.4)$$

onde

$$\hat{C}(t) = t^{H(t)} \quad (4.5)$$

$$H(t) = H_0 + \sigma_H \exp\left\{-\frac{[\ln(t) - \bar{a}_H]}{2\sigma_H^2}\right\} \quad (4.6)$$

em que $H(t)$ é o expoente de Hölder, t o instante de tempo, \bar{a} e σ são respectivamente, a média e o desvio padrão do tráfego, \bar{a}_H e σ_H são respectivamente, a média e o desvio padrão do expoente de Hölder, k é a constante relacionada à probabilidade de violação do processo envelope dada pela equação (PEREIRA, 2006):

$$k = \sqrt{-2 \ln \varepsilon} \quad (4.7)$$

Os valores do processo envelope (PE) do MFBAP se encontram em geral abaixo dos valores do PE do tráfego real (melhor visualizado no tráfego de redes sem fio), como mostra a Figura 4.9 para as séries *lbl-pkt-5* e *USC_06spring*. Neste caso, um maior número de *bytes* será descartado em um sistema com o algoritmo de policiamento em relação a um sistema sem policiamento. Os pacotes acima da curva do PE do algoritmo MFBAP serão descartados ou marcados como pacotes de baixa prioridade, onde poderão ser descartados pelo sistema de transmissão logo em seguida devido à prioridade baixa.

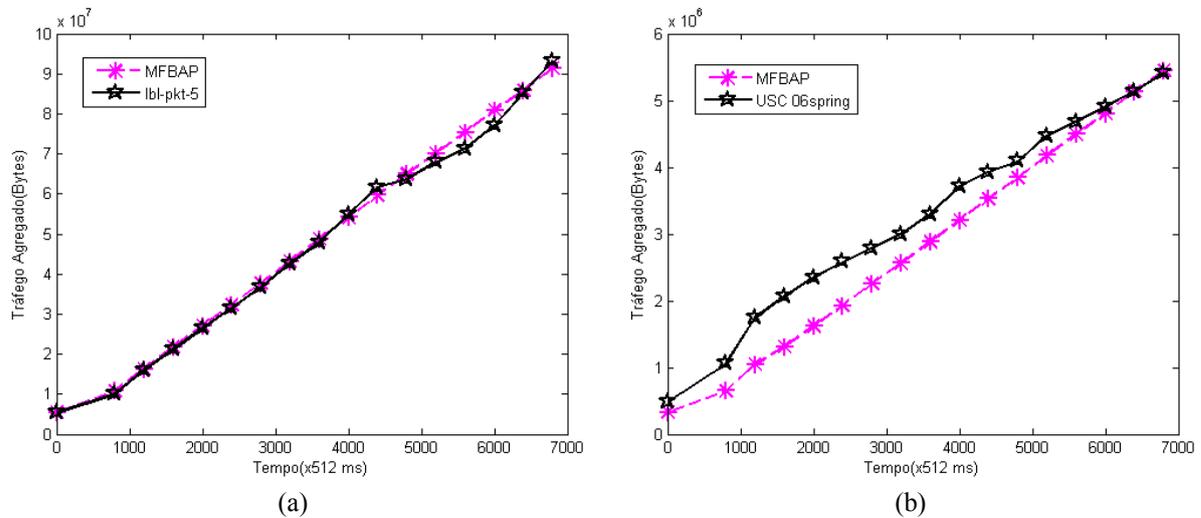


Figura 4.9 - Processo envelope MFBAP para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring

Os processos envelopes das séries de tráfego sintéticas apresentam curvas semelhantes às das séries reais que representam. Na Figura 4.10 e Figura 4.11 apresentam-se os processos envelopes das séries de tráfego USC_06spring e lbl-pkt-5, respectivamente. Verificou-se a semelhança entre os processos envelopes das séries de tráfego reais e das séries sintéticas que apresentam características multifractais como os modelos mBm e MWM, além de séries com características monofractais como a fBm e clássica como a Poissoniana.

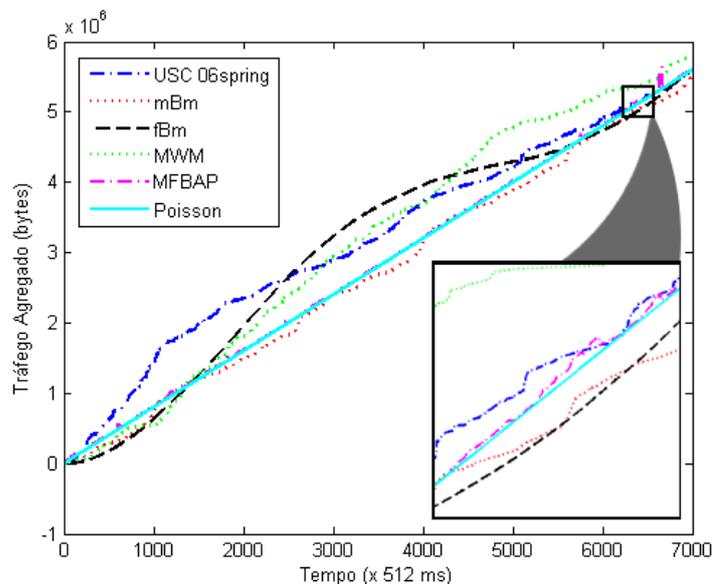


Figura 4.10 - Comparativo dos processos envelopes de séries de tráfego USC_06spring e sintéticas

Para as séries de tráfego sintéticas da Figura 4.10, a média do processo foi de 800 bytes e gerou-se 7000 amostras (devido à quantidade de amostras das outras séries de tráfego, limitou-se neste valor). Para a série mBm sintética, utilizou-se os mesmos valores de média e

expoente de Hölder da série de tráfego real. Observa-se também que à medida que o tráfego aumenta, o processo envelope MFBAP tende a acompanhar a série de tráfego real (USC_06spring) em vários pontos do processo envelope, além de amortecer os picos de rajadas.

Para uma série com tendência a ser monofractal na escala de 512 ms (Figura 4.11), os processos envelopes Poisson e fBm são capazes de representar o processo envelope do tráfego real (lbl-pkt-5), e observa-se que o PE do algoritmo MFBAP também se assemelha ao real. Com isso, pode-se afirmar que o PE do algoritmo MFBAP representa com eficiência tanto as séries de tráfego com características monofractais quanto multifractais.

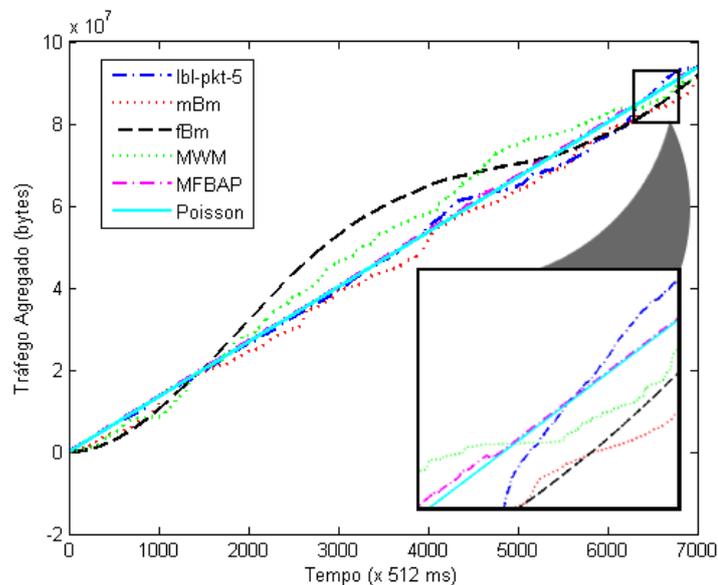


Figura 4.11 - Comparativo dos processos envelopes de séries de tráfego lbl-pkt-5 e sintéticas

4.4 Policiamento de Redes Baseado em Modelagem de Tráfego

O policiamento de tráfego de rede é a parte do sistema de transmissão responsável por garantir que as aplicações que não estejam em conformidade com o contrato de serviço (SLA) não ultrapassem os limites previamente estabelecidos pelas operadoras dos serviços contratados.

4.4.1 Balde Furado (*Leaky Bucket* - LB)

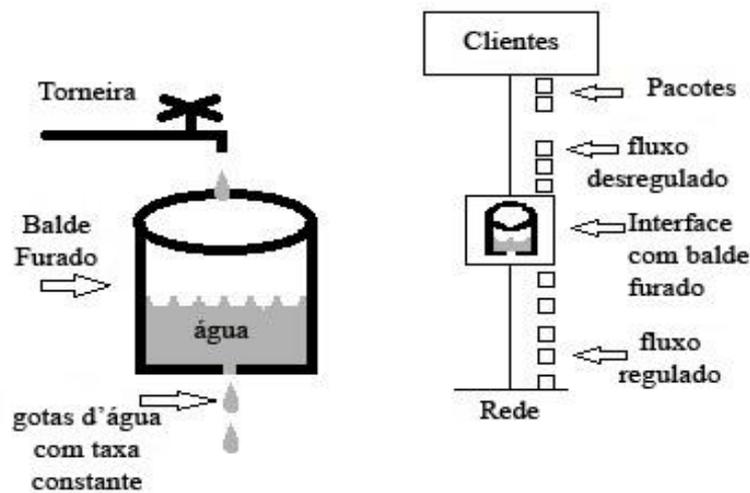


Figura 4.12 - Balde Furado (TANENBAUM, 2003)

O algoritmo de Balde Furado (LB) é comparado a um balde comum com um pequeno furo no fundo (ver Figura 4.12). Independentemente da velocidade com que a água entra no balde, o fluxo de saída apresenta taxa constante quando estiver com água ou zero se o balde estiver vazio. Além disso, quando o balde estiver cheio, a água que entrar ultrapassará o volume máximo (tamanho do balde) e escorrerá pelas bordas sendo perdida.

A mesma ideia pode ser aplicada a pacotes. Conceitualmente, cada estação (*host*) está conectada à rede por uma interface que contém um balde furado, ou seja, uma fila interna finita. Se um pacote chegar à fila quando ela estiver cheia, o pacote será descartado. Essa disposição pode ser interna à interface de *hardware* ou simulada pelo sistema operacional da estação. Este regulador de tráfego é simplesmente um sistema de enfileiramento de um único servidor com um tempo de serviço constante (BREGNI; GIACOMAZZI; SADDEMI, 2010).

A estação pode inserir um pacote na rede a cada pulso de *clock*. Novamente, isso pode ser forçado pela placa de interface de rede ou pelo sistema operacional. Esse mecanismo transforma um fluxo de pacotes irregular proveniente dos processos do usuário no *host* em um fluxo de pacotes regular para a rede, suavizando as rajadas e reduzindo bastante as possibilidades de congestionamento (NICOLA; HAGESTEIJN; KIM, 1994).

Quando todos os pacotes têm o mesmo tamanho (por exemplo, células ATM), esse algoritmo pode ser usado sem problemas, porém, quando o tráfego utilizado apresenta pacotes de tamanho variável, é melhor permitir um número fixo de *bytes* por pulso (com valor próximo ao da média), em vez de apenas um pacote (TANENBAUM, 2003).

Em uma primeira e intuitiva análise, o esquema do algoritmo de balde furado

regula e controla o tráfego de entrada. O algoritmo de Balde Furado (LB) transfere diretamente para sua saída todo o tráfego a uma taxa média ρ e armazenando dados a uma capacidade máxima S do balde. Porém, esta situação nem sempre ocorre e um tráfego de entrada bem comportado pode ter um acréscimo no retardo (*delay*) ou perdas de pacotes causados pelo algoritmo quando o tráfego apresentar pacotes em rajadas. Em geral, estipula-se o parâmetro ρ como sendo maior que a taxa média do tráfego real de chegada para garantir uma melhor execução do algoritmo.

O processo envelope do Balde Furado é dado pela equação (PEREIRA; FONSECA; ARANTES, 2006):

$$\hat{L}_{LB}(t) = \bar{a}t + S \quad (4.8)$$

onde t é o instante de tempo, \bar{a} é a média do tráfego de entrada e S o tamanho do balde (*buffer*).

Na Figura 4.13, verifica-se que o PE do Balde Furado está mais próximo do tráfego sem policiamento melhor comportado, ou seja, para a série lbl-pkt-5, que do tráfego com maiores rajadas. Por isso o LB não apresenta um resultado adequado para tráfegos em rajadas, por não prever altas variações de pacotes nos fluxos de tráfego, comportamento também observado por Bregni, Giacomazzi e Saddemi (2010).

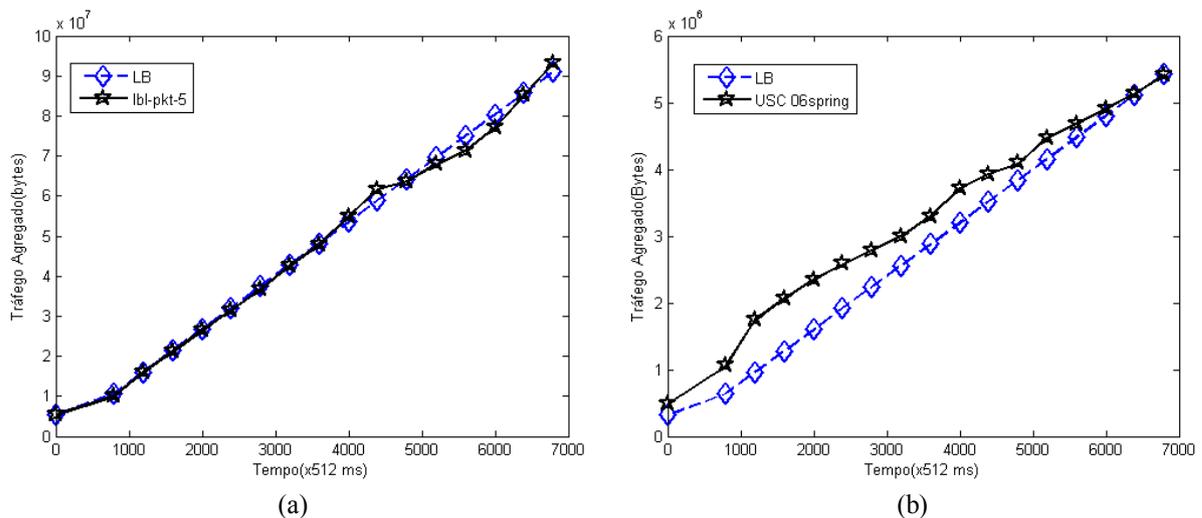


Figura 4.13 - Processo envelope para o algoritmo Balde Furado para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring

O algoritmo de Balde Furado também pode ser visto como um teste sequencial e descrito pelo seguinte conjunto de equações:

$$E_n = \max\{0, E_{n-1} + X_n - \bar{a}\Delta\} \quad (4.9)$$

$$K_n = \begin{cases} S, & E_n = 0 \\ K_{n-1} & \end{cases} \quad (4.10)$$

$$J_n = \begin{cases} 0, & E_n \leq K_n \\ X_n - \bar{a}\Delta & \end{cases} \quad (4.11)$$

A sequência J_n representa o número de pacotes marcados com prioridade baixa ou que serão descartados. Nota-se que E_n é uma sequência de teste, K_n o limiar de decisão para E_n e J_n é o controle que o algoritmo exerce na sequência X_n . S é uma constante que representa o tamanho do balde, Δ o intervalo de tempo e \bar{a} a média do tráfego de entrada X_n . A Figura 4.14 mostra os valores de J_n para as séries de tráfego lbl-pkt-5 e USC_06spring, juntamente como o valor médio de J_n que para o tráfego lbl-pkt-5 é igual a 3.783 bytes e 497 bytes para a série de tráfego USC_06spring.

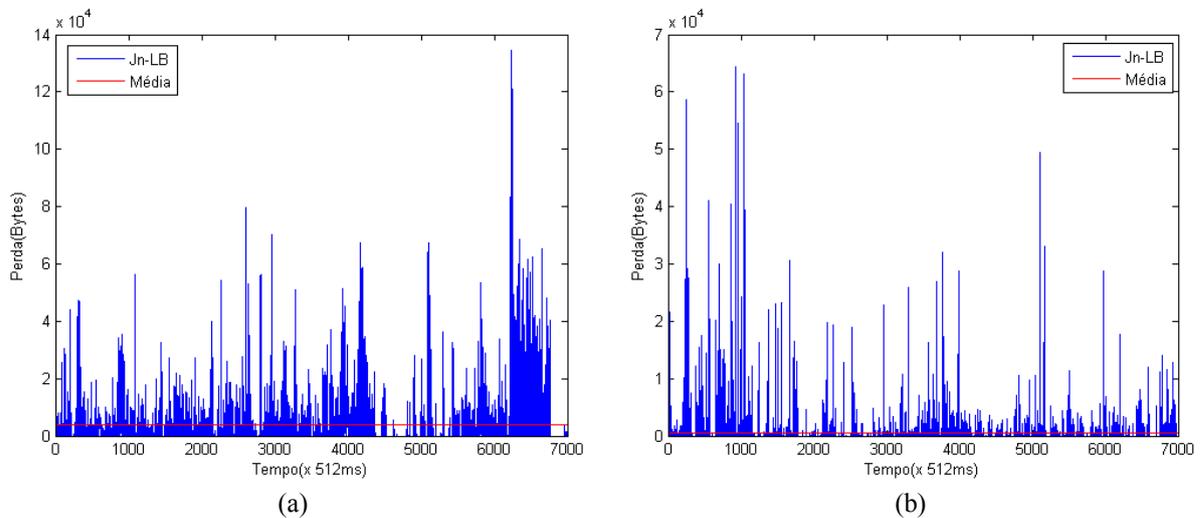


Figura 4.14 - Pacotes descartados ou marcados como baixa prioridade para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento LB

Considerou-se inicialmente as perdas P_b em um enlace simples com *buffer* de tamanho igual à média de entrada de tráfego e taxa de transmissão igual a média do tráfego de entrada. Outro fator analisado foi a taxa de perda (P_b) que representa a taxa de bytes descartados para cada série de tráfego. O valor da taxa de perda (P_b) representa o quociente da perda total do sistema pela quantidade total de bytes da série de tráfego, conforme equação abaixo:

$$P_b = \frac{\sum_{i=1}^n P(i)}{\sum_{i=1}^n X(i)} \quad (4.12)$$

onde $P(i)$ é a perda de *bytes* no sistema de transmissão e $X(i)$ o tráfego de entrada.

Os principais resultados são apresentados na Tabela 4.2. Tem-se um comparativo da perda de pacotes para as séries de tráfego de entrada sem policiamento e policiadas pelo algoritmo Balde Furado. Percebe-se que como o algoritmo não leva em conta as características dos pacotes em rajadas, a perda total de pacotes policiados com o algoritmo LB para as séries de rede com fio foi de zero *bytes*, pois o algoritmo conseguiu regular todo o fluxo de entrada.

Série (<i>trace</i>) de tráfego	Perda total sem policiamento (<i>bytes</i>)	Total de J_n com algoritmo LB (<i>bytes</i>)	Perda total P_b do tráfego regulado (<i>bytes</i>)
lbl-pkt-5	$2,09 \times 10^7$	$2,66 \times 10^7$	0
dec-pkt-3	$1,19 \times 10^7$	$2,08 \times 10^7$	0
USC_06spring	$2,80 \times 10^6$	$3,48 \times 10^6$	$7,84 \times 10^5$
Clean_Unina	$3,86 \times 10^6$	$5,50 \times 10^7$	$5,59 \times 10^5$

Tabela 4.2 - Comparativo entre as séries de tráfego sem policiamento e com o algoritmo de policiamento LB

Para as séries de rede sem fio (USC_06spring e Clean_Unina), a perda sem algoritmo de policiamento foi maior que para uma série policiada pelo LB. Verificou-se que a marcação total de *bytes* (J_n) não representa a quantidade de *bytes* descartados (P_b) em sua totalidade, conforme Tabela 4.2.

A relação da taxa de perda (P_b) pelo tamanho do *buffer* também foi observada para as séries de tráfego lbl-pkt-5 e USC_06spring. A Figura 4.15 (a) apresenta a perda para a série lbl-pkt-5, onde para o tráfego já policiado é igual a zero *bytes*. Na Figura 4.15 (b) apresenta-se a taxa de perda (P_b) da série USC_06spring, que apesar de haver uma taxa de perda para o tráfego policiado pelo algoritmo LB, esse valor é menor que para a mesma série sem policiamento.

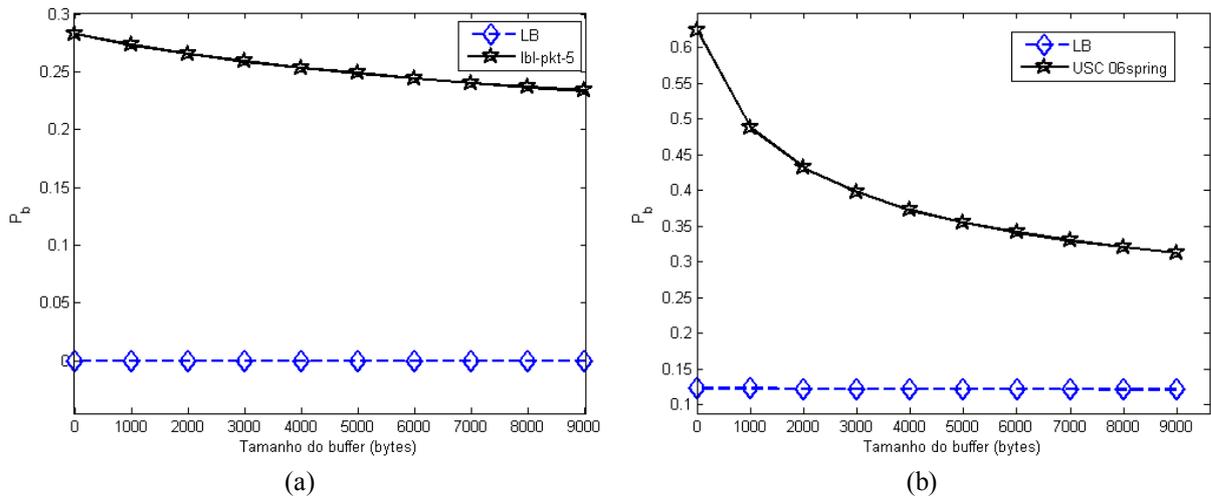


Figura 4.15 - P_b versus Tamanho do *buffer* para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento LB

4.4.2 Balde Furado Fractal (*Fractal Leaky Bucket - FLB*)

O Balde Furado Fractal (FLB) é um mecanismo de policiamento introduzido por Melo e Fonseca (2004). O FLB é baseado no modelo fBm (*fractional Brownian motion*) de processo de tráfego de pacotes e foi demonstrado que o fBm descreve com precisão fluxos de tráfego dada sua média (\bar{a}), desvio padrão (σ) e parâmetro de Hurst (H) (TAKADA, 2007).

A quantidade máxima de pacotes policiados, ou seja, o seu processo envelope do algoritmo FLB apresentado é dado pela equação (TAKADA, 2007):

$$\hat{L}_{FLB}(t) = \bar{a}t + \kappa\sigma t^H + S \quad (4.13)$$

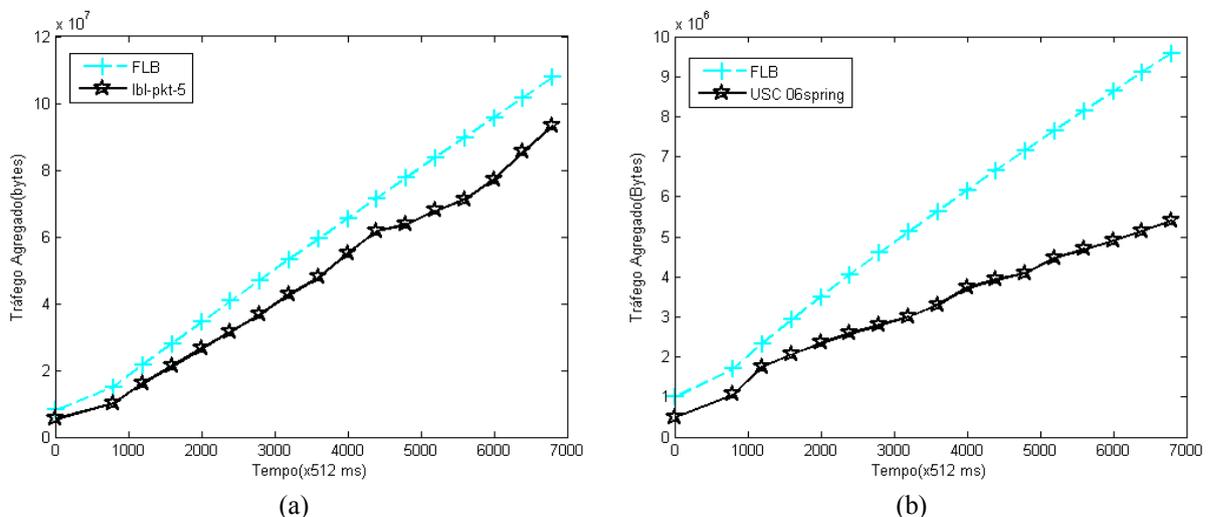


Figura 4.16 - Processo envelope Balde Furado Fractal para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring

Observa-se que o processo envelope FLB (Figura 4.16) tem sua envoltória acima da envoltória do tráfego sem policiamento. Isso faz com que o tráfego de redes seja pouco policiado, e esse comportamento também foi observado por Melo e Fonseca (2004).

O algoritmo FLB pode ser descrito como um teste sequencial da mesma forma que o algoritmo LB, entretanto têm-se as seguintes equações (TAKADA, 2007):

$$E_n = \max\{0, E_{n-1} + X_n - \bar{a}\Delta\} \quad (4.14)$$

$$K_n = \begin{cases} S, & E_n = 0 \\ k\sigma\Delta^H [n^H - (n-1)^H] + K_{n-1}, & E_n > 0 \end{cases} \quad (4.15)$$

$$J_n = \begin{cases} 0, & E_n \leq K_n \\ X_n - \bar{a}\Delta - k\sigma\Delta^H [n^H - (n-1)^H], & E_n > K_n \end{cases} \quad (4.16)$$

A Figura 4.17 mostra a sequência J_n , ou seja, o número de pacotes marcados com prioridade baixa ou que serão descartados para as séries (a) lbl-pkt-5 e (b) USC_06spring. Nota-se que E_n é uma sequência de teste, K_n o limiar de decisão para E_n e J_n é o controle que o algoritmo exerce na sequência X_n . S é uma constante análoga ao tamanho do balde no algoritmo LB, Δ o intervalo de tempo, \bar{a} e σ representam, respectivamente, a média e o desvio padrão do tráfego de entrada X_n , H representa o parâmetro de Hurst e k a constante relacionada à probabilidade de violação do processo envelope ε (no valor de 6×10^{-6}) dada pela equação (4.7). Os valores médios de J_n na Figura 4.17 foram iguais a 100 bytes e 2 bytes para as séries de tráfego lbl-pkt-5 e USC_06spring, respectivamente.

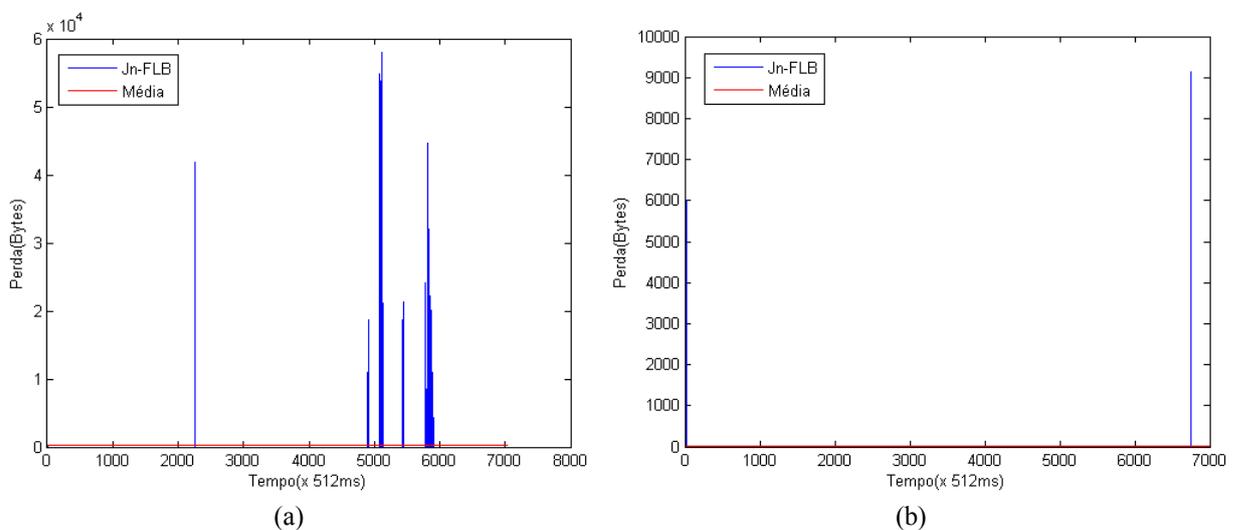


Figura 4.17 - Pacotes descartados ou marcados como baixa prioridade para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento FLB

A Tabela 4.3 apresenta um comparativo da quantidade de pacotes marcados como mal comportados ou descartados (J_n) para os tráfegos de entrada sem policiamento e policiado pelo algoritmo Balde Furado Fractal (FLB). Como o algoritmo superestima o processo envelope da série de tráfego, verifica-se que a perda média de pacotes P_b dada pela equação (4.12) com o algoritmo FLB é menor que sem algoritmo de policiamento para a série Clean_Unina (novamente considera-se um sistema simples de transmissão com *buffer* e capacidade de transmissão com valores iguais a média dos pacotes de entrada), pois são punidos somente os fluxos com grande quantidade de pacotes em intervalo de tempo muito pequeno.

Série (<i>trace</i>) de tráfego	Perda total sem policiamento (<i>bytes</i>)	Total de J_n com algoritmo FLB (<i>bytes</i>)	Perda total P_b do tráfego regulado (<i>bytes</i>)
lbl-pkt-5	$2,09 \times 10^7$	$7,09 \times 10^7$	$3,42 \times 10^7$
dec-pkt-3	$1,19 \times 10^7$	$3,28 \times 10^6$	$3,52 \times 10^7$
USC_06spring	$2,80 \times 10^6$	$1,58 \times 10^6$	$5,09 \times 10^6$
Clean_Unina	$3,86 \times 10^6$	$5,61 \times 10^7$	$3,62 \times 10^7$

Tabela 4.3 - Comparativo entre as séries de tráfego sem policiamento e com o algoritmo de policiamento FLB

De acordo com os valores de J_n apresentados na Figura 4.16, o FLB descarta ou marca como mal comportados mais *bytes* na série de tráfego lbl-pkt-5 que na USC_06spring devido a sua envoltória (curva do processo envelope) estar mais próxima da curva do processo envelope da série USC_06spring. Observa-se também que para as séries de tráfego lbl-pkt-5, dec-pkt-3 e USC_06spring apresentadas na Tabela 4.3, o tráfego policiado pelo algoritmo FLB apresentou maior taxa de perda (P_b) que sem o policiamento, além do J_n também apresentar valor menor que o valor total da perda (P_b) para as séries dec-pkt-3 e USC_06spring.

Para verificação da eficiência do algoritmo FLB, comparou-se a taxa de perda (P_b) das séries lbl-pkt-5 [Figura 4.18 (a)] e USC_06spring [Figura 4.18 (b)] *versus* o tamanho do *buffer* para cada valor. Observou-se que para o tráfego USC_06spring, quando o tamanho do *buffer* ultrapassa os 7.000 *bytes*, a taxa de perda sem policiamento torna-se menor que a taxa de perda P_b da série policiada pelo algoritmo FLB.

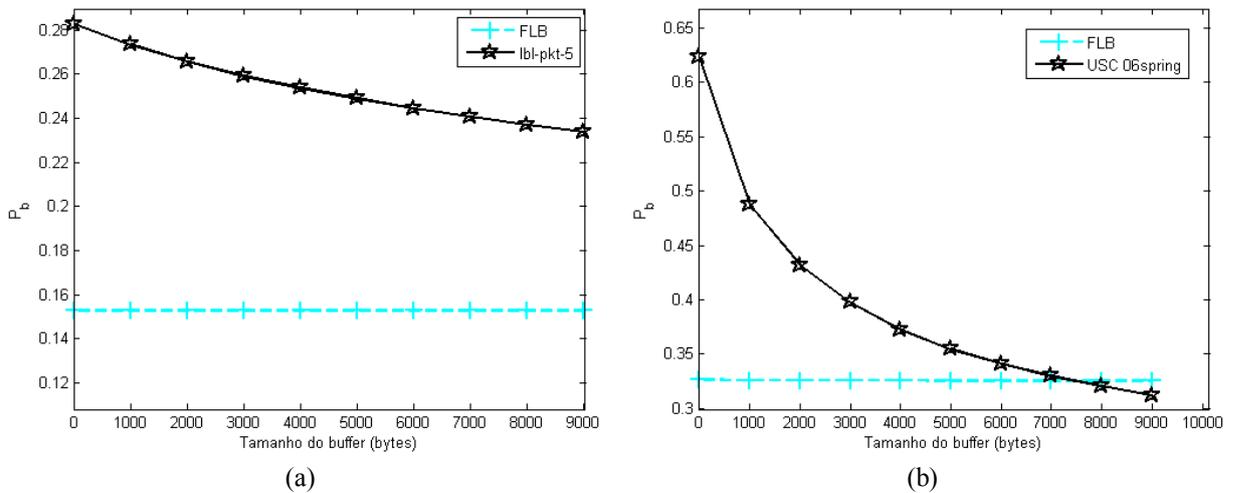


Figura 4.18 - P_b versus Tamanho do *buffer* para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento FLB

4.4.3 Balde Furado Multifractal Gaussiano (*Gaussian Multifractal Leaky Bucket – GMLB*)

O algoritmo chamado Balde Furado Multifractal Gaussiano (GMLB) é baseado no processo envelope mBm (*multifractal Brownian motion*). O mesmo é definido pelo seguinte conjunto de equações (TAKADA; ANZALONI, 2006):

$$E_n = \max\{0, E_{n-1} + X_n - \bar{a}\Delta\} \quad (4.17)$$

$$K_n = \begin{cases} S, & E_n = 0 \\ k\sigma \int_{\Delta(n-1)}^{\Delta n} H(t)x^{H(t)-1} dx + K_{n-1} \end{cases} \quad (4.18)$$

$$J_n = \begin{cases} 0, & E_n \leq K_n \\ X_n - \bar{a}\Delta - k\sigma \int_{\Delta(n-1)}^{\Delta n} H(t)x^{H(t)-1} dx \end{cases} \quad (4.19)$$

É fácil notar que K_n , E_n e J_n possuem as mesmas atribuições citadas no FLB, porém o parâmetro de Hurst (H) de cada série é substituído pelo expoente de Hölder $H(t)$ que apresenta valores característicos para cada amostra do tráfego e k é dado pela equação (4.7). A quantia máxima de pacotes de tráfego aceita pelo algoritmo GMLB é dada por (TAKADA, 2007):

$$\hat{L}_{GMLB}(t) = \bar{a}t + \kappa\sigma \int_0^t H(x)x^{H(x)-1} dx + S \quad (4.20)$$

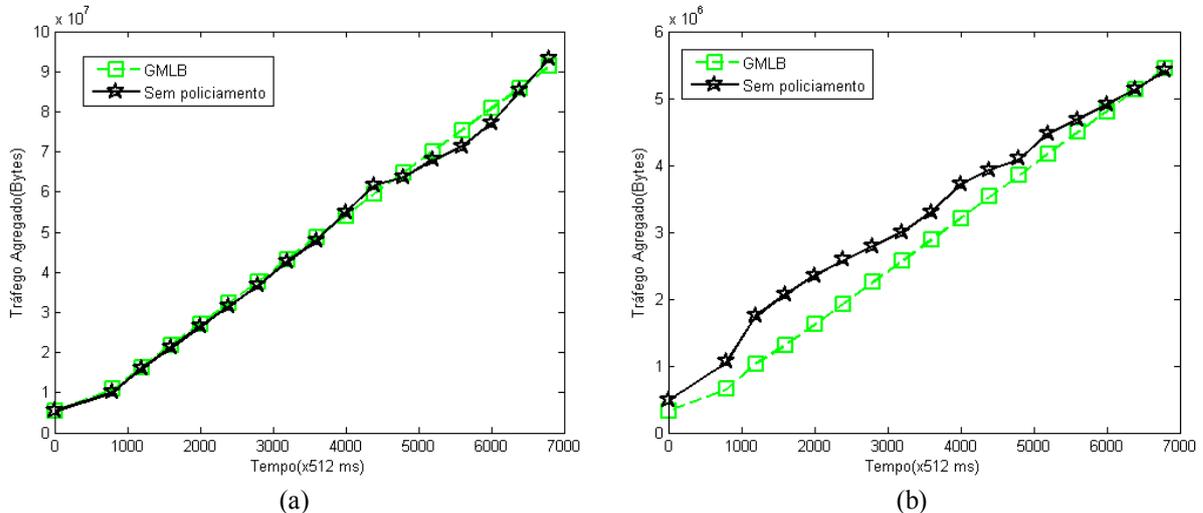


Figura 4.19 - Processo envelope Balde Furado Multifractal Gaussiano para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring

O processo envelope (PE) do algoritmo de policiamento representa a quantidade máxima de pacotes admitidos para a rede. A Figura 4.19 apresenta o processo envelope para $\epsilon = 10^{-6}$ para o algoritmo de policiamento GMLB. Quando o mesmo está abaixo do processo envelope do tráfego sem policiamento, implica em uma maior taxa de perda (P_b) de pacotes para um sistema com o algoritmo de policiamento que para um sistema sem policiamento. A vantagem do uso do algoritmo de policiamento GMLB é que ele mantém o acordo de serviço com a operadora, porém os pacotes acumulados acima da curva do processo envelope do algoritmo serão descartados ou marcados como pacotes de baixa prioridade e poderão ser descartados pelo sistema de transmissão logo em seguida devido a prioridade baixa.

Apesar de apresentar uma grande quantidade de pacotes descartados ou mal comportados (J_n) e os valores médios de J_n , no qual se obteve 3.047 bytes para a série lbl-pkt-5 e 554 bytes para a série USC_06spring, conforme Figura 4.20, o balde furado GMLB apresenta um desempenho melhor que os reguladores de tráfego anteriores devido a sua envoltória estar mais próxima da envoltória do tráfego real (Figura 4.19) para os fluxos de tráfego lbl-pkt-5 e USC_06spring.

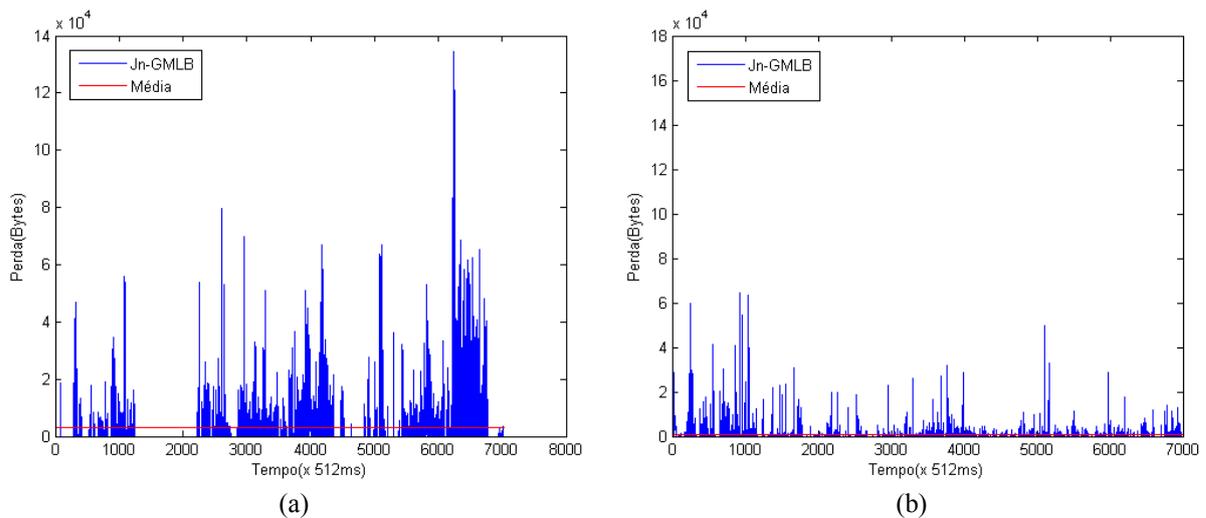


Figura 4.20 - Pacotes descartados ou marcados como baixa prioridade para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento GMLB

Na Tabela 4.4 tem-se a comparação de pacotes marcados como mal comportados (J_n) e da taxa de perda (P_b) de *bytes* para as séries de tráfego sem policiamento e policiadas pelo algoritmo Balde Furado Multifractal Gaussiano (GMLB) para um enlace simples, conforme feito anteriormente com os outros algoritmos de policiamento. Assim, a taxa de saída de pacotes do enlace e tamanho do *buffer* foram considerados novamente iguais a média da quantidade de *bytes* da série de tráfego.

Série (<i>trace</i>) de Tráfego	Perda total sem policiamento (<i>bytes</i>)	Total de J_n com algoritmo GMLB (<i>bytes</i>)	Perda total P_b do tráfego regulado (<i>bytes</i>)
lbl-pkt-5	$2,09 \times 10^7$	$2,14 \times 10^7$	$7,80 \times 10^6$
dec-pkt-3	$1,19 \times 10^7$	$1,72 \times 10^7$	$5,42 \times 10^5$
USC_06spring	$2,80 \times 10^6$	$3,88 \times 10^6$	$1,98 \times 10^6$
Clean_Unina	$3,86 \times 10^6$	$5,50 \times 10^7$	$1,02 \times 10^6$

Tabela 4.4 - Comparativo entre tráfego sem policiamento e com o algoritmo de policiamento GMLB

Na aplicação do algoritmo GMLB, observa-se que a quantidade de *bytes* marcados com baixa prioridade é maior que a quantidade de *bytes* descartados das séries já policiadas, tanto para as séries de tráfego com fio (lbl-pkt-5 e dec-pkt-3), quanto para as séries sem fio (USC_06spring e Clean_Unina).

Verificou-se também através da Figura 4.21, a taxa de perda (P_b) em relação ao tamanho do *buffer* utilizando as séries lbl-pkt-5 [Figura 4.21 (a)] e USC_06spring [Figura 4.21 (b)], onde se confirmou que as séries policiadas pelo algoritmo GMLB apresentam uma

menor taxa de perda que a série sem policiamento.

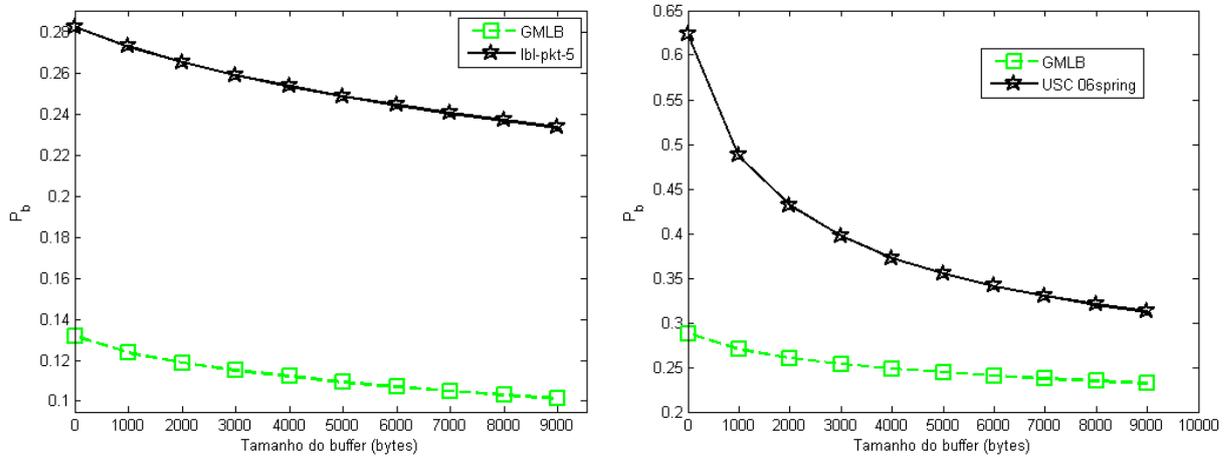


Figura 4.21 - P_b versus tamanho do *buffer* para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento GMLB

4.5 Mecanismo de Policiamento de Chegada Multifractal (*Multifractal Arrival Policing Mechanism* – MAPM)

Nesta seção apresenta-se a proposta de algoritmo de policiamento denominado Mecanismo de Policiamento de Chegada Multifractal (MAPM – *Multifractal Arrival Policing Mechanism*). O MAPM tem seu processo envelope baseado no processo envelope já apresentado anteriormente, o MFBAP. O processo envelope do algoritmo proposto é dado por:

$$\hat{L}_{MAPM}(t) = \bar{a}t + \kappa\sigma^{H(t)} + S \quad (4.21)$$

onde $H(t)$ é o expoente de Hölder, t o instante de tempo, \bar{a} e σ são respectivamente, a média e o desvio padrão do tráfego de entrada, κ é a constante relacionada à probabilidade de violação (para $\varepsilon = 10^{-6}$) do processo envelope. A Figura 4.22 apresenta o processo envelope MAPM para as séries de tráfego lbl-pkt-5 e USC_06spring.

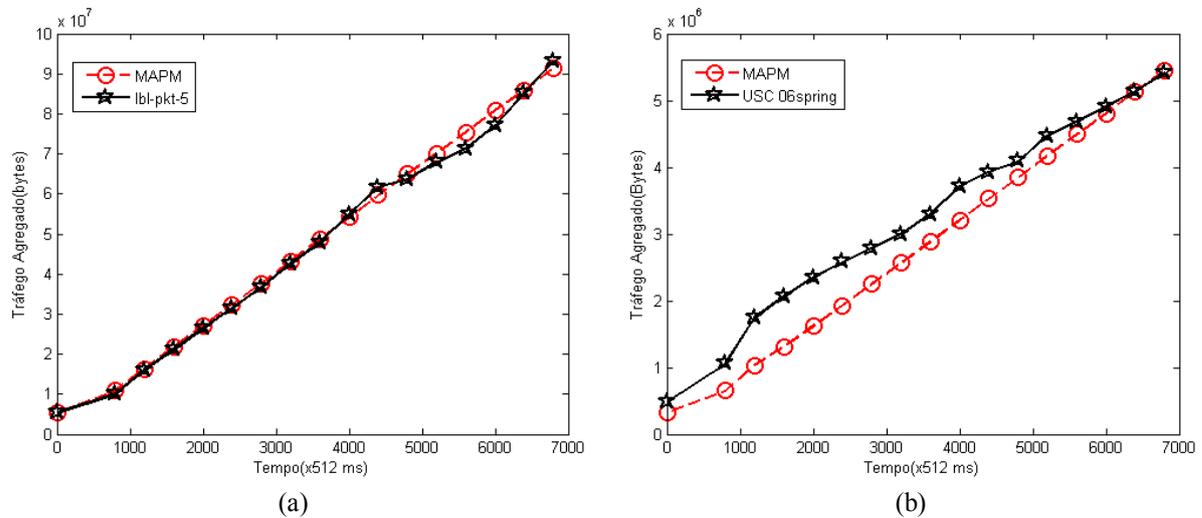


Figura 4.22 - Processo envelope MAPM para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring

O processo envelope MAPM é semelhante ao processo envelope MFBAP. Entretanto, para garantir um melhor desempenho do algoritmo de policiamento, utilizou-se o *software* FracLab (LEGRAND et al., 2009) para estimação do expoente de Hölder.

O controle do algoritmo MAPM é definido pelo seguinte conjunto de equações:

$$E_n = \max\{0, E_{n-1} + X_n - \bar{a}\Delta\} \quad (4.22)$$

$$K_n = \begin{cases} S, & E_n = 0 \\ k\sigma\Delta^{H(n)} \left[n^{H(n)} - (n-1)^{H(n)} \right] + K_{n-1} \end{cases} \quad (4.23)$$

$$J_n = \begin{cases} 0, & E_n \leq K_n \\ X_n - \bar{a}\Delta - k\sigma\Delta^{H(n)} \left[n^{H(n)} - (n-1)^{H(n)} \right] \end{cases} \quad (4.24)$$

onde K_n , E_n e J_n (que possuem as mesmas atribuições citadas para o FLB), sofreram modificações de forma que o policiamento sugerido aproveite as variações do expoente de Hölder das séries de tráfego, e não o parâmetro de Hurst, como no FLB. Esta modificação prevê melhor o comportamento das séries de modo a descartar pacotes o mínimo possível, sem comprometer com isso o desempenho de toda a rede.

O número de *bytes* marcados como mal comportados (J_n) pelo algoritmo MAPM, conforme se observa na Figura 4.23, é maior que os valores de J_n obtidos para os algoritmos anteriores. Porém, essa marcação não prejudicou o tráfego, pois como se observa na Figura 4.22, o tráfego acumulado real está próximo ao processo envelope MAPM. Essa marcação de pacotes como mal comportados ocorreu devido a violação (pacotes em rajadas) por parte do

tráfego entrante que apresentou rajadas superiores às esperadas pelo mecanismo de policiamento. Os valores médios de J_n obtidos para as séries lbl-pkt-5 e USC_06spring foram, respectivamente, 3179 bytes e 542 bytes.

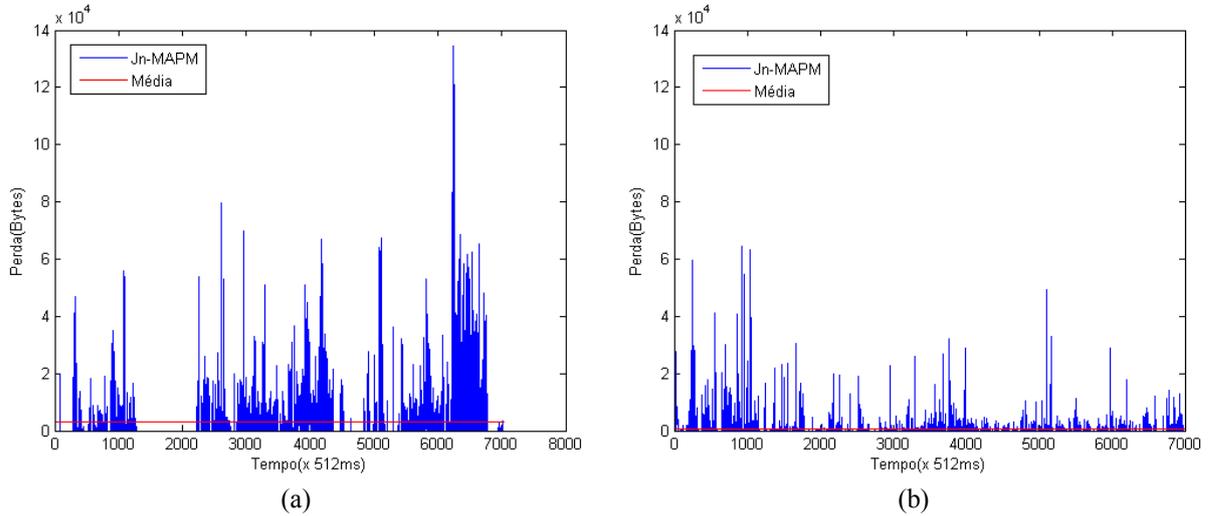


Figura 4.23 - Pacotes descartados ou marcados como baixa prioridade para as séries de tráfego (a) lbl-pkt-5 e (b) USC_06spring utilizando algoritmo de policiamento MAPM

Verifica-se pela Tabela 4.5 que os valores de P_b para as séries de tráfego utilizadas apresentaram valores menores que os valores obtidos para J_n em todas as séries analisadas. Observa-se também, que as taxas de perda (P_b) com o algoritmo de policiamento MAPM foram menores que as séries sem policiamento analisadas (lbl-pkt-5, dec-pkt-3, USC_06spring e Clean_Unina).

Série (<i>trace</i>) de Tráfego	Perda total sem policiamento (<i>bytes</i>)	Total de J_n com algoritmo MAPM (<i>bytes</i>)	Perda total P_b do tráfego regulado (<i>bytes</i>)
lbl-pkt-5	$1,69 \times 10^8$	$9,45 \times 10^7$	$1,32 \times 10^7$
dec-pkt-3	$1,19 \times 10^7$	$1,44 \times 10^8$	$5,41 \times 10^5$
USC_06spring	$2,80 \times 10^6$	$6,24 \times 10^6$	$2,00 \times 10^6$
Clean_Unina	$3,86 \times 10^6$	$5,51 \times 10^7$	$1,12 \times 10^6$

Tabela 4.5 - Comparativo entre tráfego sem policiamento e com o algoritmo de policiamento MAPM

Com base nas informações de perda total do sistema, verifica-se com a Figura 4.24, a relação entre a taxa de perda (P_b) e o tamanho do *buffer* para as séries lbl-pkt-5, Figura 4.24 (a), e USC_06spring, Figura 4.24 (b). A taxa de perda (P_b) das séries policiadas pelo algoritmo MAPM é menor do que a taxa de perda (P_b) sem o policiamento, conforme se

observa na Figura 4.24.

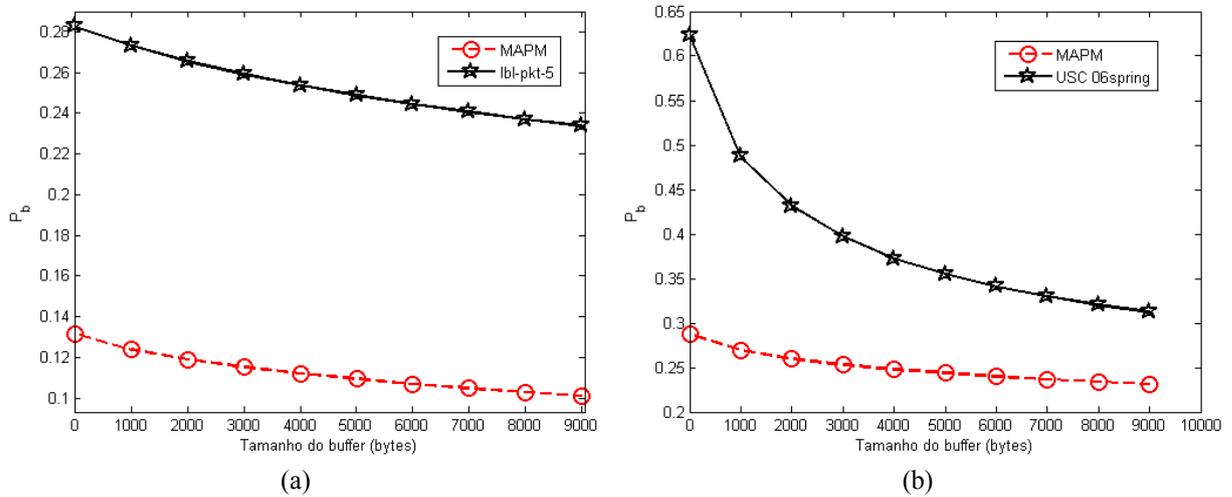


Figura 4.24 - P_b versus tamanho do *buffer* para as séries de tráfego (a) *lbl-pkt-5* e (b) *USC_06spring* utilizando algoritmo de policiamento MAPM

4.6 Comparações Entre os Processos Envelopes dos Algoritmos de Policiamento

O GMLB mostrou-se superior ao FLB em relação a proximidade entre o processo envelope (do algoritmo GMLB) ao do tráfego sem policiamento e da quantidade de pacotes descartados (P_b) para as séries de tráfego analisadas, conforme verificado também por Melo e Fonseca (2004). O objetivo desta seção é comparar o desempenho dos algoritmos MAPM, GMLB, FLB e LB na presença de fluxos de tráfego monofractais e multifractais.

O expoente de Hölder $H(t)$ descreve o grau de singularidade do tráfego, o que é importante na caracterização das rajadas dos dados nas redes de computadores com séries de tráfego multifractais (BIANCHI, 2005). Para o tráfego monofractal, o expoente de Hölder possui teoricamente valor único que é igual ao parâmetro de Hurst (H). Os expoentes de Hölder para as séries de tráfego utilizadas foram obtidos através do programa em Matlab chamado Fraclab (LEGRAND et al., 2009).

Nas simulações, utilizou-se as mesmas séries de tráfego para os algoritmos LB, FLB, GMLB e MAPM, onde Δ foi fixado em 512 ms, S (igual ao valor da média das séries de tráfego em *bytes*) em 13.300 *bytes* para o *trace* *lbl-pkt-5*, 19.665 *bytes* para *dec-pkt-3*, 800 *bytes* para *USC_06spring* e 8.440 *bytes* para o *trace* *USC_2005summer*, e ϵ igual a 10^{-6} para todos os algoritmos de policiamento. O parâmetro de Hurst de cada amostra dos dados requerido pelo FLB foi obtido usando o programa Selfis (KARAGIANNIS, 2010).

Apresenta-se também os processos envelopes obtidos no mesmo gráfico para cada série de tráfego analisada, para melhor verificação do comportamento de cada algoritmo. Nota-se que para um tráfego acumulado com maior variação, o algoritmo de policiamento FLB obteve uma resposta (valor para o processo envelope) muito acima do tráfego acumulado de entrada (sem policiamento).

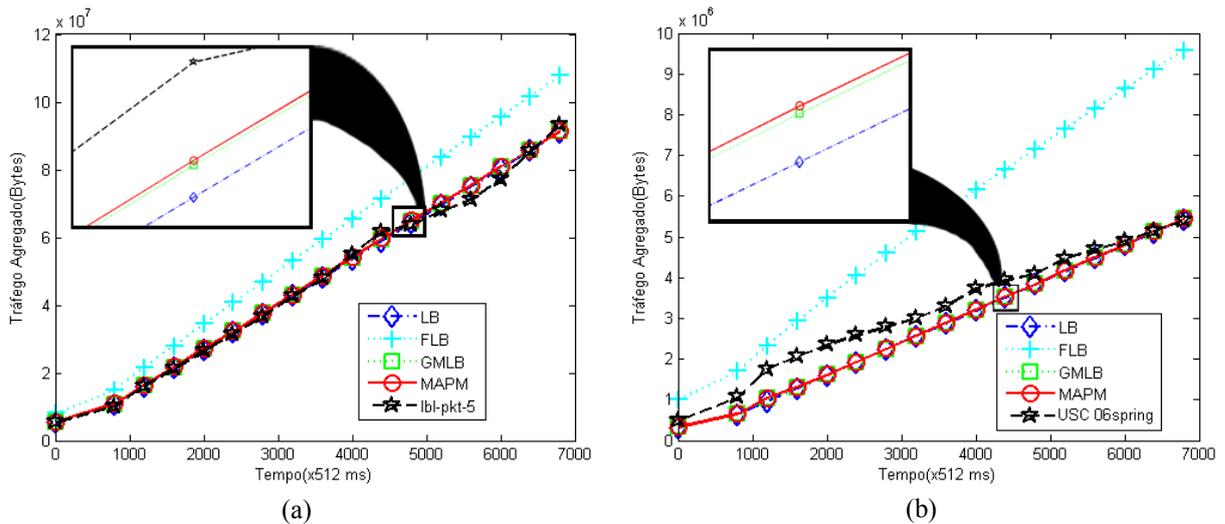


Figura 4.25 - Processo Envelope MAPM, GMLB, FLB e LB para tráfegos (a) lbl-pkt-5 e (b) USC_06spring

Na Figura 4.25, observa-se que o algoritmo de policiamento MAPM foi o que apresentou o processo envelope mais próximo do tráfego sem policiamento, comparado aos outros algoritmos analisados, tanto para o tráfego lbl-pkt-5 [Figura 4.25 (a)], quanto para o USC_06spring [Figura 4.25 (b)].

Para comprovação da eficiência do algoritmo de policiamento MAPM em relação aos processos envelopes apresentados (pois graficamente os valores são muito próximos), calculou-se o erro quadrático médio (EQM) entre o tráfego real acumulado e o processo envelope de cada algoritmo de policiamento, utilizando a seguinte equação (MELLO, 2009):

$$EQM = \frac{\sum_{i=1}^n (Z_m(i) - Z_a(i))^2}{n} \quad (4.25)$$

onde n representa a quantidade de amostras, Z_m o processo envelope real e Z_a o processo envelope de cada algoritmo de policiamento analisado.

Tem-se na Tabela 4.6 o erro quadrático médio entre o processo envelope da série Real (sem policiamento) e os processos envelopes dos algoritmos analisados. O algoritmo

MAPM apresentou um erro quadrático médio menor do que todos os algoritmos para a série USC_06spring. Para as séries lbl-pkt-5 e dec-pkt-3, o algoritmo MAPM foi superado somente pelo algoritmo LB, que em termos de erro quadrático médio, apresentou menor valor que o algoritmo MAPM.

Algoritmo de policiamento	Erro quadrático médio (EQM) ($bytes^2$)			
	lbl-pkt-5	dec-pkt-3	USC_06spring	Clean_Unina
LB	$25,93 \times 10^{11}$	$17,66 \times 10^{11}$	$21,29 \times 10^{10}$	$46,47 \times 10^{11}$
FLB	$14,27 \times 10^{13}$	$21,75 \times 10^{12}$	$10,36 \times 10^{11}$	$28,36 \times 10^{13}$
GMLB	$29,71 \times 10^{11}$	$19,62 \times 10^{11}$	$20,45 \times 10^{10}$	$48,52 \times 10^{11}$
MAPM	$29,31 \times 10^{11}$	$19,44 \times 10^{11}$	$20,26 \times 10^{10}$	$48,33 \times 10^{11}$

Tabela 4.6 - Erro quadrático entre os processos envelopes dos algoritmos LB, FLB, GMLB, MAPM com o Real

A Figura 4.26 apresenta a comparação das taxas de perda (P_b) de todos os algoritmos de policiamento considerados para a série de tráfego lbl-pkt-5, enquanto que a Figura 4.27 compara os valores de P_b para a série de tráfego USC_06spring.

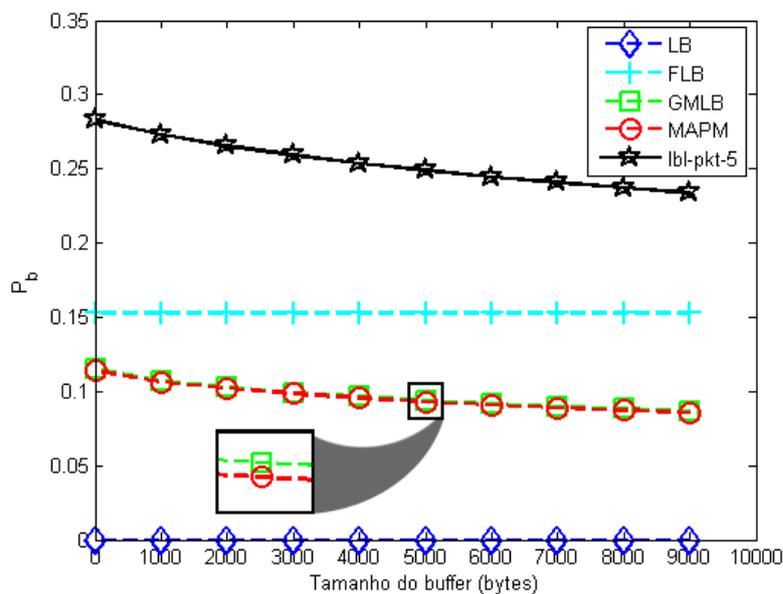


Figura 4.26 - P_b para os algoritmos MAPM, GMLB, FLB e LB para a série de tráfego lbl-pkt-5

Observa-se pela Figura 4.26, que o algoritmo LB apresentou a menor taxa de perda (P_b) de todos os algoritmos, mas o LB não leva em consideração as rajadas do tráfego e após a aplicação dele todos os pacotes estão com valores máximos de $bytes$ iguais à taxa de saída, por isso o algoritmo proposto é mais vantajoso, pois apesar de apresentar P_b maior que

LB, o algoritmo MAPM considera essas características em rajadas. Resultado semelhante se observa na Figura 4.27.

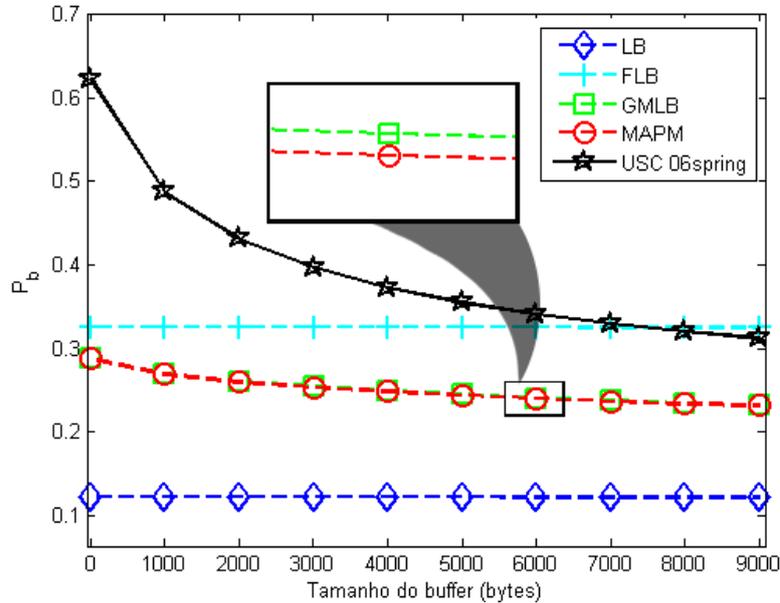


Figura 4.27 - P_b para os algoritmos MAPM, GMLB, FLB e LB para a série de tráfego USC_06spring

Para confirmar o total de *bytes* descartados que as séries poderiam sofrer, calculou-se a soma de J_n e P_b de cada algoritmo de policiamento para as séries de tráfego e apresentou-se os valores obtidos na Tabela 4.7. Observa-se que o algoritmo LB apresenta a menor somatória de perdas para as séries lbl-pkt-5, USC_06spring e Clean_Unina, e o GMLB, para a série dec-pkt-3.

Série de tráfego	$J_n + P_b$ (bytes)			
	LB	FLB	GMLB	MAPM
lbl-pkt-5	$2,66 \times 10^7$	$1,05 \times 10^8$	$2,92 \times 10^7$	$3,98 \times 10^7$
dec-pkt-3	$2,08 \times 10^7$	$3,85 \times 10^7$	$1,77 \times 10^7$	$2,13 \times 10^7$
USC_06spring	$4,26 \times 10^6$	$6,67 \times 10^6$	$5,86 \times 10^6$	$4,48 \times 10^6$
Clean_Unina	$7,00 \times 10^6$	$1,01 \times 10^7$	$7,50 \times 10^6$	$7,59 \times 10^6$

Tabela 4.7 – Somatório de J_n e P_b dos algoritmos de policiamento analisados para as séries de tráfego reais

O retardo provocado pela aplicação dos algoritmos de policiamento nas séries de tráfego será analisado no Capítulo 5.

4.7 Resumo do Capítulo

Neste capítulo apresentou-se alguns dos mais conhecidos algoritmos de policiamento como o Balde Furado (TANENBAUM, 2003) e suas variantes, como o Balde Furado Fractal (MELO; FONSECA, 2004) e Balde Furado Multifractal Gaussiano (TAKADA, 2007) além do modelo mais recente de processo envelope conhecido como Processo de Chegada com Limitante Multifractal (MFBAP) (PEREIRA, 2006).

Apresentou-se também uma proposta de algoritmo de policiamento denominado Mecanismo de Policiamento de Chegadas Multifractais (MAPM). Observou-se, essencialmente neste capítulo:

- Processo Envelope (PE) para os tráfegos com fio e sem fio;
- Processos Envelopes para tráfego com características monofractais e multifractais;
- Principais características dos algoritmos de policiamento LB, FLB, GMLB e MAPM.
- Pacotes descartados ou marcados com baixa prioridade pelo algoritmo de policiamento.

Com estes resultados pode se observar as diferentes formas de tratamento que cada algoritmo efetua para o mesmo tráfego. Diante dessas informações serão apresentadas no Capítulo 5, as avaliações do retardo (*delay*) dos algoritmos de policiamento e do tamanho médio da fila (*backlog*) utilizando o Cálculo de Rede.

CAPÍTULO 5

CÁLCULO DE REDE DETERMINÍSTICO: ESTIMAÇÃO DE *BACKLOG* E RETARDO

Neste capítulo apresentam-se os principais conceitos do Cálculo de Rede (*Network Calculus*) utilizados em análise de tráfego de rede de comunicações para estimação de parâmetros de qualidade, tais como o tamanho médio da fila (*backlog*) e o retardo (*delay*) para cada algoritmo de policiamento de rede aplicado no controle de um enlace simples.

O capítulo está organizado da seguinte forma: na seção 5.1 apresenta-se os principais conceitos do Cálculo de Rede. Na seção 5.2, discursa-se sobre limitantes para *backlog* e retardo. Na seção 5.3, apresenta-se a definição de curvas de chegada e curvas de serviço na seção 5.4. Na seção 5.5, calcula-se o tamanho médio da fila (*backlog*) e retardo. Com a seção 5.6, apresenta-se a análise da utilização média do *buffer* e do enlace para um sistema de fila única e por último, com a seção 5.7 apresenta-se o resumo do capítulo.

5.1 Introdução ao Cálculo de Rede

O Cálculo de Rede Determinístico pode ser utilizado para estimar recursos a fim de prover qualidade de serviço (QoS) em redes e tem fornecido ferramentas poderosas para estimação do *backlog* e do retardo em uma rede com garantia de serviço para fluxos de tráfego individuais. Usando a noção de processo envelope, curvas de chegada e curvas de serviço (CRUZ, 1995), vários trabalhos têm demonstrado que os limitantes de *backlog* e de retardo podem ser concisamente expressos pela álgebra Min-Plus, detalhada no Apêndice A (AGRAWAL et al., 1999; LE BOUDEC, 1998).

O Cálculo de Rede também pode ser visto como a teoria de sistemas que se aplica às redes de computadores, mas a principal diferença é considerar-se outra álgebra, onde as operações são alteradas da seguinte forma: adição torna-se o cálculo do mínimo, e a

multiplicação torna-se adição.

Um algoritmo de policiamento obriga o fluxo de entrada $x(t)$ a ter uma saída $y(t)$ que se conforma a um determinado conjunto de taxas de acordo com um processo envelope de tráfego A (série de tráfego), à custa de, possivelmente, atrasar *bits* no *buffer*. A entrada e saída de fluxos acumulados são definidas, por Le Boudec (1998), como o número de *bits* visto no fluxo de dados no intervalo de tempo $[0, t]$. Essas funções são não-decrescentes com o tempo t . O parâmetro t pode ser contínuo ou discreto.

A convolução Min-Plus entre A e x é dada por:

$$y(t) = (A \otimes x)(t) = \inf_{s \in \mathbb{R} | 0 \leq s \leq t} \{A(t-s) + x(s)\} \quad (5.1)$$

A convolução na teoria de sistemas tradicionais é tanto comutativa quanto associativa. Por exemplo, a resposta ao impulso do circuito da Figura 5.1 (a) é a convolução da resposta ao impulso de cada uma das células elementares:

$$h(t) = (h_1 \otimes h_2)(t) = \int_0^t h_1(t-s)h_2(s)ds \quad (5.2)$$

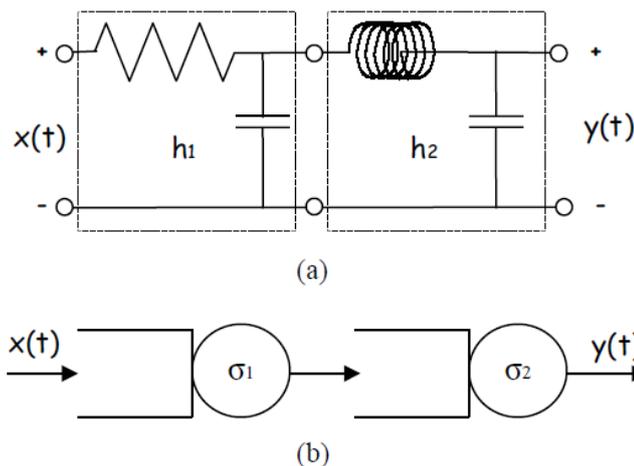


Figura 5.1 - A resposta ao impulso da concatenação de dois circuitos lineares é (a) a convolução da resposta ao impulso individual, a curva de formação da concatenação de dois reguladores é (b) a convolução das curvas individuais modeladas (LE BOUDEC; THIRAN, 2004)

A mesma propriedade é utilizada para o regulador de tráfego. A saída do segundo regulador na Figura 5.1 (b) é na verdade igual a $y(t) = (A \otimes x)(t)$, onde:

$$A(t) = (A_1 \otimes A_2)(t) = \inf_{s \in \mathbb{R} | 0 \leq s \leq t} \{A_1(t-s) + A_2(s)\} \quad (5.3)$$

5.2 Limitantes para *Backlog* e Retardo

Dadas as funções de entrada $R(t)$ e saída $R^*(t)$, derivam-se as duas seguintes quantidades de interesse.

Define-se que para se obter os valores de *backlog* e retardo em um sistema sem perdas tem-se (LE BOUDEC; THIRAN, 2004):

- O tamanho médio da fila (*backlog*) no tempo t é dado por $R(t) - R^*(t)$.
- O retardo (*delay*) no instante t é dado por:

$$d(t) = \inf \{ \tau \geq 0 : R(t) \leq R^*(t + \tau) \} \quad (5.4)$$

O *backlog* é a quantidade de *bits* que são mantidos dentro do sistema. Se o sistema possui *buffer* único, o *backlog* representa o comprimento da fila. Em contrapartida, se o sistema é mais complexo, então o *backlog* é o número de *bits* em trânsito, assumindo que se pode observar a entrada e saída simultaneamente. O retardo no instante t é o retardo experimentado por um *bit* chegando no tempo t se todos os *bits* recebidos antes dele forem servidos antes também. Na Figura 5.2 (a), o *backlog*, chamado de $x(t)$, é mostrado como o desvio vertical entre as funções de entrada e saída.

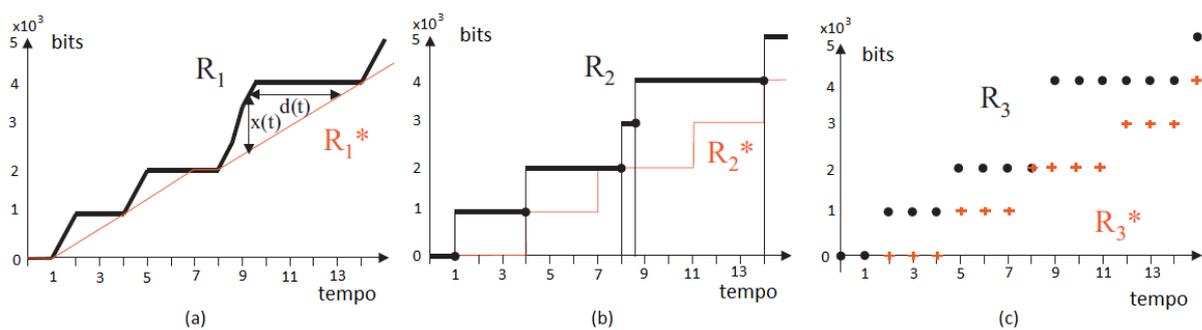


Figura 5.2 - Exemplos de funções de entradas e saídas (LE BOUDEC; THIRAN, 2004)

O retardo é o desvio horizontal apresentado na Figura 5.2 (a) e chamado de $d(t)$. Se as funções de entrada e de saída são contínuas (modelo fluido), então é fácil ver que $R^*(t + d(t)) = R(t)$, e que $d(t)$ é o menor valor que satisfaça esta equação.

A Figura 5.2 mostra que os valores de *backlog* e retardo são ligeiramente diferentes para os três modelos. Assim, o retardo experimentado pelo último *bit* do primeiro

pacote é $d(2) = 2$ unidades de tempo para a Figura 5.2 (a). Nota-se que $d(1) = 3$ unidades de tempo para o retardo, conforme demonstrado na Figura 5.2 (b). Ambos, naturalmente, estão de acordo com as diferentes hipóteses feitas para cada um dos modelos. Da mesma forma, o retardo para o quarto pacote na Figura 5.2 (b) é $d(8,6) = 5,4$ unidades de tempo, o que corresponde a 2,4 unidades de tempo de espera e 3 unidades de tempo de serviço. Contudo, na Figura 5.2 (c), R_3 tem-se $d(9) = 6$ unidades; a diferença é a perda de precisão resultante da discretização.

5.3 Definição de Curva de Chegada

Aborda-se nesta seção o conceito de Processo Envelope (apresentado no Capítulo 4) do Cálculo de Rede, também denominado Curva de Chegada.

Para oferecer garantias de QoS aos fluxos de dados é necessário suporte apropriado na rede (LE BOUDEC; THIRAN, 2004). Além disso, é preciso limitar o tráfego enviado pelas fontes.

Define-se para curva de chegada, que dada uma função α definida para $t \geq 0$, diz-se que um fluxo R é limitado por α se todo $t \leq s$, onde (LE BOUDEC; THIRAN, 2004):

$$R(t) - R(s) \leq \alpha(t - s) \quad (5.5)$$

Pode se dizer que R tem α como uma curva de chegada, ou ainda que R é α -suave.

5.4 Definição de Curvas de Serviço

As chegadas de um fluxo em um nó de rede no intervalo de tempo $[0, t)$ são dadas em termos da função $A(t)$. As saídas de um fluxo a partir do nó, no intervalo de tempo $[0, t)$ são denotadas por $D(t)$ com $D(t) \leq A(t)$. O *backlog* de um fluxo no tempo t , denotado por $B(t)$, é dado por:

$$B(t) = A(t) - D(t) \quad (5.6)$$

O retardo no tempo t , denotado por $W(t)$, é o retardo experimentado por um processo de chegada que se afasta no tempo t , dado por:

$$W(t) = \inf \{d \geq 0 \mid A(t - d) \leq D(t)\} \quad (5.7)$$

Utiliza-se $A(x, y)$ e $D(x, y)$ para denotar as chegadas e partidas no intervalo de tempo $[x, y)$, com $A(x, y) = A(y) - A(x)$ e $D(x, y) = D(y) - D(x)$. Adotou-se as seguintes hipóteses sobre as funções de chegada:

(A1) não-negatividade: Os pacotes recém-chegados em qualquer intervalo de tempo são não-negativos. Ou seja, para qualquer $x < y$, tem-se que $A(y) - A(x) \geq 0$.

(A2) limite superior: Os pacotes recém-chegados A de um fluxo são limitados por uma função subadaptativa A^* , chamado de envelope de chegada, tal que $A(t + \tau) - A(t) \leq A^*(\tau)$ para todo $t, \tau \geq 0$.

A convolução é denotada por $*$ (exemplo, $f * g$ de duas funções f e g) e a deconvolução é denotada por \otimes (exemplo, $f \otimes g$ de duas funções f e g) (LE BOUDEC; THIRAN, 2004).

Uma curva mínima de serviço para um fluxo é uma função S que especifica um limite inferior para o serviço prestado ao fluxo de tal forma que, para todo $t \geq 0$,

$$D(t) \geq A * S(t) \quad (5.8)$$

Uma curva de serviço máxima para um fluxo é uma função \bar{S} que especifica um limite superior sobre o serviço prestado a um fluxo tal que, para todo $t \geq 0$,

$$D(t) \leq A * \bar{S}(t) \quad (5.9)$$

A curva de serviço mínima desempenha um importante papel no Cálculo de Rede, uma vez que ela provê garantias de serviço. Portanto, assim como ocorre na literatura relacionada, muitas vezes a referência a uma curva mínima de serviço ocorre simplesmente como curva de serviço. Caso uma curva máxima de serviço não seja dada, pode-se usar $\bar{S}(t) = Ct$, onde C é a capacidade do enlace.

Os dois teoremas apresentados por Agrawal et al. (1999) e Le Boudec (1998) resumem alguns resultados-chave do Cálculo de Rede Determinístico. Nesta seção seguiu-se a notação utilizada em Agrawal et al. (1999).

Para o Cálculo de Rede Determinístico, dado um envelope de chegada de um fluxo com curva mínima de serviço S , tem-se (AGRAWAL et al., 1999; LE BOUDEC, 1998):

- **Processo Envelope.** A função $D^* = A^* \otimes S$ é um processo envelope para as séries de tráfego, no sentido de que, para todo $t, \tau \geq 0$,

$$D^*(t) \geq D(t + \tau) - D(\tau) \quad (5.10)$$

- **Limitante para o Tamanho Médio da Fila (*Backlog Bound*).** Um limitante superior para o *backlog*, denotado por b_{\max} , é dado por:

$$b_{\max} = A^* \otimes S(0) \quad (5.11)$$

- **Limitante para Retardo (*Delay Bound*).** Um limitante superior para o retardo, denotado por d_{\max} , é dada por:

$$d_{\max} = \inf \{d \geq 0 \mid \forall t \geq 0: A^*(t - d) \leq S(t)\} \quad (5.12)$$

Com o Teorema 5.5.1 as curvas de serviço de rede podem ser usadas para determinar os limitantes para retardo e *backlog* dos fluxos individuais em uma rede.

5.5 Cálculo do Tamanho Médio da Fila (*Backlog*) e do Retardo (*Delay*)

Nesta seção são apresentados os resultados do Cálculo de Rede (*Network Calculus*) aplicado a uma rede de transmissão constituída por um enlace simples (*buffer* finito). Obtiveram-se os resultados da equação (5.11) para os limitantes do tamanho médio da fila (*backlog bound*) considerando um sistema de fila única finita, onde se propôs para o envelope A^* , o processo envelope (tráfego agregado) de cada algoritmo de policiamento analisado.

Apresenta-se da Figura 5.3 até a Figura 5.6 os limitantes para o tamanho médio das filas de acordo com cada algoritmo de policiamento considerado. Para as séries de tráfego com fio lbl-pkt-5 e dec-pkt-3 obteve-se a Figura 5.3 e Figura 5.4, respectivamente. Os limitantes para as séries de tráfego sem fio USC_06spring e USC_2005summer são apresentadas na Figura 5.5 e Figura 5.6, respectivamente. Note que Real na legenda das figuras representa o limitante para *backlog* para o tráfego sem policiamento. Para a obtenção das figuras foram coletados diversos resultados com a variação no tamanho do *buffer* do enlace considerado.

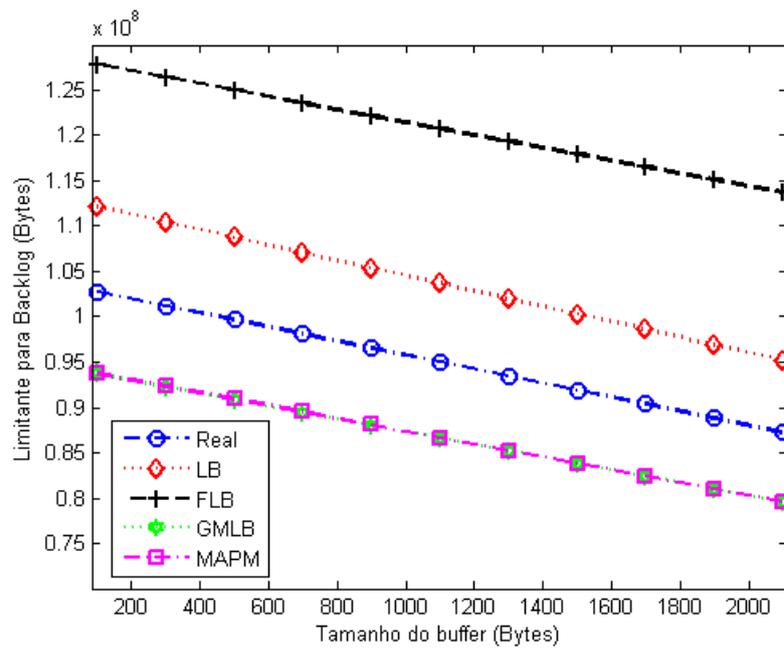


Figura 5.3 - Limitantes para *backlog* para a série de tráfego com fio lbl-pkt-5

Observa-se que para o tráfego lbl-pkt-5 (Figura 5.3), o algoritmo de policiamento MAPM obteve os menores valores de *backlog*, acompanhado pelo GMLB que está sobreposto a ele (ao MAPM). Sendo assim, observa-se que a aplicação do algoritmos GMLB e MAPM apresentaram limitantes para *backlog* menores que o tráfego sem policiamento (Real). Os algoritmos LB e FLB apresentaram os maiores valores de limitante para *backlog* para a série (lbl-pkt-5). Resultado observado também para a série dec-pkt-3 (Figura 5.4).

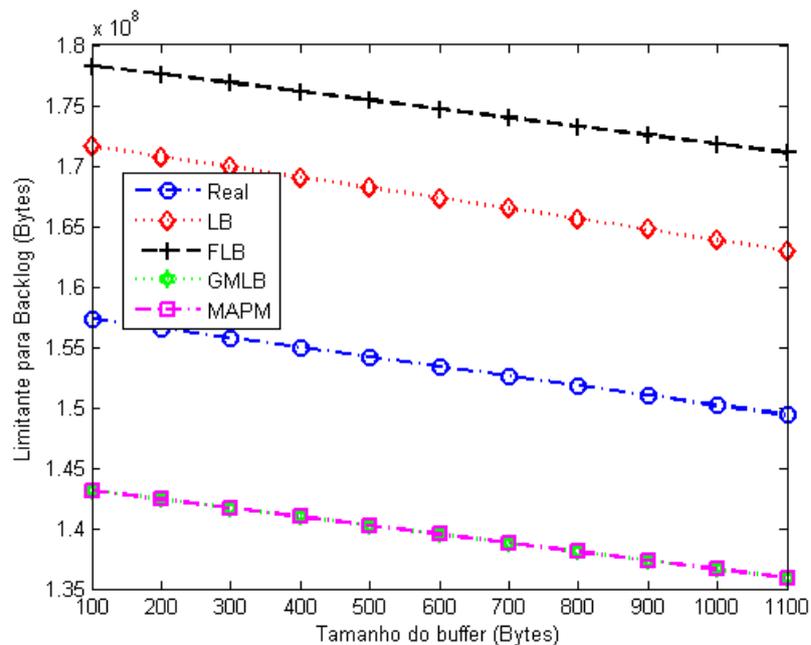


Figura 5.4 - Limitantes para *backlog* para a série de tráfego com fio dec-pkt-3

Com a série USC_06spring, apresentada na Figura 5.5, observa-se que o algoritmo LB apresentou menor valor de limitante para *backlog*, após o tamanho do *buffer* ultrapassar o valor de 700 bytes. O algoritmo FLB apresentou o maior valor de limitante para *backlog* e os algoritmos MAPM e GMLB estão sobrepostos e com valor de limitante para *backlog* abaixo do tráfego sem policiamento.

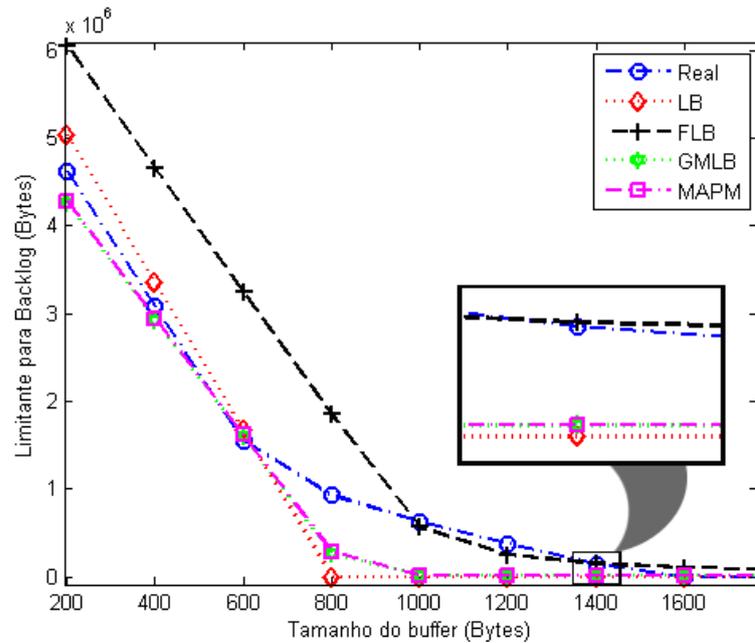


Figura 5.5 - Limitantes para *backlog* para a série de tráfego sem fio USC_06spring

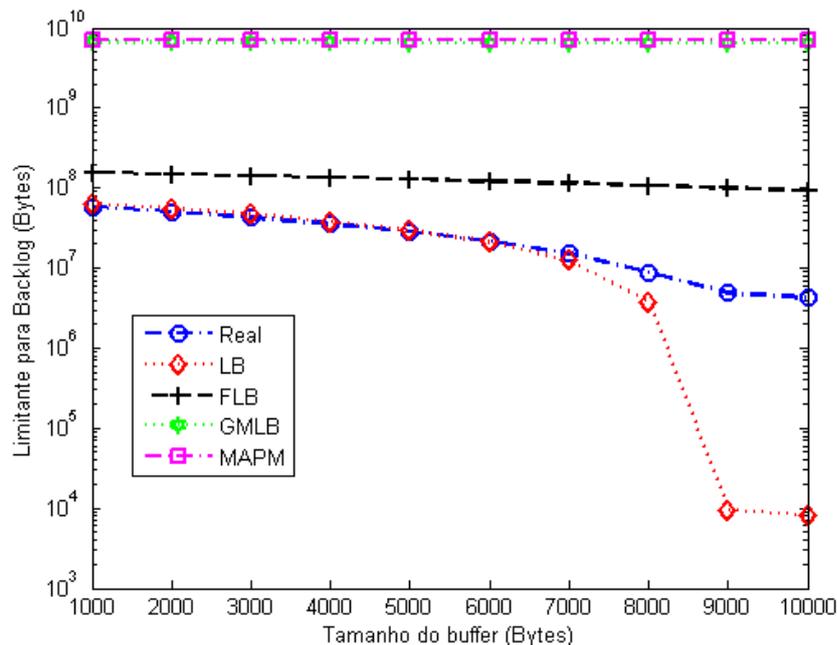


Figura 5.6 - Limitantes para *backlog* para a série de tráfego sem fio USC_2005summer

Conforme se observa na Figura 5.6, para a série USC_2005summer, os algoritmos MAPM e GMLB apresentam limitante para *backlog* bem próximos um do outro, além de representarem os maiores valores obtidos (de limitante para *backlog*). O algoritmo LB, após o tamanho do *buffer* superior a 6.000 *bytes*, apresentou o menor valor de limitante para *backlog*.

Em relação às simulações envolvendo retardo, observou-se o limitante para retardo obtido pela equação (5.12) para as séries de tráfego analisadas, onde se propôs a substituição de A^* pelo processo envelope de cada algoritmo de policiamento e das séries de tráfego sem policiamento, conforme se apresenta da Figura 5.7 até a Figura 5.10.

Para a série lbl-pkt-5, apresentada na Figura 5.7, observa-se que o algoritmo MAPM apresenta o maior valor de limitante para retardo de todos os algoritmos de policiamento. O algoritmo LB apresenta a menor limitante para retardo, porém esse valor é superior ao do Real (tráfego sem policiamento).

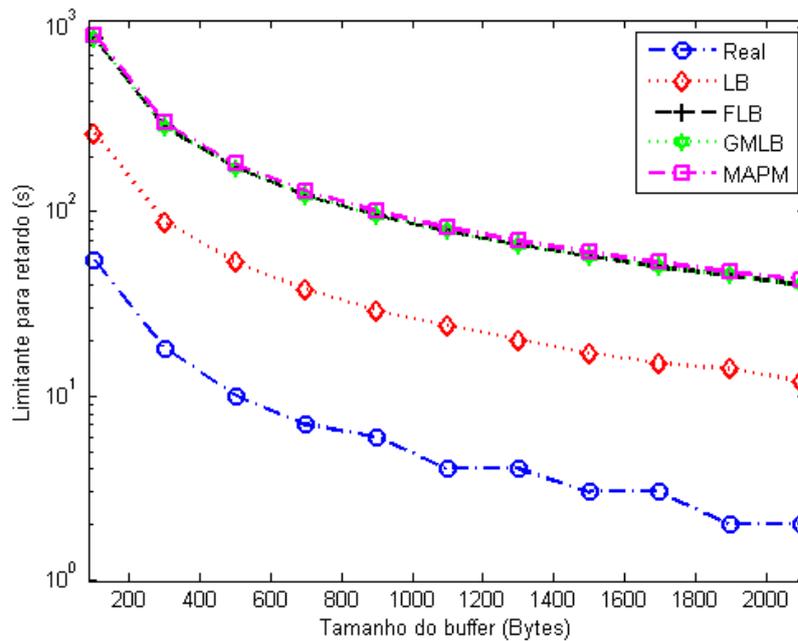


Figura 5.7 - Limitantes para retardo para a série de tráfego com fio lbl-pkt-5

Com a Figura 5.8, observa-se que a série dec-pkt-3 apresentou o menor limitante para retardo sem policiamento. O MAPM apresentou o maior valor de retardo dos algoritmos de policiamento, seguido do GMLB e FLB, que seguem sobrepostos.

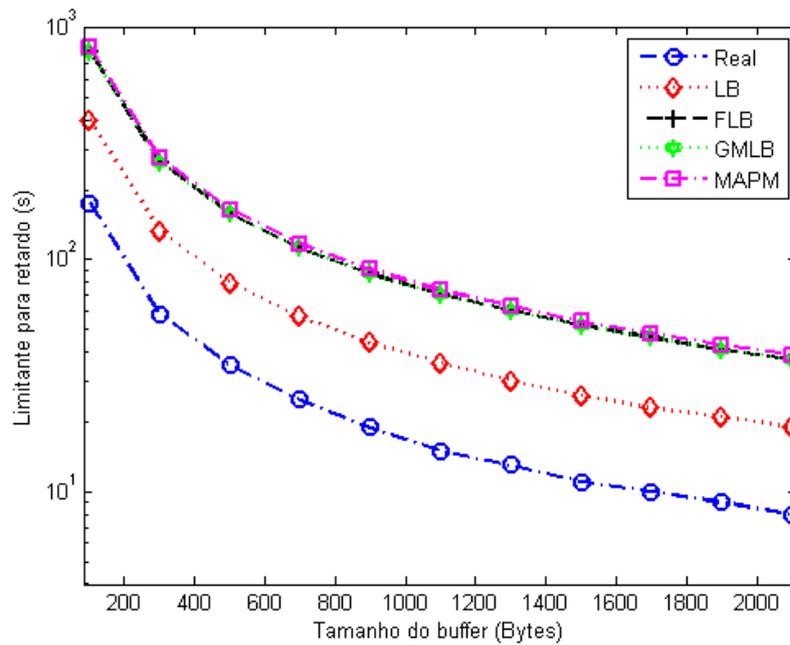


Figura 5.8 - Limitantes para retardo para a série de tráfego com fio dec-pkt-3

Observa-se com a Figura 5.9 (para a série USC_06spring), que para o tamanho do *buffer* superior a 600 bytes, o valor do limitante para retardo do FLB passa a ser o maior de todos os valores apresentados. O algoritmo LB apresentou o menor valor de limitante (para retardo), comparado a todos os algoritmos de policiamento analisados, que após o tamanho do *buffer* superar o valor de 800 bytes, apresentou limitante para retardo sobreposta à da série sem policiamento (Real).

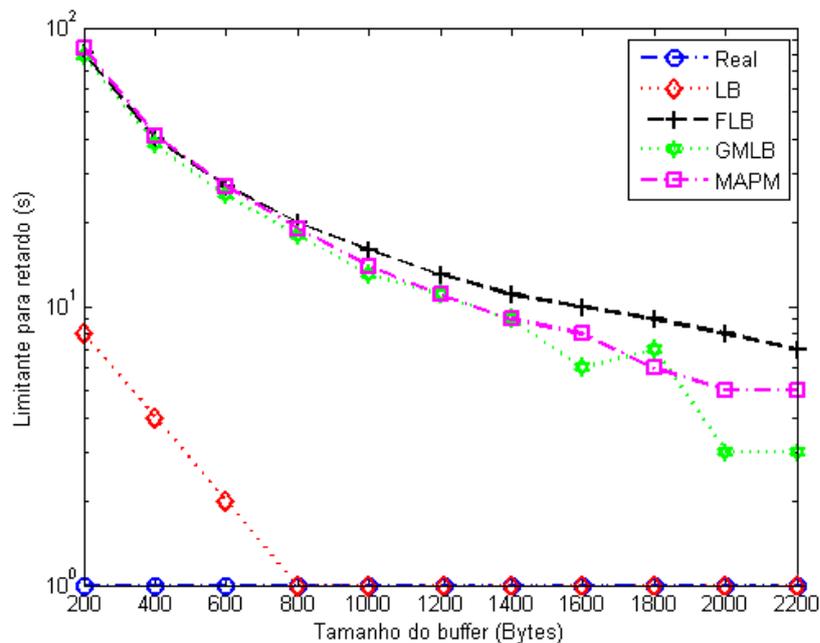


Figura 5.9 - Limitantes para retardo para a série de tráfego sem fio USC_06spring

Com a série de tráfego USC_2005summer, apresentada na Figura 5.10, obteve-se o maior valor de limitante para retardo com o algoritmo MAPM. Observou-se também, que o GMLB e FLB seguem sobrepostos logo abaixo do valor de MAPM, além do LB apresentar menor valor de limitante para retardo de todos os algoritmos de policiamento estudados (para a série USC_2005summer).

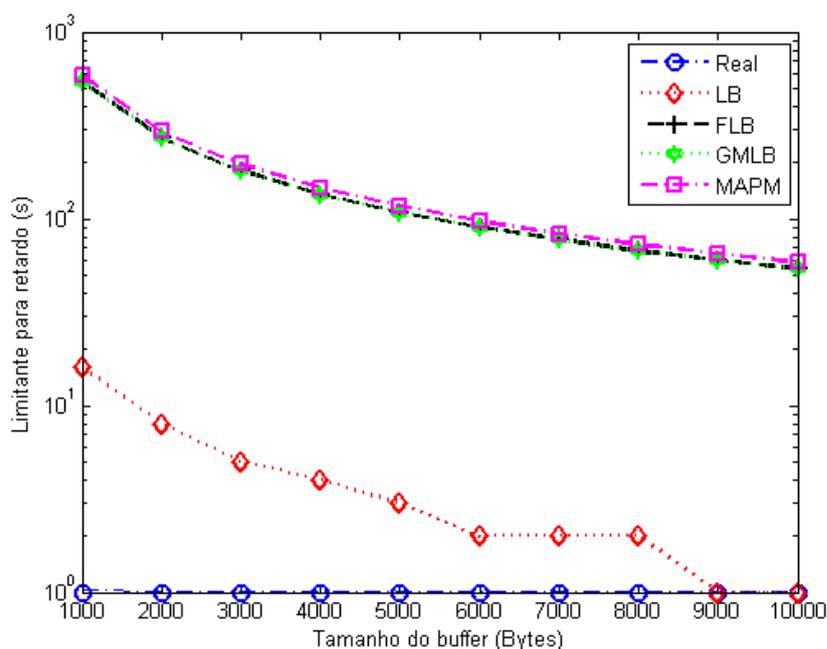


Figura 5.10 - Limitantes para retardo para a série de tráfego sem fio USC_2005summer

Também é possível observar que houve um aumento no retardo para as séries de tráfego de rede após a aplicação dos algoritmos de policiamento. No caso da proposta MAPM, houve tanto um acréscimo no retardo quanto no *backlog* para as séries de tráfego USC_06spring e USC_2005summer. Porém a quantidade de pacotes descartados foi menor que o tráfego sem policiamento em todos os casos, fator de grande relevância para um algoritmo de policiamento de tráfego de rede.

5.6 Análise da Utilização Média do *Buffer* e do Enlace

Nesta seção, apresentam-se os resultados obtidos das análises de utilização média do *buffer* e utilização do enlace, para um enlace simples com *buffer* finito, conforme ilustra a Figura 5.11. Para este enlace, a taxa de transmissão do sistema (capacidade), foi fixada como sendo a média da taxa de *bytes* das séries sem algoritmo de policiamento.

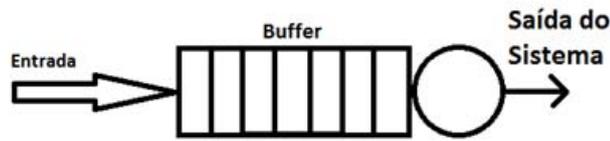


Figura 5.11 - Sistema de enlace simples e *buffer* finito

O *buffer* é aplicado em situações que exigem armazenamento temporário de dados, como no caso de um enlace simples, onde os dados são armazenados caso cheguem em um intervalo de tempo superior ao intervalo de saída do sistema. A utilização instantânea do *buffer* $u_b(t)$ é dada pela equação:

$$u_b(t) = \frac{Q_r(t)}{Q_{\max}} \quad (5.13)$$

onde $Q_r(t)$ é o tamanho do *buffer* utilizado no instante de tempo t e Q_{\max} o tamanho máximo do *buffer*.

A análise da utilização média do *buffer* $E\{u_b(t)\}$ para as séries de tráfego com fio é apresentada na Figura 5.12. Observa-se que a série policiada pelo algoritmo proposto (MAPM) apresentou-se mais próxima da série sem policiamento lbl-pkt-5 [Figura 5.12 (a)], porém a série sem policiamento e a policiada pelo algoritmo LB apresentaram menores valores para utilização de *buffer*. Para o tráfego dec-pkt-3, Figura 5.12 (b), observa-se que à medida que se aumentou a capacidade do *buffer* (acima de 6.000 bytes), a utilização do *buffer* pelo algoritmo MAPM que inicialmente estava acima do tráfego sem policiamento, passou a ser menor que a mesma, ficando acima somente do tráfego policiado pelo algoritmo LB.

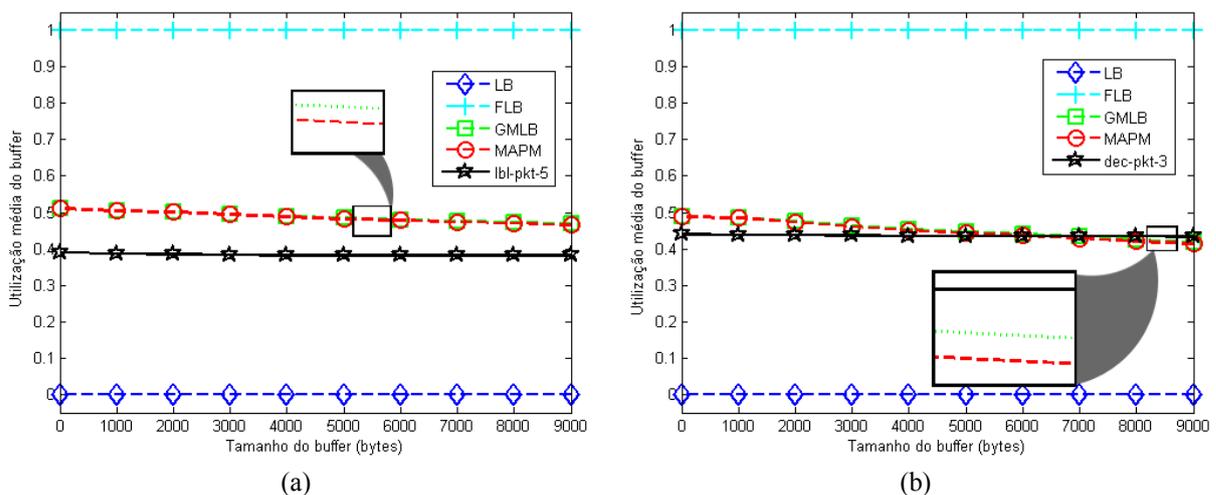


Figura 5.12 - Utilização média do *buffer* para séries de tráfego com fio (a) lbl-pkt-5 e (b) dec-pkt-3

Com as séries de tráfego sem fio, Figura 5.13, observou-se que para o tráfego USC_06spring [Figura 5.13 (a)], a série policiada pelo algoritmo MAPM apresentou utilização média do *buffer* menor que do algoritmo GMLB quando o tamanho do *buffer* ultrapassou os 7.000 *bytes*, porém continuou acima da utilização média do *buffer* da série de tráfego sem policiamento e policiado pelo LB.

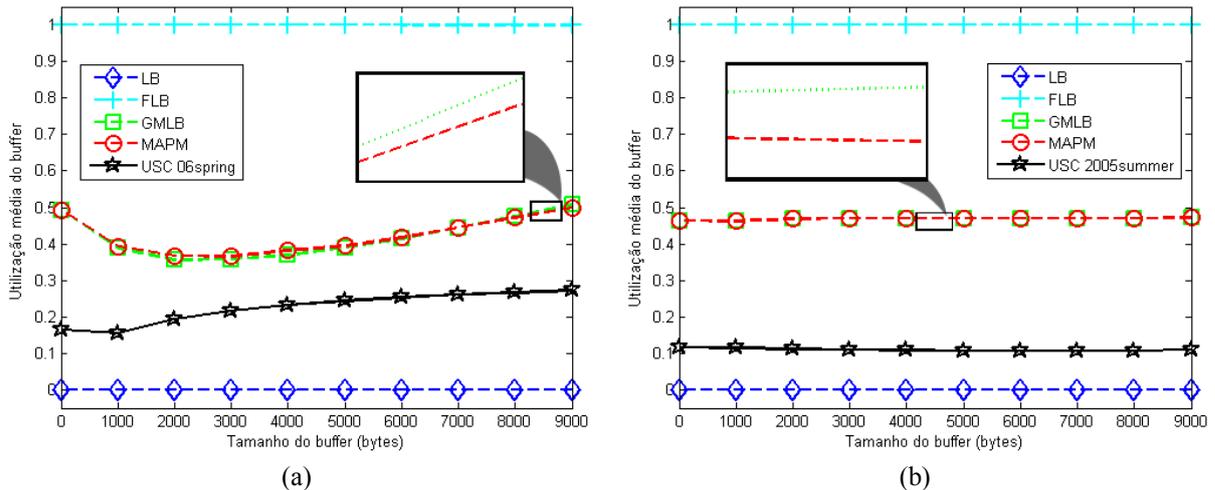


Figura 5.13 - Utilização média do *buffer* para séries de tráfego sem fio (a) USC_06spring e (b) USC_2005summer

Para a série USC_2005summer conforme mostra a Figura 5.13 (b), a utilização média do *buffer* para o algoritmo MAPM e GMLB ficaram bem próximos e somente com o aumento da figura, visualiza-se que a utilização média do *buffer* do MAPM se apresenta ligeiramente abaixo do GMLB, mas ainda está acima do algoritmo LB e da série sem policiamento. Observou-se também que o algoritmo FLB apresentou utilização do *buffer* em 100% para todas as séries de tráfego analisadas e que o algoritmo LB não utilizou o *buffer* do enlace, visto que o tráfego após ser policiado obteve todos os pacotes acima da taxa média de saída (capacidade do enlace) descartados.

Outro fator importante a ser analisado é a utilização do enlace u_e , que pode ser obtida através da equação (MATA, 2002):

$$u_e = \frac{\lambda_i \cdot E\{X(t)\}}{C} \quad (5.14)$$

onde λ_i é a taxa média de chegada em pacotes/s, $E\{X(t)\}$ a esperança matemática da série de tráfego (tamanho médio do pacote) e C a capacidade de transmissão do enlace (para as

simulações utilizou-se C igual a média da série de tráfego analisada).

A utilização do enlace pelos algoritmos LB e FLB foi máxima (100%) para as séries de tráfego de rede com fio (lbl-pkt-5 e dec-pkt-3) e sem fio (USC_06spring e USC_2005summer), conforme se observa na Figura 5.14 para as séries de rede com fio e Figura 5.15 para as séries de rede sem fio

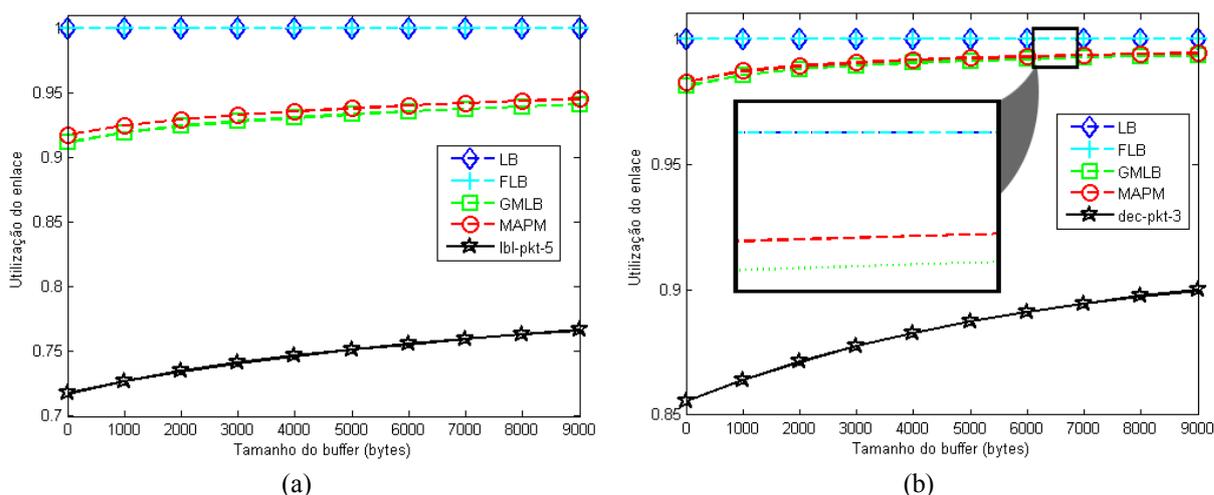


Figura 5.14 - Utilização do enlace para séries de tráfego com fio (a) lbl-pkt-5 e (b) dec-pkt-3

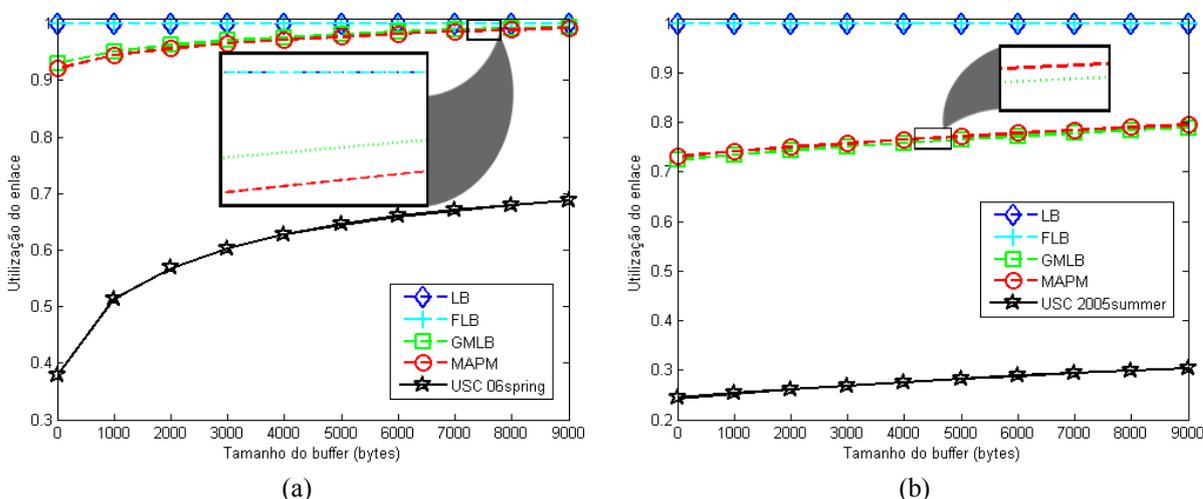


Figura 5.15 - Utilização do enlace para séries de tráfego sem fio (a) USC_06spring e (b) USC_2005summer

Com o algoritmo MAPM obteve-se a utilização de enlace mais próxima da série sem policiamento [conforme Figura 5.15 (a)], além de representar o menor valor (de utilização de enlace) entre os algoritmos de policiamento para a série USC_06spring. Já para as séries lbl-pkt-5, dec-pkt-3 (Figura 5.14) e USC_2005summer [Figura 5.15 (b)], o algoritmo GMLB apresentou a utilização do enlace mais próxima da série sem policiamento. Isso faz

com que o dimensionamento de enlace para o algoritmo MAPM apresente menor custo que os outros algoritmos de policiamento.

5.7 Resumo do Capítulo

Neste capítulo apresentou-se os principais conceitos do Cálculo de Rede (*Network Calculus*) Determinístico aplicado à análise do comportamento do tráfego de rede (para análise de *backlog* e retardo) utilizando os diferentes processos envelopes dos algoritmos de policiamento. As principais questões analisadas envolvendo os algoritmos de policiamento foram:

- Limitante para o tamanho da fila (*backlog bound*);
- Limitante para o retardo (*delay bound*);
- Utilização média do *buffer* para enlace simples;
- Utilização do enlace para *buffer* finito.

CAPÍTULO 6

POLICIAMENTO DE TRÁFEGO EM REDES WiMAX BASEADO EM MODELAGEM MULTIFRACTAL

Neste capítulo, aplica-se os algoritmos de policiamento descritos a um sistema de transmissão WiMAX simplificado. O sistema WiMAX considerado é o descrito em Niyato e Hossain (2005), onde se utiliza modulação OFDM/TDMA e escalonamento *round-robin* para encaminhamento dos pacotes vindos dos diferentes usuários.

Algoritmos de policiamento de tráfego de rede são utilizados para organizar a chegada dos pacotes na entrada do sistema WiMAX. Dentre os modelos apresentados, o algoritmo de policiamento proposto MAPM, que leva em consideração as características multifractais do tráfego real, foi aplicado a fim de se comprovar a sua eficiência no sistema WiMAX considerado.

Utilizou-se o Cálculo de Rede apresentado no capítulo anterior para verificação do tamanho médio da fila (*backlog*) e retardo (*delay*) de pacotes no sistema WiMAX sem e com algoritmos de policiamento.

Na seção 6.1, descreve-se o sistema de transmissão OFDM/TDMA baseado em redes WiMAX. Apresenta-se na seção 6.2, as simulações e resultados obtidos como as perdas de dados (*bytes*) para cada algoritmo de policiamento de tráfego de rede (na subseção 6.2.1) e a análise de retardo e tamanho médio da fila através do Cálculo de Rede para o sistema WiMAX (na seção 6.3). Finalizando, apresenta-se na seção 6.4 o resumo dos resultados obtidos.

6.1 Sistema de Transmissão OFDM/TDMA Baseado em Redes WiMAX

O modelo considerado para o sistema WiMAX baseado em OFDM/TDMA é apresentado na Figura 6.1. Considera-se um sistema de transmissão OFDM semelhante ao cenário apresentado em Niyato e Hossain (2005), com n usuários e o número total de m canais de tráfego (ROCHA; VIEIRA; SANTOS JR., 2010).

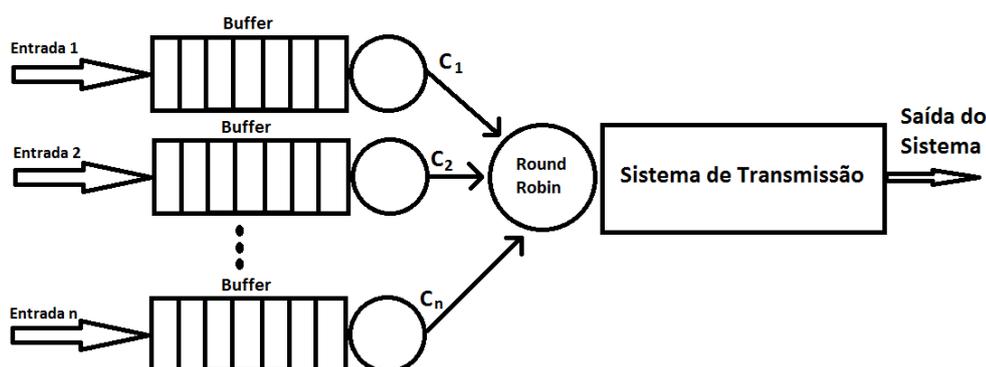


Figura 6.1 - Modelo OFDM/TDMA com escalonamento *Round Robin* (ROCHA; VIEIRA; SANTOS JR., 2010)

No sistema WiMAX considerado, o tráfego de dados para cada usuário é protegido em uma fila separada e o tamanho do *buffer* é fixo. Considerou-se um cenário baseado em características TDMA de múltiplos acessos e escalonamento *round-robin* (BURNS; HARBOUR; WELLINGS, 2003). A ideia central do algoritmo *round-robin* é que todos os processos são armazenados em uma fila circular, conforme Figura 6.1 (ROCHA; VIEIRA; SANTOS JR., 2010; BURNS; HARBOUR; WELLINGS, 2003).

O escalonador inspeciona fila por fila alocando os recursos necessários para cada processo de um *quantum* (pequena unidade de tempo). Se o processo não terminar após um *quantum*, a fila entra em modo de espera (*vacation*), até chegar outra oportunidade para ser servido. Se o processo terminar antes de um *quantum*, o servidor é liberado da fila e o próximo é servido. Em ambos os casos, após a liberação da fila atual, um novo (ou próximo) processo é escolhido na fila seguinte. Devido às suas características, o escalonamento *round-robin* é amplamente utilizado, especialmente para sistemas de tempo compartilhado (*time-sharing*) (ROCHA; VIEIRA; SANTOS JR., 2010).

Usando modulação e codificação adaptativa (AMC - *Adaptive Modulation and Coding*, Codificação e modulação adaptativa), o número máximo de *bits* por símbolo (por Hz) denominado por $c_{m,n}(t)$, com subportadora m e usuário n , que pode ser transmitido por unidade de tempo t , pode ser expresso como uma função da SNR (*Signal-to-Noise Ratio*,

Relação sinal-ruído) e da taxa de erro de *bit* (BER) requerida. Embora existam algumas aproximações para essa função, por exemplo, a dada em Crovella e Bestavros (1996), todas elas podem ser aproximadas pela expressão de capacidade (QIU; CHAWLA, 1999):

$$c_{m,n}(t) = \left\lceil \log_2 \left(1 + \frac{-1,5}{\ln(5P_{ber})} \gamma_{m,n}(t) \right) \right\rceil \quad (6.1)$$

onde $\gamma_{m,n}(t)$ é a SNR instantânea no intervalo de tempo t para um subcanal m correspondente a um usuário n e P_{ber} é a taxa de erro de *bit* (BER).

6.2 Aplicação de Algoritmos de Policiamento em Redes OFDM/TDMA WIMAX: Simulações e Resultados

O desempenho dos algoritmos de policiamento de tráfego apresentados anteriormente são comparados com o regulador proposto aplicado ao sistema WiMAX simplificado (Figura 6.1).

6.2.1 Comparações entre as perdas de *bytes* dos algoritmos de policiamento de tráfego de rede

Para quantificar o descarte do tráfego pelo algoritmo de policiamento, calcula-se a taxa de pacotes descartados (P_b), que é a relação entre os pacotes perdidos pelo número de pacotes que entraram na rede ou sistema de comunicação (VIEIRA, 2006).

A largura de banda de cada subportadora é de 15 kHz. Assumiu-se um canal de desvanecimento rápido Rayleigh. Para capturar o efeito da frequência de desvanecimento seletivo, o SNR médio para cada subportadora foi selecionado a partir de uma distribuição Gaussiana com média de 15 dB, como empregado em Rocha; Vieira; Santos Jr.(2010). A taxa de erro de *bits* (BER - *Bit Error Rate*) foi definida em 10^{-6} e o nível máximo de modulação 5 (ou seja, $c = 5$).

Foram consideradas 5 entradas (5 usuários), com a mesma série de tráfego de rede para se obter o valor médio de todas as variáveis analisadas (taxas de perda, utilização de *buffer*, *backlog* e retardo). Considerou-se também o mesmo tamanho de *buffer* para todos os usuários. A perda média P_b do sistema é a razão dos *bytes* descartados pela quantidade de *bytes* que entraram no sistema. Após esta estimativa, comparou-se o tamanho do *buffer*

utilizado com a perda (P_b) para cada algoritmo de policiamento.

Quando o processo envelope do tráfego de entrada é maior que o estabelecido pelo algoritmo de policiamento, o tráfego é considerado fora dos padrões exigidos e os pacotes são descartados (castigados) (VIEIRA; LEE, 2009). A fim de quantificar o grau de punição de cada algoritmo de policiamento de tráfego, estima-se a probabilidade (P_b) de um pacote ser descartado para diferentes séries de tráfego de rede com fio e sem fio (VIEIRA; LEE, 2009). Esta estimativa é obtida com a diferença entre a quantidade de *bytes* de saída e a de entrada dividida pela quantidade total de tráfego.

As taxas de perda (P_b) foram obtidas considerando todos os usuários recebendo as séries de tráfego previamente tratadas (pacotes marcados como mal comportados ou descartados) pelo algoritmo de policiamento de tráfego, de modo a se obter uma média da taxa de perda de todas as entradas, conforme ilustrado na Figura 6.2.

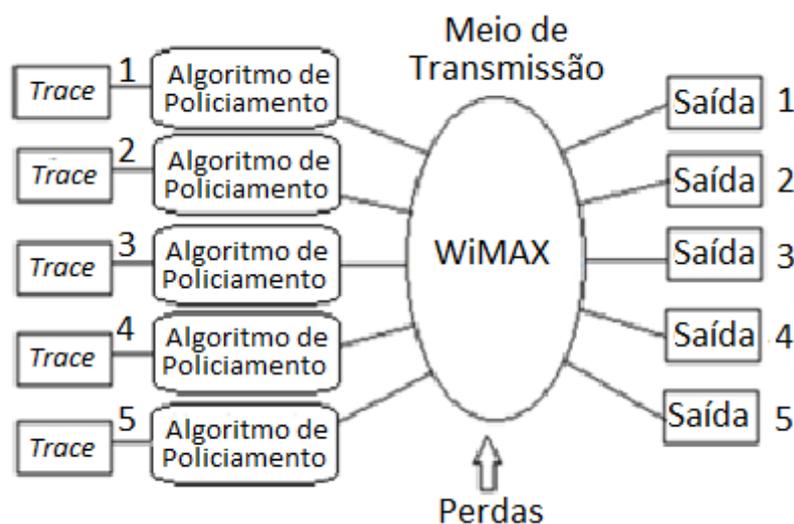


Figura 6.2 - Sistema WiMAX com algoritmo de policiamento

Comparado a outros algoritmos de policiamento, o algoritmo MAPM apresentou algumas características importantes: um processo envelope tão preciso quanto o do tráfego real e uma marcação de pacotes (P_d) menor que as abordagens FLB e GMLB para a série lbl-pkt-5 (Figura 6.3), acima de todos os algoritmos de policiamento para as séries dec-pkt-3 (Figura 6.4), USC_06spring (Figura 6.5) e dec-pkt-2 (Figura 6.6).

Conforme se observa na Figura 6.3, para a série de tráfego lbl-pkt-5, o algoritmo de policiamento MAPM apresentou a menor taxa P_d de *bytes* marcados como sendo de baixa prioridade, comparado a todos os algoritmos de policiamento analisados. Na Figura 6.4, analisou-se a série de tráfego dec-pkt-3, na qual se tem os maiores valores de P_d para os

algoritmos MAPM e os menores valores para o LB.

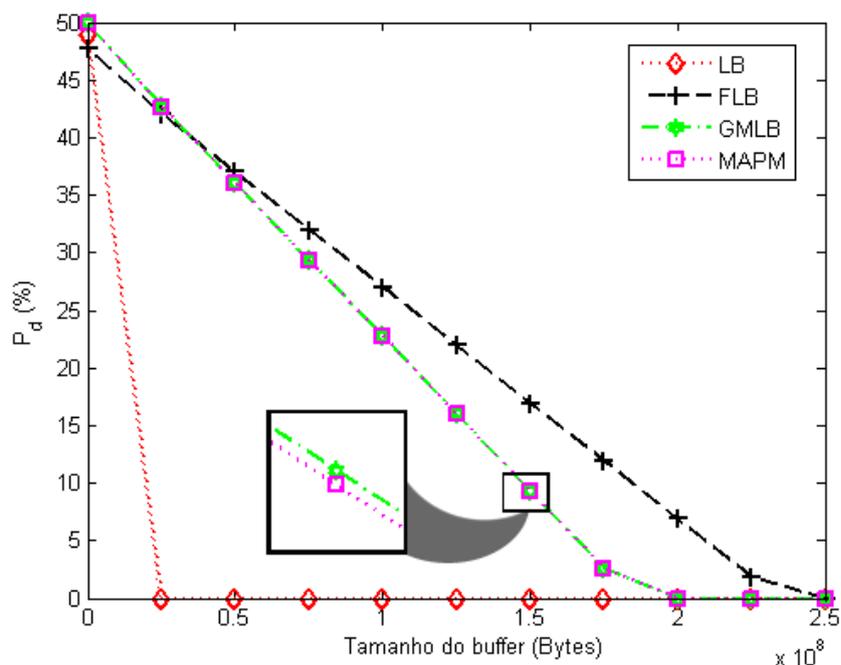


Figura 6.3 - Probabilidade de descarte de pacotes *versus* tamanho do *buffer* para série de tráfego lbl-pkt-5

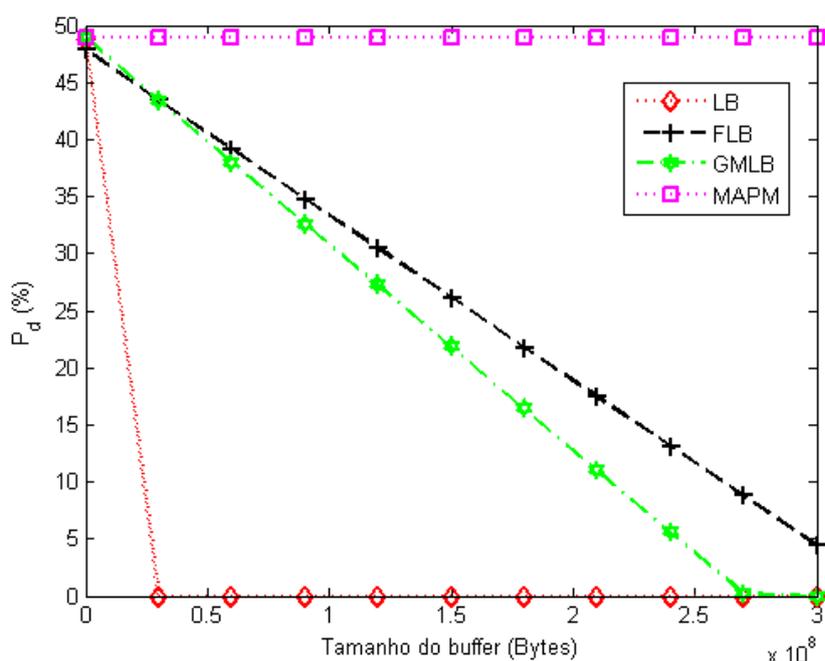


Figura 6.4 - Probabilidade de descarte de pacotes *versus* tamanho do *buffer* para série de tráfego dec-pkt-3

A Figura 6.5 apresenta os valores de P_d para a série de tráfego USC_06spring, onde se observou menores valores de P_d para o algoritmo de policiamento FLB e o maior valor para o algoritmo MAPM. Obteve-se na Figura 6.6 a taxa P_d para a série de tráfego dec-pkt-2, onde é possível se observar que o algoritmo MAPM apresentou segundo menor valor

de P_d , ficando acima somente do algoritmo LB, que apresentou menor P_d após *buffer* maior que $0,5 \times 10^7$ bytes.

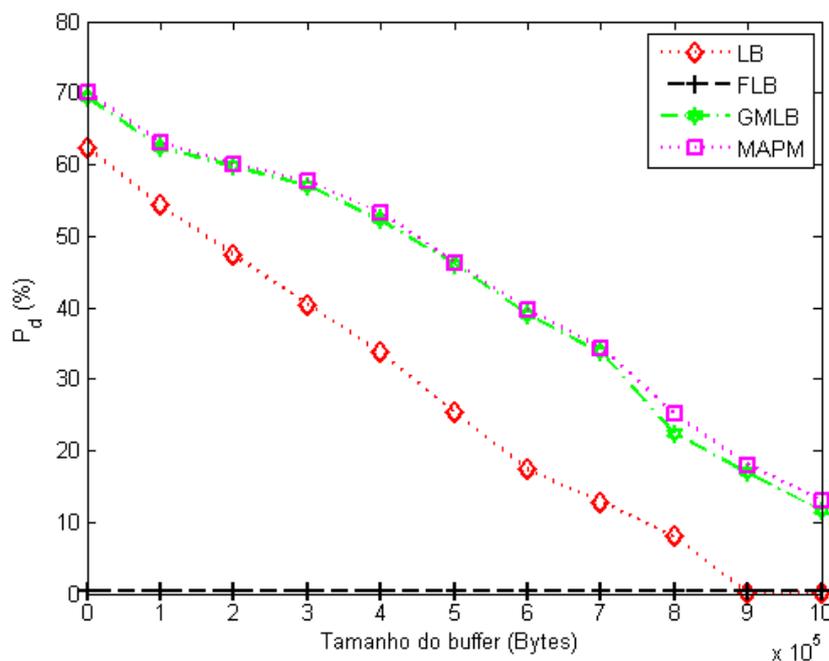


Figura 6.5 - Probabilidade de descarte de pacotes *versus* tamanho do *buffer* para série de tráfego USC_06spring

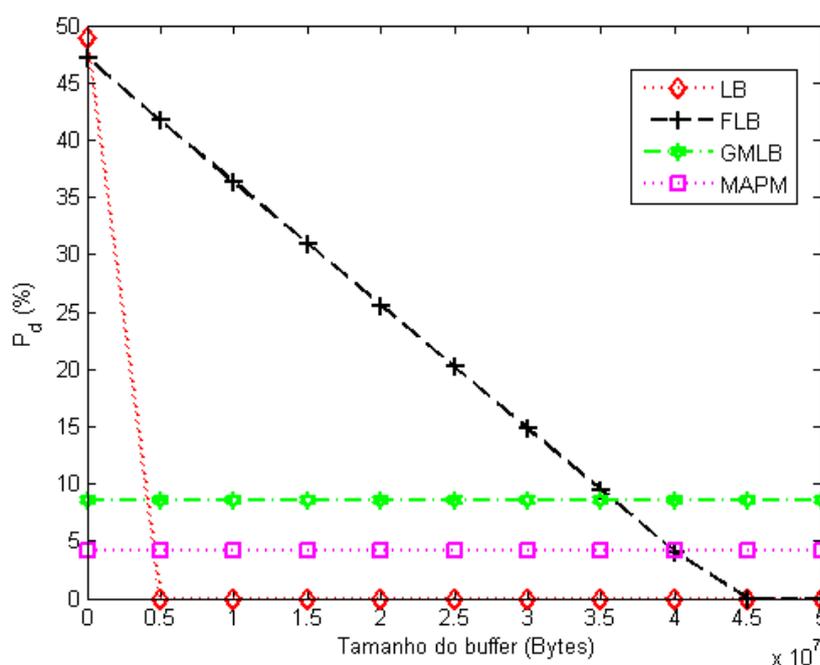


Figura 6.6 - Probabilidade de perda de pacotes *versus* tamanho do *buffer* para série de tráfego dec-pkt-2

O comportamento de P_b em função do tamanho do *buffer* foi apresentado a partir da Figura 6.7 até a Figura 6.10.

Com a Figura 6.7, apresenta-se a série lbl-pkt-5, onde o algoritmo FLB apresentou as menores taxas de perda (P_b), seguido pelo algoritmo LB. Os valores das taxas de perda (P_b) para os algoritmos MAPM e GMLB estão sobrepostos e são os mais próximos do tráfego sem policiamento após o *buffer* ultrapassar o valor de $3,5 \times 10^6$ bytes.

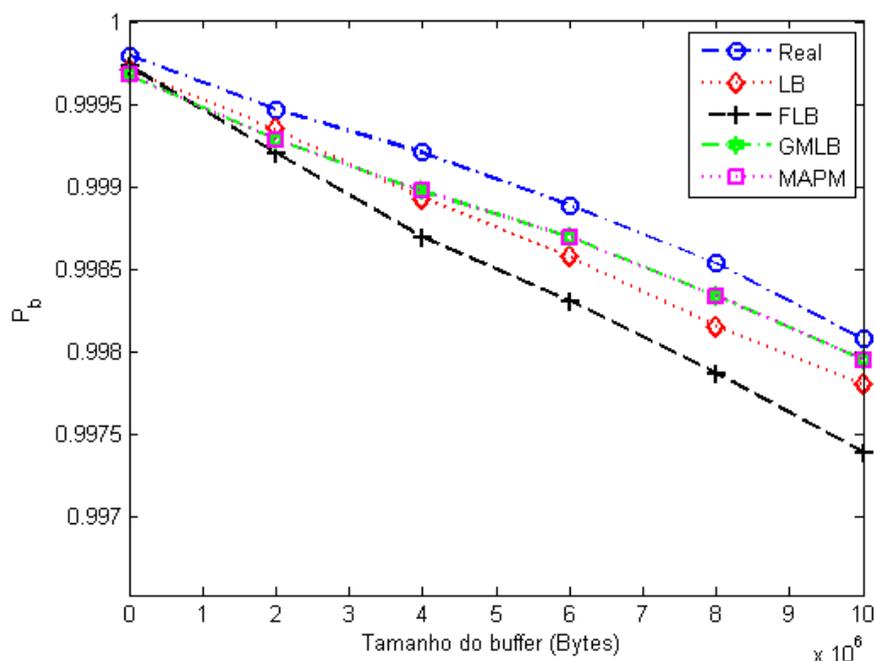


Figura 6.7 - Taxa de perda *versus* capacidade do *buffer* para série de tráfego lbl-pkt-5

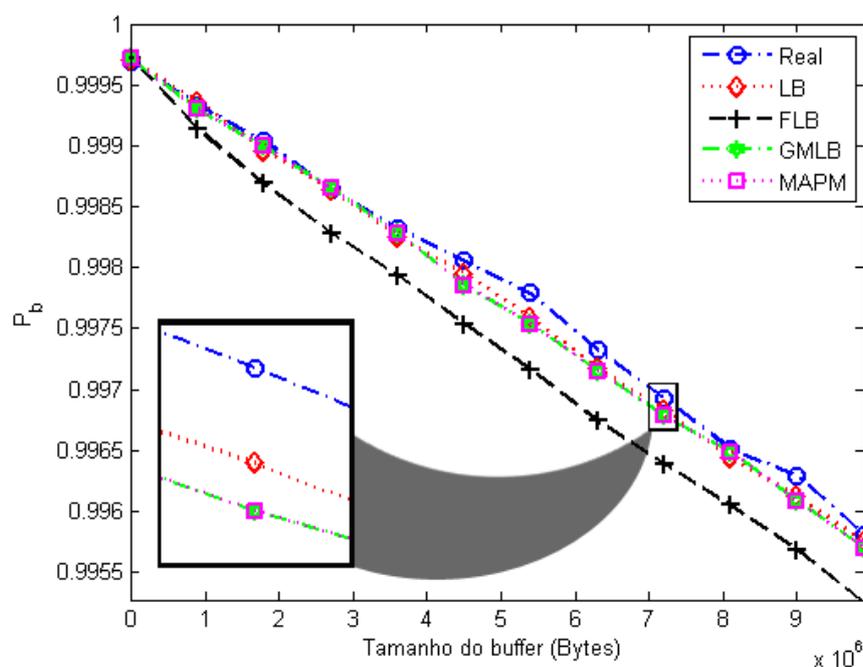


Figura 6.8 - Taxa de perda *versus* capacidade do *buffer* para série de tráfego dec-pkt-3

A taxa de perda P_b obtida pelo algoritmo FLB para a série de tráfego dec-pkt-3 apresentada na Figura 6.8, foi a menor entre todos os algoritmos analisados, seguida dos algoritmos MAPM e GMLB, que ficaram sobrepostos. O algoritmo LB foi o que apresentou taxa de perda mais próxima do tráfego sem policiamento, que por sua vez (o tráfego sem policiamento) apresentou maior taxa de perda.

Para a taxa de perda (P_b) da série USC_06spring, apresentada na Figura 6.9, o algoritmo MAPM apresentou o menor valor de todos os algoritmos de policiamento. O algoritmo de policiamento GMLB apresentou taxa de perda ligeiramente maior que o MAPM. Os algoritmos de policiamento LB e FLB apresentaram taxas iguais (sobrepostas) até o tamanho de *buffer* próximo de 7×10^6 bytes. Para o tamanho do *buffer* superior a 7×10^6 bytes, o LB se mostrou menor que o FLB.

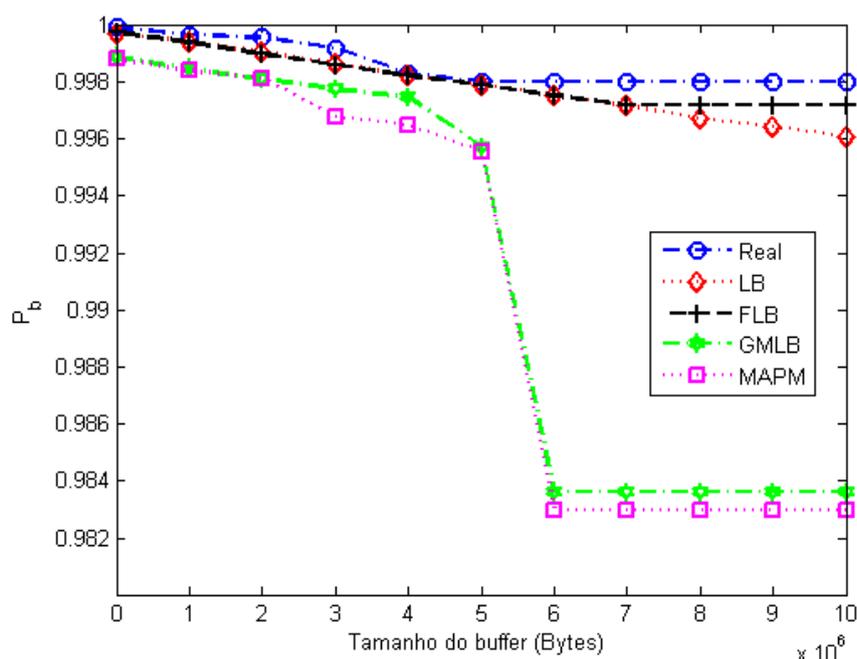


Figura 6.9 - Taxa de perda *versus* capacidade do *buffer* para série de tráfego USC_06spring

Para a série dec-pkt-2 apresentada na Figura 6.10, verificou-se que a taxa de perda do algoritmo LB é a mais próxima da taxa de perda do tráfego sem policiamento, seguida da taxa de perda do MAPM. Observa-se também que o FLB obteve o menor valor de taxa de perda para a série dec-pkt-2.

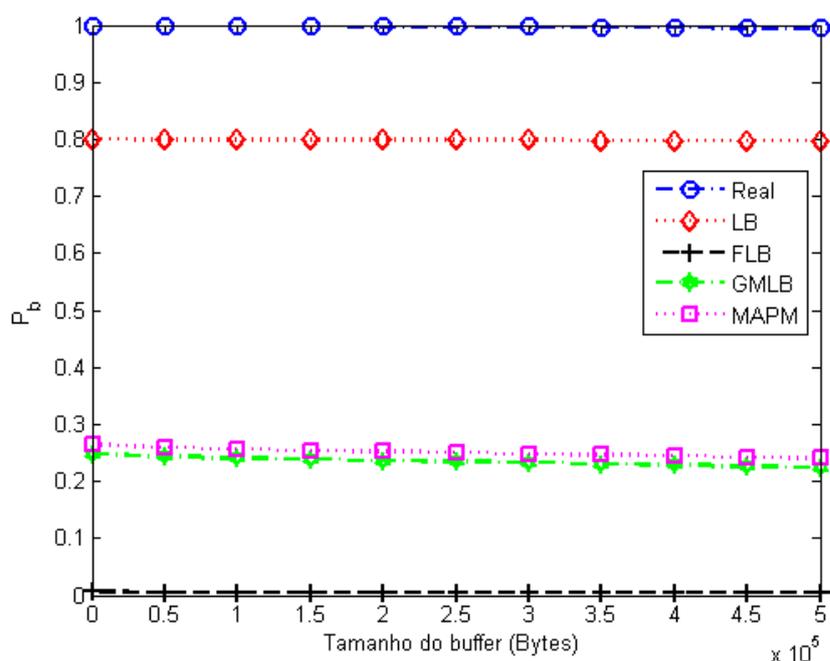


Figura 6.10 - Taxa de perda *versus* capacidade do *buffer* para série de tráfego dec-pkt-2

No geral, observou-se também que o algoritmo LB apresentou menor P_b para as séries lbl-pkt-5, USC_06spring e dec-pkt-3, enquanto que o FLB obteve a menor taxa de perda para a série dec-pkt-2. O MAPM apresentou taxa de perda próxima do tráfego sem policiamento para as séries lbl-pkt-5 e dec-pkt-3.

Avaliou-se também a utilização média do *buffer versus* o tamanho médio do *buffer* para as séries de tráfego lbl-pkt-5 e USC_06spring e apresentadas na Figura 6.11 e Figura 6.12, considerando todos os algoritmos de policiamento analisados.

Para o tráfego lbl-pkt-5 (Figura 6.11), o MAPM e GMLB apresentaram curvas de utilização média do *buffer* sobrepostas e as menores utilizações de *buffer* para o tamanho do *buffer* superior a 8×10^5 bytes. Contudo, observou-se que o valor da série sem policiamento apresentou menor utilização média de *buffer*, para o tamanho de *buffer* inferior a 4×10^5 bytes. Após esse limite do *buffer* (4×10^5 bytes) o menor valor de utilização média alternou entre os algoritmos MAPM e GMLB (que estão sobrepostos) e o tráfego sem policiamento até o tamanho do *buffer* ultrapassar o valor de 8×10^5 bytes, onde as utilizações dos algoritmos MAPM e GMLB se mantiveram menores.

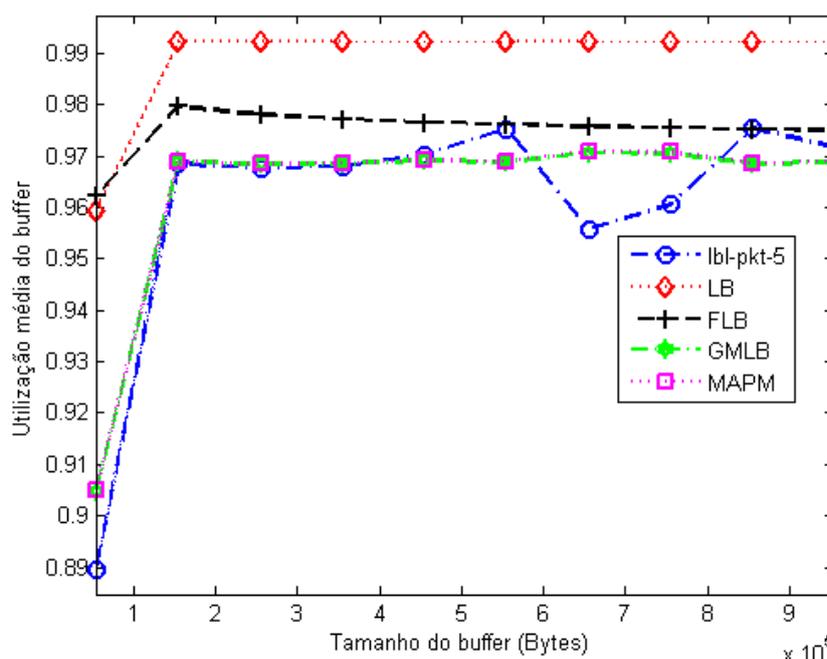


Figura 6.11 - Utilização média do *buffer* versus tamanho do *buffer* para a série de tráfego lbl-pkt-5

Com algoritmo MAPM, obteve-se a menor utilização média de *buffer* de todos os algoritmos de policiamento para a série de tráfego USC_06spring, conforme se observa na Figura 6.12. Para o tamanho do *buffer* menor que 7×10^6 bytes, a utilização média do *buffer* do MAPM foi a menor, superando até mesmo o tráfego sem policiamento.

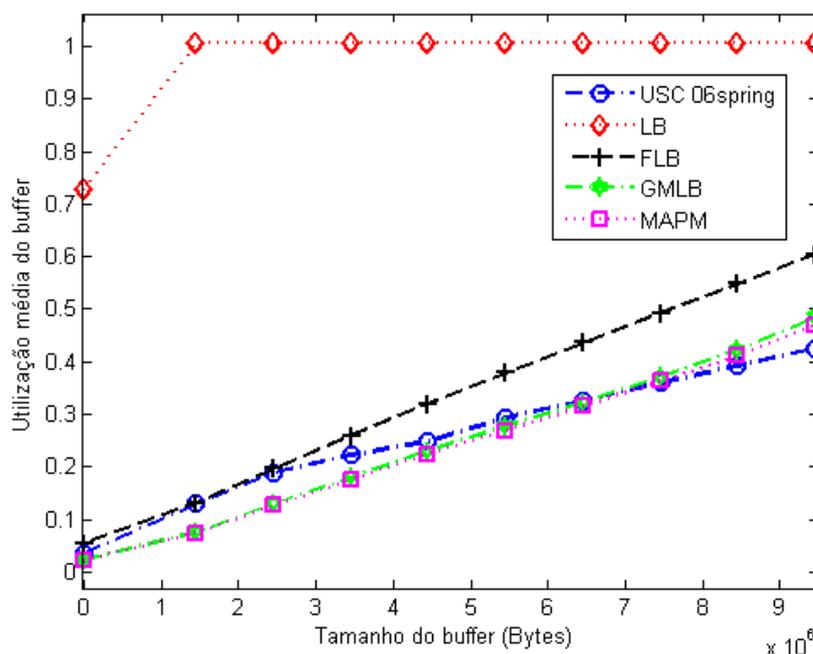


Figura 6.12 - Utilização média do *buffer* versus tamanho do *buffer* para a série de tráfego USC_06spring

Os resultados das simulações enfatizam que um algoritmo de policiamento de

tráfego baseado em um modelo mais adequado pode proporcionar uma melhor qualidade de serviço em geral, mesmo com um descarte menor no tráfego de pacotes, ou seja, através de um algoritmo de policiamento menos severo. Para o tráfego em rajadas, o algoritmo LB não é eficiente conforme apontado em outros trabalhos envolvendo o tráfego multifractal e também verificado por Bregni, Giacomazzi e Saddemi (2007).

A utilização do enlace também foi analisada e apresentada na Figura 6.13 considerando a série de tráfego *lbl-pkt-5* e na Figura 6.14 para a série de tráfego *USC_06spring*.

Observou-se na Figura 6.13, que a medida que o tamanho do *buffer* aumenta, a utilização do enlace para a série *lbl-pkt-5* sem policiamento atinge valores de pico mais altos do que para a série policiada pelos algoritmos. O algoritmo FLB inicialmente apresentou o maior valor de utilização do enlace, porém, quando o tamanho do *buffer* apresentou valor superior a $3,5 \times 10^5$ bytes a utilização do enlace passou a ser menor que a do LB e em seguida (com o tamanho do *buffer* superior a 4×10^5 bytes), tornou-se o menor valor de utilização do enlace para todos os algoritmos de policiamento. No momento em que o tamanho do *buffer* ultrapassou o valor de 8×10^5 bytes, definiu-se o FLB como a menor utilização de enlace.

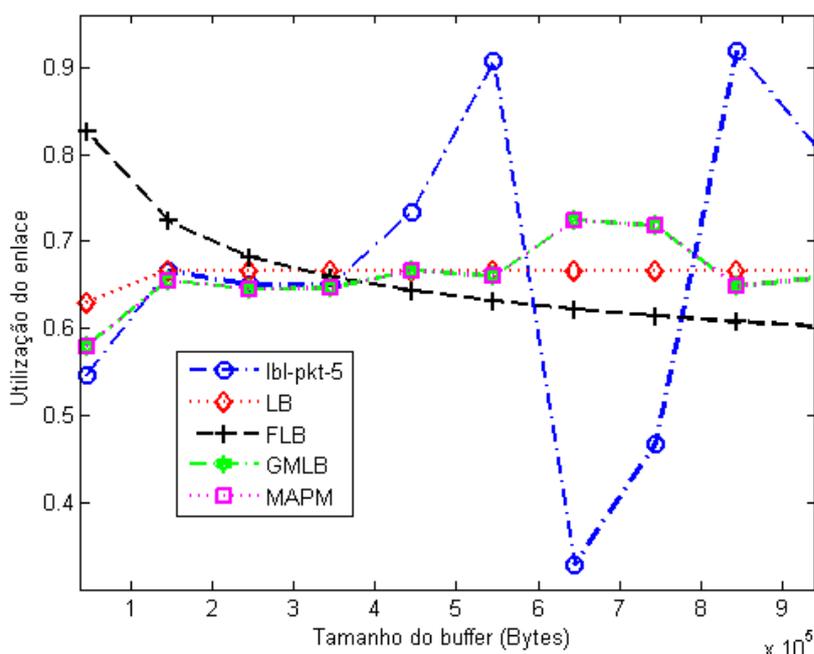


Figura 6.13 – Utilização do enlace para a série de tráfego *lbl-pkt-5*

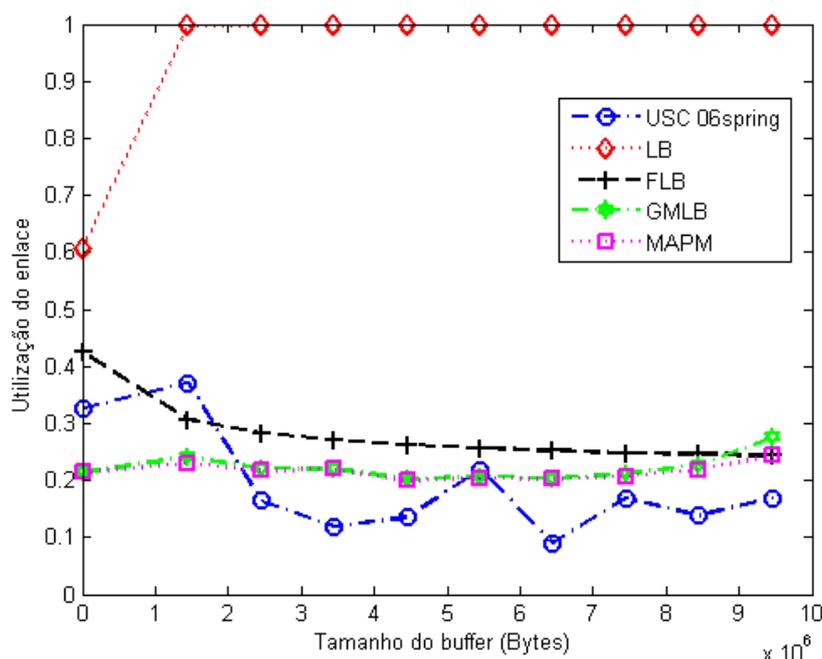


Figura 6.14 – Utilização do enlace para a série de tráfego USC_06spring

Para a série USC_06spring, apresentada na Figura 6.14, observou-se que a série sem policiamento apresentou a menor utilização de enlace para o *buffer* superior a 2×10^6 bytes. Antes desse limite (tamanho do *buffer* superior a 2×10^6 bytes), o algoritmo MAPM apresentou menor utilização de enlace, seguido do GMLB. O algoritmo de policiamento LB fez o tráfego policiado por ele apresentar utilização máxima do enlace após o tamanho do *buffer* ultrapassar o valor próximo a $1,5 \times 10^6$ bytes. Obteve-se com algoritmo MAPM, a menor utilização de enlace de todos os algoritmos de policiamento estudados, ficando acima somente da utilização do enlace para o tráfego não policiado.

6.3 Cálculo de *Backlog* e de Retardo em Rede WiMAX Utilizando Cálculo de Rede

Aplicou-se nesta seção, o Cálculo de Rede (*Network Calculus*) para estimativa dos parâmetros *backlog* (b_{max}) pela equação (5.11) e retardo máximo (d_{max}) pela equação (5.12) para o sistema WiMAX simplificado apresentado na seção 6.1, para as séries de tráfego de rede com fio e sem fio. Para obtenção dos resultados, os fluxos de tráfego foram limitados em 7 (sete) mil amostras (devido ao tempo necessário para as simulações computacionais) e o tempo de cada pacote Δ de 512 ms. As séries de tráfego utilizadas foram a lbl-pkt-5 e dec-pkt-3 para rede com fio e o sem fio os tráfegos USC_06spring e USC_2005summer. O retardo máximo d_{max} para o tráfego Real foi obtido pela seguinte equação:

$$d_{\max} = \frac{Q_{med}}{C} \quad (6.2)$$

onde Q_{med} é a utilização média do *buffer* e C a taxa de transferência, ou seja, capacidade de transmissão de dados.

Nas Figura 6.15 e Figura 6.16 têm-se o limitante para *backlog* (b_{max}) referente ao tráfego dec-pkt-3 e USC_06spring, respectivamente. Observa-se que o limitante para *backlog* do algoritmo de policiamento MAPM está próximo do Real (tráfego sem policiamento). Ampliando-se a Figura 6.15, verifica-se que o limitante para *backlog* do algoritmo MAPM está próximo do limitante para *backlog* do algoritmo LB que ficou entre o Real e o MAPM, porém todos estes três (Real, LB e MAPM) apresentaram valores próximos uns dos outros.

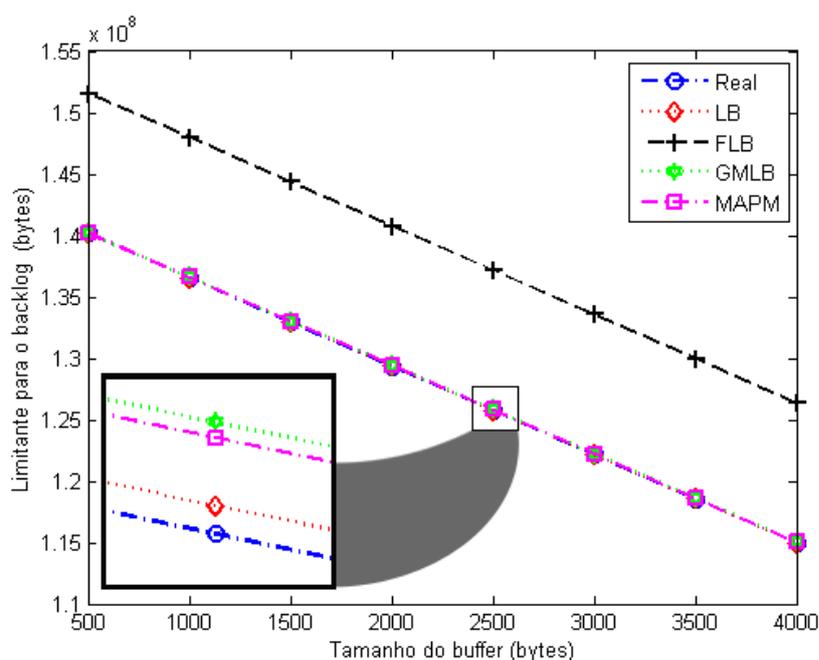


Figura 6.15 - Limitante para *Backlog* para a série de tráfego dec-pkt-3 no sistema WiMAX

Para o tráfego USC_06spring (Figura 6.16), o *backlog* do MAPM se mostrou abaixo do Real. Ao ampliar a Figura 6.16, verifica-se que o limitante para *backlog* do algoritmo MAPM é o mais próximo do Real e o LB apresenta o menor limitante para *backlog*.

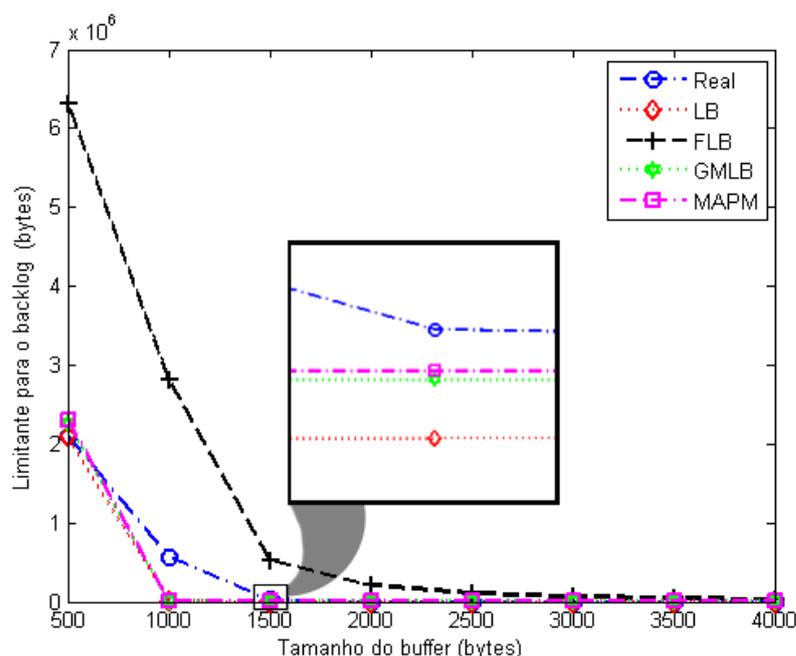


Figura 6.16 - Limitante para *Backlog* para a série de tráfego USC_06spring no sistema WiMAX

Para verificação da diferença do limitante do *backlog* com algoritmo de policiamento para o tráfego Real, utilizou-se novamente o erro quadrático médio (*EQM*). A Tabela 6.1 comprova que os valores obtidos pela Figura 6.15 e Figura 6.16 apresentam valores que quantificam o distanciamento entre os valores de *backlog* obtidos com os algoritmos de policiamento de tráfego e a série de tráfego Real.

Algoritmo de policiamento	Erro quadrático médio (<i>EQM</i>) (<i>bytes</i> ²)			
	lbl-pkt-5	dec-pkt-3	USC_06spring	USC_2005summer
LB	$83,05 \times 10^{10}$	$40,00 \times 10^7$	$40,18 \times 10^9$	$51,53 \times 10^{11}$
FLB	$18,13 \times 10^{13}$	$13,06 \times 10^{13}$	$38,37 \times 10^{11}$	$16,47 \times 10^{15}$
GMLB	$57,03 \times 10^{10}$	$63,70 \times 10^8$	$35,16 \times 10^9$	$42,12 \times 10^{18}$
MAPM	$59,00 \times 10^{10}$	$79,33 \times 10^8$	$35,85 \times 10^9$	$56,22 \times 10^{18}$

Tabela 6.1 - Erro quadrático entre os limitantes para *backlog* dos algoritmos LB, FLB, GMLB, MAPM e Real

Os valores ilustrados na Tabela 6.1 comprovam que o algoritmo LB e GMLB apresentam valores de *EQM* menores que o MAPM para as séries dec-pkt-3 e USC_2005summer, mas para a série lbl-pkt-5, o MAPM apresentou valores de *EQM* menores que os algoritmos LB e FLB.

O limitante para retardo máximo (d_{max}) dos fluxos de entrada do sistema WiMAX simplificado também foi analisado de acordo com cada fluxo de tráfego e para os resultados

foram obtidos utilizou-se a equação (5.12) e foi apresentado na Figura 6.17 e Figura 6.18.

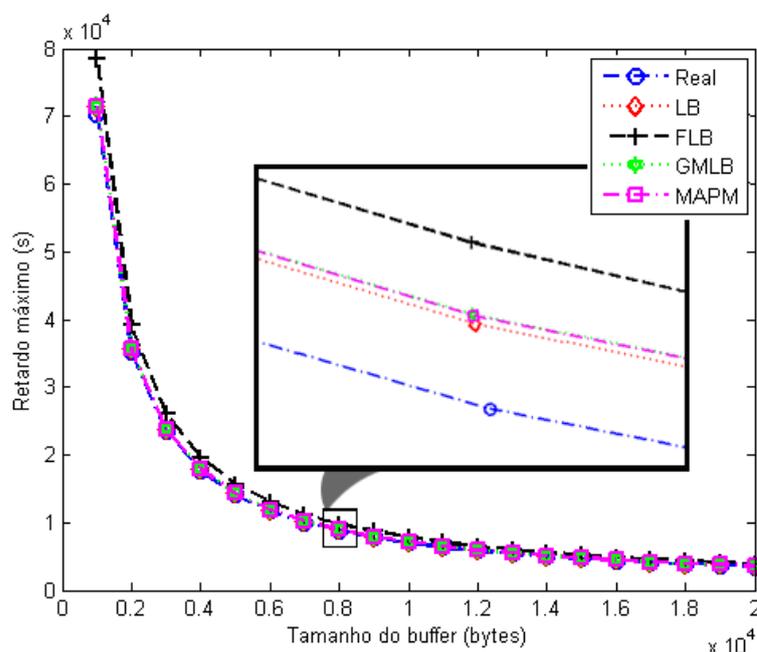


Figura 6.17 - Limitante para retardo para a série de tráfego dec-pkt-3 para um sistema WiMAX simplificado

O limitante para retardo na entrada do sistema para o fluxo dec-pkt-3 (Figura 6.17), mostrou que o MAPM apresenta, para o sistema WiMAX simplificado, valor de retardo máximo menor que as curvas FLB e GMLB. O tráfego sem policiamento apresentou menor valor de retardo máximo comparado a todos os algoritmos de policiamento. Observa-se também que os valores de retardo máximo para MAPM e GMLB foram iguais e por isso apresentaram as curvas sobrepostas.

Para o tráfego USC_06spring, apresentado na Figura 6.18, observou-se que com o tamanho do *buffer* até a metade do valor analisado (≤ 2.000 bytes), o algoritmo MAPM apresentou maior valor de retardo máximo e após esse ponto, o algoritmo FLB apresentou maior valor (de retardo máximo).

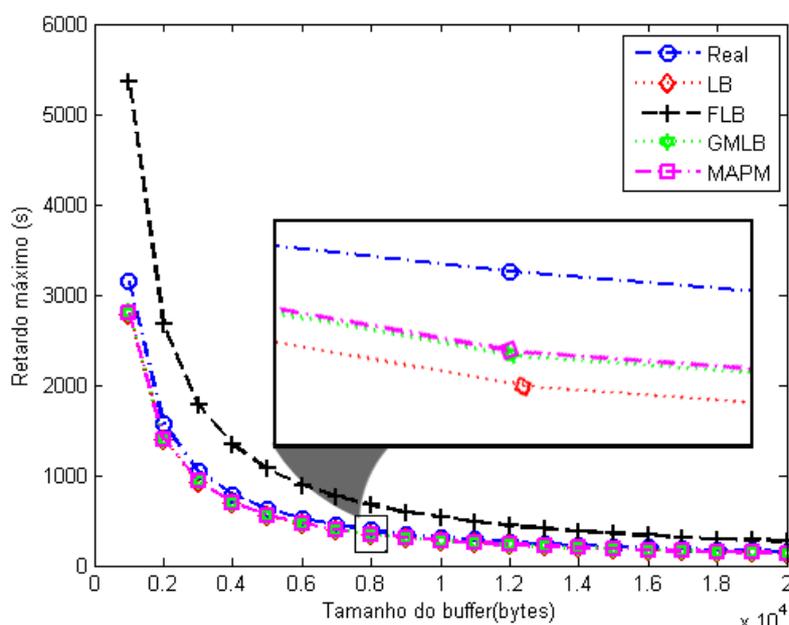


Figura 6.18 - Limitante para retardo para a série de tráfego USC_06spring para um sistema WiMAX simplificado

Também se conferiu o erro quadrático médio (EQM) e apresentou-se os resultados na Tabela 6.2. Verifica-se que o algoritmo de policiamento MAPM se mostrou o método que apresentou menor EQM para a série USC_06spring, se comparado aos outros algoritmos de policiamento estudados e o segundo menor para lbl-pkt-5 e dec-pkt-3, com LB sendo o menor valor.

Algoritmo de policiamento	Erro quadrático médio (EQM) (s^2)			
	lbl-pkt-5	dec-pkt-3	USC_06spring	USC_2005summer
LB	$23,24 \times 10^3$	$10,95 \times 10^4$	$11,35 \times 10^3$	$73,40 \times 10^3$
FLB	$96,31 \times 10^5$	$53,41 \times 10^5$	$38,75 \times 10^4$	$67,81 \times 10^7$
GMLB	$55,86 \times 10^3$	$13,38 \times 10^4$	$10,33 \times 10^3$	$95,47 \times 10^7$
MAPM	$52,48 \times 10^3$	$13,17 \times 10^4$	$10,18 \times 10^3$	$12,76 \times 10^8$

Tabela 6.2 - Erro quadrático entre os limitantes para retardo dos algoritmos LB, FLB, GMLB, MAPM e Real

Através da utilização do Cálculo de Rede Determinístico, pode-se observar a eficiência dos algoritmos de policiamento para um sistema WiMAX simplificado para as séries de tráfego analisadas.

O algoritmo MAPM provocou um aumento no *backlog* e retardo para a série de tráfego dec-pkt-3 e proporcionou a segunda menor taxa de perda (P_b) para esta série, cujo valor obtido pelo algoritmo GMLB está sobreposto e onde se obteve o menor valor (de

backlog) para o algoritmo LB. Observa-se também, que o limitante para retardo apresentado pelo algoritmo MAPM para o sistema WiMAX se mostrou o mais próximo do Real para o fluxo sem fio USC_06spring.

6.4 Resumo do Capítulo

Neste capítulo apresentou-se o sistema de transmissão OFDM/TDMA baseado em redes WiMAX. Demonstrou-se os resultados das análises do sistema WiMAX simplificado com a aplicação do algoritmo de policiamento proposto, o MAPM (Mecanismo de Policiamento de Chegada Multifractal). Os principais pontos apresentados neste capítulo foram:

- Pacotes descartados ou marcados como baixa prioridade pelo algoritmo MAPM para um sistema WiMAX simplificado;
- Sistema de transmissão OFDM/TDMA baseado em redes WiMAX;
- *Backlog* e Retardo *versus* o tamanho do *buffer*.

Com os valores obtidos nesta análise, apresentou-se os principais resultados da utilização do algoritmo de policiamento MAPM para sistemas de transmissão OFDM/TDMA como a estimação do tamanho médio de fila (*backlog*) e retardo máximo através do Cálculo de Rede.

CAPÍTULO 7

CONCLUSÕES

As propriedades multifractais do tráfego de redes apresentam grande impacto no desempenho e qualidade de serviço das redes, conforme descreveu Erramilli, Narayan e Willinger (1996). Por isso, algoritmos de policiamento de tráfego de redes mais eficientes podem ser obtidos ao se considerar modelos multifractais, de acordo com Vieira (2006).

Com o estudo das diversas modelagens de tráfego de rede apresentadas neste trabalho, pode-se afirmar que o processo envelope do tráfego real pode ser modelado com precisão, utilizando-se modelos baseados em processos que consideram as características multifractais.

Neste trabalho, foi proposto um novo algoritmo de policiamento de tráfego de rede chamado de Mecanismo de Policiamento de Chegadas Multifractais (MAPM), que faz uso do processo envelope MFBAP para descrever o tráfego acumulado, por apresentar uma curva característica próxima ao processo envelope dos tráfegos reais, conforme comprovado por simulações computacionais.

Comparou-se o desempenho do algoritmo proposto de policiamento de tráfego de rede com o desempenho dos algoritmos de policiamento Balde Furado (LB) e Balde Furado Fractal (FLB). Com o foco na análise multifractal, também se analisou o algoritmo de policiamento Balde Furado Multifractal Gaussiano (GMLB) com o MAPM utilizando séries de tráfego sintéticas e reais. Os resultados obtidos em simulação com enlace simples e *buffer* finito comprovam que o MAPM se mostrou um algoritmo de policiamento eficiente e de custo computacional menor do que o GMLB (sem o cálculo da integral, como acontece no algoritmo GMLB).

O mecanismo de policiamento de fluxos de tráfego deve permitir pacotes na rede somente se o fluxo de dados estiver bem comportado. Consequentemente, a precisão é uma característica de policiamento de tráfego de extrema importância. O FLB foi desenvolvido

para regular fluxos de séries de tráfego monofractais. Porém, algumas das séries analisadas apresentam características multifractais, conforme observado por Rocha, Vieira e Santos Jr. (2011), fazendo com que o GMLB e MAPM fossem mais eficientes que os anteriores para o tráfego real utilizado em termos por exemplo de taxa de perda.

O algoritmo FLB pode não ser eficiente para um tráfego entrante em rajadas porque não leva em consideração alguns dos parâmetros de um tráfego multifractal, como por exemplo, o expoente de Hölder (que determina a regularidade para cada amostra do tráfego). O algoritmo GMLB apresentou processo envelope menor que os algoritmos de policiamento FLB e MAPM, porém o algoritmo MAPM apresentou o processo envelope com maior proximidade do processo envelope obtido com a série de tráfego acumulada real para as séries USC_06spring e lbl-pkt-5.

Se propôs também estimar o limitante para *backlog* e retardo máximos utilizando o Cálculo de Rede, resultados importantes foram obtidos, como os limitantes determinísticos sobre envelope de séries de tráfego (curva de chegada e curva de serviço) e limitantes para retardo e *backlog*. Os resultados computacionais do MAPM mostraram a eficiência do algoritmo de policiamento em relação aos outros métodos de policiamento. Obteve-se como um dos resultados a estimação do limitante para *backlog* das séries de tráfego de rede (com fio) analisadas, onde o MAPM mostrou-se com valores menores que os encontrados para as séries de tráfego lbl-pkt-5 e dec-pkt-3.

Ainda ao se verificar os limitantes de *backlog* e retardo em função do tamanho do *buffer*, observou-se que o MAPM apresentou resultados menores que o tráfego real para a série lbl-pkt-5 e USC_06spring. Observou-se também que o algoritmo LB apresentou *backlog* menor que o Real para a série USC_2005summer, mesmo não sendo capaz de representar com precisão o tráfego real, por não ter um controle eficiente para tráfego em rajada, causando o transbordo do *buffer* e conseqüentemente a perda de pacotes, também observado por Bregni, Giacomazzi e Saddemi (2010). Observa-se como custo da aplicação do MAPM o acréscimo de retardo para todas as séries analisadas.

Por fim, utilizou-se também o Cálculo de Rede para a análise do tráfego em termos de limitante para *backlog* e retardo máximo considerando um sistema de transmissão OFDM / TDMA baseado em WiMAX simplificado. Com os resultados obtidos, verifica-se que o MAPM foi o mecanismo de policiamento de tráfego de rede que descartou o menor número de pacotes P_b para a série de tráfego USC_06spring e apresentou menores valores de limitantes para *backlog* e retardo para a série de tráfego dec-pkt-3.

Observou-se também que com a aplicação do MAPM em redes WiMAX obtiveram-se valores comparáveis ao do GMLB (que leva em conta o tráfego multifractal) em relação à proporção de tráfego marcado como mal comportado (P_d) e à taxa de perda de pacotes (P_b). Porém o custo da aplicação do MAPM é o limitante para *backlog* e retardo máximo apresentarem valores maiores que o GMLB para a série USC_06spring.

Os resultados mostram que a melhor modelagem do processo envelope para um tráfego real acontece, no geral, para o Mecanismo de Policiamento de Chegada Multifractal (MAPM), uma vez que foram obtidos valores de probabilidade de perda (P_b) para este algoritmo bem próximos dos obtidos para as séries sem policiamento, tanto para as séries de tráfego de rede com fio, quanto sem fio. Observa-se também que o MAPM apresenta valores próximos aos do GMLB para todas as análises realizadas, porém de forma computacional simplificada, ou seja, as equações de controle do MAPM são mais simples que as do GMLB. A utilização média do *buffer* e do enlace do MAPM igual ao GMLB para a série lbl-pkt-5 e menores que o GMLB para a série USC_06spring.

Uma das possíveis extensões deste trabalho é o de avaliar em um simulador de rede o algoritmo de policiamento proposto considerando diferentes tipos de redes e cenários. Pretende-se também analisar melhor o impacto das variações dos parâmetros de Hurst e Hölder no desempenho de rede. De forma geral, pode-se concluir que as propostas apresentadas nesta dissertação de estimação de *backlog* e retardo utilizando o Cálculo de Rede e a utilização do algoritmo de policiamento MAPM contribuem para a pesquisa na área de engenharia de tráfego de redes e o desenvolvimento de novas tecnologias de policiamento e qualidade de serviço (QoS).

REFERÊNCIAS

- AGRAWAL, R.; CRUZ, R. L.; OKINO, C. E.; RAJAN, R.; Performance bounds for flow control protocols. *IEEE/ACM Transactions on Networking*, 7(3):310–323, Junho de 1999.
- AHMADI, S., An Overview of Next Generation Mobile WiMAX: Technology and Prospects, em *WiMAX Evolution: Emerging Technologies and Applications* (eds M. D. Katz and F. H. Fitzek), John Wiley & Sons, Ltd, Chichester, UK, 2009.
- ALI, N. A. e HASSANEIN, H. S.; *IEEE 802.16 Standards and Amendments. WiMAX Handbook*, pp. 19 – 34, CRC Press, 2007.
- AMODEI Jr. A., Esquemas de Modulação do IEEE 802.11, seminário UFRJ, 2003. disponível em: http://www.gta.ufrj.br/seminarios/semin2003_1/aurelio acessado em 22/07/2010.
- ANDRADE, M. B. e COLLI, R.; *Redes Ad-Hoc. Comunicações Digitais e Tópicos Relacionados – Vol. I – Agosto de 2003*.
- BACCELLI, F., COHEN, G., OLSDER, G. J., e QUADRAT, J.-P. *Synchronization and Linearity, An Algebra for Discrete Event Systems*. John Wiley and Sons, 1992.
- BARTHOLD, J., HDTV and 802.11n. *Communications Technology, Cable 360: Wireless*. 3 de março de 2008. Último acesso em 18/01/2011 – 23:25, disponível em: http://www.cable360.net/ct/wireless/HDTV-and-802-11n_28458.html
- BATISTA, C. A., *Métodos Emergentes de Física-Estatística Aplicados a Séries Temporais*. Universidade Federal Rural de Pernambuco, fevereiro de 2006.
- BEACHY, J. A. *Introductory Lectures on Rings and Modules*. Cambridge, England: Cambridge University Press, 1999.
- BIANCHI, G. R. Um modelo multifractal aplicado à previsão de tráfego de redes-proposta e avaliação / Gabriel Rocon Bianchi. -- Campinas, SP: [s.n.], 2005.
- BRADEN, R.; CLARK, D.; SHENKER, S., “Integrated services in the internet architecture: an overview”. *IETF Request for Comments: 1633*, 1994.
- BREGNI, S.; GIACOMAZZI, P.; SADDEMI, G.: Properties of the traffic output by a leaky-bucket policer with long-range dependent input traffic. *Proc. IEEE ICC 2007*.
- _____; “Characterization of Long-Range Dependent Traffic Regulated by Leaky-Bucket Policers and Shapers”, *Elsevier Computer Communications*, Vol. 33, No. 6, April 2010, pp. 714-720
- BURNS, A., HARBOUR, M. G., WELLINGS, A. J.; A Round Robin Scheduling Policy for Ada. *Proceedings of the International Conference on Reliable Software Technologies, Ada-Europe*, 2003.
- CAVALCANTE, M. D.; Modelagem e determinação de desempenho de redes de comunicações através da álgebra de díóides – Campinas – SP [s.n.], 2008.
- CHANG, C.S.; *Performance Guarantees in Communication Networks*. Springer-Verlag, New York, 2000.
- CHEN, Y.; QIAO, C.; YU, X.; Optical burst switching: a new area in optical networking research. *IEEE Network*, may/jun., 2004.

- CHEN, Y.; LIN, Y. W.; LEE, C. Y.; A Block Scaling FFT/IFFT Processor for WiMAX Applications. pp. 203-206, 13-15 de novembro de 2006. ASSCC 2006. IEEE Asian. Solid-State Circuits Conference, 2006.
- CLEGG, R. G. A Practical Guide to Measuring the Hurst Parameter, Proceedings of 21st UK Performance Engineering Workshop, School of Computing Science, Technical Report, 2005.
- CROUSE, M. S., BARANIUK, R.G., RIBEIRO, V.J., RIEDI, R.H. –Multiscale queueing analysis of long-range dependent traffic”. IEEE INFOCOM, 2:1026-1035, 2000.
- CROVELLA, M. E.; BESTAVROS, A. Self-similarity in world wide web traffic – evidence and possible causes. Proceedings of ACM Sigmetrics, p.160-169, 1996.
- CRUZ, R. L., Quality of service guarantees in virtual circuit switched networks. IEEE Journal on Selected Areas in Communications, 13(6):1048–1056, August 1995.
- CRUZ, T.; LEITE, T.; BATISTA, P.; VILÃO, R.; SIMÕES, P.; BASTOS, F.; MONTEIRO, E.; –Um IDS cooperativo para redes de acesso de banda larga”. CIBSI09 (Ibero-American Congress on Information Security). Uruguay, novembro de 2009.
- DeBEASI, P.; 802.11n: Enterprise Deployment Considerations. White Paper Network and Telecom Strategies, 16 de maio de 2008.
- DIAS, B. Z. e ALVES JR., N., Evolução do Padrão *Ethernet*, CBPF-NT-002/02 de 13/05/2002. Disponível em: <http://www.rederio.br/downloads/pdf/nt00202.pdf> (último acesso em 14/04/2011 - 11:55h).
- DIAS, R. A., WILLRICH, R., Serviços Diferenciados Baseado na Tecnologia MPLS em Redes Heterogêneas. VII Simpósio Brasileiro de Sistemas Multimídia e Hipermídia, Florianópolis, 2001.
- EMBRATEL. Fato Relevante Embratel Participações S.A.; Rio de Janeiro, 18 de março de 2008. Disponível em <http://www.embratel.com.br/Embratel02/files/dc/05/04/FR%20EBPAR%2018-03-2008.pdf> (último acesso em: 27/08/2011 – 15:22h).
- ENGST, Adam; FLEISHMAN, Glenn. Kit do iniciante em redes sem fio. 2ª Edição. São Paulo: Makron Books, 2005.
- ERICSSON. White Paper: LTE – an introduction. 284 23-3124 Uen Rev B, Junho de 2009.
- ERRAMILI, A.; NARAYAN, O. e WILLINGER, W. Experimental Queueing Analysis with Long-Range Dependent Traffic. IEEE Transactions Networking, v.4, n.2, p.209-222, 1996.
- FELDMANN, A.; GILBERT, A.; WILLINGER, W. Data networks as cascades: Explaining the multifractal nature of Internet WAN traffic, Proceedings of ACM Sigcomm, p.42-55, September 1998.
- FIGUEIREDO, F. L., Fundamentos da tecnologia WIMAX. Ano Desconhecido. 11 f. Artigo Científico - Centro de pesquisa e desenvolvimento em telecomunicações - CPqD, Campinas. Acessado em 24/08/2011. Disponível em: http://www.cpqd.com.br/file.upload/sas1437_tecnologia_wimax_port_v02.pdf.
- GASPARINI, R. T., Redes Sem Fio; tecnologias, padrões e aspectos de segurança. Londrina: UEL / Universidade Estadual de Londrina, 2007.

- GASPARINI, R. T., 2007 apud ENGST, A.; FLEISHMAN, G., Kit do iniciante em redes sem fio. 2ª Edição. São Paulo: Makron Books, 2005.
- GUÉVEL, R. L. e VÉHEL, J. L. Incremental moments and Hölder exponents of multifractional multistable processes. hal-00448190, version 3, maio de 2010. Disponível em <http://hal.archives-ouvertes.fr/hal-00448190/fr/> (último acesso 07/01/2011 - 14:05h).
- HALFORD, K.; HALFORD, S.; WEBSTER, M.; ANDREN, C.; Complementary code keying for RAKE-based indoor wireless communication. Complementary code keying for RAKE-based indoor wireless communication, pp. 427 – 430, vol. 4, Orlando, FL , USA, 1999.
- HOCK, N. C. e HEE, S. B., Queueing Modelling Fundamentals: With Applications in Communication Networks. 2nd ed., 292 páginas, junho de 2008.
- HOYMAN, C.; PÜTTNER, M.; FORKEL, I; “The HIPERMAN standard—a performance analysis,” in Proceedings of the IST Mobile & Communication Summit, pp. 827–831, Aveiro, Portugal, junho de 2003.
- HSU, Wei-jen. “Memo: Generating Association History from the WLAN log (new format) at USC”. Agosto de 2006. Disponível em: http://nile.cise.ufl.edu/MobiLib/USC_trace/Memo_processing_USC06.pdf (último acesso 30/03/2011 - 14:45)
- HUSTON, G. RFC 2990: next steps for the IP QoS architecture. 2000.
- IEEE Standard Association. Disponível em <http://www.ieee.org> (último acesso 07/08/2010 - 16:50h). IEEE Std. 802.11-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Reference number ISO/IEC 8802-11:1999(E), IEEE Std 802.11, 1999 edition, 1999.
- _____. 802.11a, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band, IEEE Std. 802.11a-1999, 1999.
- _____. 802.11b, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.4 GHz Band, IEEE Std. 802.11b-1999, 1999.
- _____. 802.11F, IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11TM Operation, IEEE Std. 802.11F-2003.
- _____. 802.11k, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 1: Radio Resource Measurement of Wireless LANs, IEEE Std 802.11kTM-2008.
- _____. 802.11h, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe, IEEE Std 802.11hTM-2003.
- _____. 802.11n, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 5: Enhancements for Higher Throughput, IEEE Std 802.11nTM-2009.

- _____. 802.11r, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 2: Fast Basic Service Set (BSS) Transition, IEEE Std 802.11r™-2008.
- _____. 802.11y, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 3: 3650–3700 MHz Operation in USA, IEEE Std 802.11y™-2008.
- _____. 802.11w, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 4: Protected Management Frames, IEEE Std 802.11w™-2009.
- IEEE P802.11 - TASK GROUP U - INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. Status of project IEEE 802.11u: interworking with external networks. 2007. Último acesso em 09/01/2011 – 21:26h. Disponível em: <http://grouper.ieee.org/groups/802/11/Reports/tgu_update.htm>.
- IEEE 802.16a Standard and WiMAX Igniting Broadband Wireless Access. White Paper. WiMAX Forum.
- INTEL Corporation. IEEE 802.16* and WiMAX – Broadband Wireless Access for Everyone. White Paper. July 1, 2003. Disponível em http://belajarit.um.ac.id/belajar/artikel/80216_wimax.pdf [último acesso em 03/07/2010 – 15:22h].
- INTEL PRO/Wireless 2011/2011B LAN System. International Roaming - IEEE 802.11d, 01/10/2009. Disponível em http://www.intel.com/support/pt/mt/mt_win.htm (último acesso 30/09/2010 - 20:50h).
- ITA – Traces available in the Internet Traffic Archive. 2008. Último acesso em 08/01/2011 – 13:15h. Disponível em <http://ita.ee.lbl.gov/html/traces.html>.
- ITU-T Recommendation I.371. TRAFFIC CONTROL AND CONGESTION CONTROL IN B-ISDN. Approved under the WTSC Resolution No. 1 27/08/1996.
- JHA, U. S., PRASAD R., OFDM Towards Fixed and Mobile Broadband Wireless Access. Artech House, 2007.
- KARAGIANNIS, T., The Selfis Tool (Versão 0.1b). Copyright © University Of California, Riverside, disponível em <http://alumni.cs.ucr.edu/~tkarag/Selfis/Selfis.html> (último acesso 02/09/2010 - 22:45h).
- KHAN, J. e KHWAJA, A., Building Secure Wireless Networks With 802.11. Wiley, 2003.
- KLEINROCK, L., Queueing systems: theory. v.1. 556 p. New York: J. Wiley, 1975.
- LABIOD, H.; AFIFI, H.; SANTIS, C.; Wi-Fi™, Bluetooth™, Zigbee™ and WiMax™. Springer: Nova York, junho de 2007.
- LADOCICCO, L. E.; WiMAX em foco. Seção Técnica de Projetos e Equipamentos de Rede, SCPROER/TUTORIAL – 03/2007. Universidade de São Paulo, 2007.
- LAUWERIER, H. Fractals: Endlessly Repeated Geometric Figures. Princeton, NJ: Princeton University Press, pp. 72-77, 1991.
- LE BOUDEC, J. Y., Application of network calculus to guaranteed service networks. IEEE/ACM Transactions on Information Theory, 44(3):1087–1097, May 1998.

- LE BOUDEC, J. Y. e THIRAN, P.; Network Calculus: A Theory of Deterministic Queuing Systems for the Internet. Springer Verlag, Lecture Notes in Computer Science, LNCS 2050, 2004.
- LEE, B. G. e CHOI, S., Broadband Wireless Access and Local Networks: Mobile WiMAX and WiFi, Artech House, Norwood, MA, USA, May 31, 2008.
- LEGRAND, P., VÉHEL, J. L., BARRIÈRE, O. e ECHELARD, A. FRACLAB: a Fractal Matlab/Scilab toolbox. Software copyright INRIA - França (1998 - 2009). Disponível em <http://fraclab.saclay.inria.fr> (último acesso em 03/07/2010 – 11:15h).
- LELAND, W. E., TAQQU, M. S., WILLINGER, W. WILSON, D. V.e BELLCORE, B., On the self similar nature of *Ethernet* Traffic (extended version). IEEE/ACM Transactions on Networking, v.2, n.1, p.1-15, Feb. 1994.
- LUTHER, J., Um guia para os padrões sem fio: O Alfabeto 802.11. Padrões Wireless, pp. 22 - 24. 7ed., 22 de abril de 2005, disponível em <http://linuxmagazine.com.br> (último acesso em 09/01/2011 – 16:20h).
- MANDELBROT, B. B.e NESS, J. W. V., Fractional Brownian Motions, Fractional Noises and Applications. SIAM Review, Vol. 10, N. 4, pp. 422 – 437, Outubro de 1968.
- MARQUES DE SÁ, J. P; Introdução à Teoria da Medida. FEUP – DEEC – 2003.
- MARTÍN-SACRISTÁN, D.; MONSERRAT, J. F.; CABREJAS-PEÑUELAS, J.; CALABUIG, D.; GARRIGAS, S.; CARDONA, N.; On the Way towards Fourth-Generation Mobile: 3GPP LTE and LTE-Advanced. EURASIP Journal on Wireless Communications and Networking, v. 2009, pp. 11-21, doi:10.1155/2009/354089, 2009.
- MATA, R. S.; Dimensionamento de Enlaces em Redes com Integração de Serviços – Campinas – SP [s.n.], 2002.
- MATHWORKS, Software Matlab, 2007. Último acesso em 19/01/2011 – disponível em: <http://www.mathworks.com/products/matlab/description1.html>.
- MELO, C. A. V.; FONSECA, N. L. S. An envelope process for multifractal traffic modeling. In: IEEE ICC, 2004. Proceedings... IEEE, 2004.
- MELLO, M.; Métodos de Previsão. Faculdades Ibmecc-RJ. Fev/Maio de 2009. Disponível em: <http://professores.ibmeccrj.br/mmello/metprev23.pdf> (último acesso em 27/08/11 - 9:01)
- MISHURA, Y., Stochastic Calculus for Fractional Brownian Motion and Related Processes, Lecture Notes in Mathematics, Vol. 1929, XVIII, 398 p., Springer, 2008.
- NICOLA, V. F., HAGESTEIJN, G. A. e KIM, B. G., *Fast simulation of the leaky bucket algorithm*. In: Winter Simulation Conference, WSC 1994, Orlando, Flórida, 1994.
- NIYATO, D., HOSSAIN, E., "Queueing Analysis of OFDM/TDMA Systems". IEEE Globecom 2005 Proceedings. 2005.
- OLIVEIRA, L. C. B. e MENDES, E. A., Estudo da teoria do caos e dos fractais, e dos sistemas complexos e suas possíveis aplicações em Matemática. Exacta, São Paulo, v. 4, n. especial, p. 99-101, 25 nov. 2006.
- PAPOULIS, A.; Probability, random variables, and stochastic processes. 3ed., McGraw-Hill (ISBN: 9780073660110), 1991.
- PARK, K. e WILLINGER, W. Self-similar Network Traffic and Performance Evaluation", John Wiley and Sons, New York, 2000.

- PARTRIDGE, C. RFC 1363: A proposed flow specification. 1992.
- PAXSON, V.; FLOYD S. Wide area traffic: The failure of poisson modeling. *IEEE/ACM Transactions on Networking*, v.3, n.3, p.226-244, June 1995.
- PEARSON, B.; Complementary Code Keying Made Simple. Intersil, Application Note May, AN9850.1, 2000.
- PELTIER, R. F. e VÉHEL J. L., Multifractional Brownian motion: definition and preliminary results. N° 2645, Rapport de Recherche, 39 páginas, INRIA - agosto de 1995.
- PEREIRA, F. M., FONSECA, N. L. S., ARANTES, D. S., On the Performance of Generalized Processor Sharing Servers under Long-Range Dependent Traffic. Technical Report – IC-01-11, outubro de 2001.
-
- _____, Fractal Traffic Modeling and Policing Using Envelope Process. Technical Report – IC-06-03, fevereiro de 2006.
- PEREIRA, F. M., Policiamento e escalonamento de tráfego em redes *Ethernet* PON. – Campinas, SP: [s.n.], 2006.
- PRADO, E. Todo Mundo Está Falando VoIP. E Você?, São José dos Campos, dez. 2004. Disponível em: <http://www.teleco.com.br/emdebate/eprado07.asp> Acesso em: 30/09/2010 - 15:30h
- PRAKASA RAO, B. L. S., Statistical Inference for Fractional Diffusion Processes. (Wiley series in probability and statistics), India – setembro de 2010.
- PRASAD, R. e VELEZ, F. J., WiMAX Networks: Techno-Economic Vision and Challenges. 488p. XXVII. 1ed., 2010.
- QIU, X. e CHAWLA, K., “On the performance of adaptive modulation in cellular systems” *IEEE Trans. Commun.*, v. 47, no. 6, pp. 884-895, junho de 1999.
- RAICHURA, 802.16a wireless links the last mile. *Revista NETWORKWORLD*, 03 de novembro de 2003. Último acesso: 11/01/2011 – 01:17h. Disponível em <http://www.networkworld.com/news/tech/2003/1103techupdate.html>.
- RATHGEB, E. Modeling and performance comparison of policing mechanisms for ATM nets. *IEEE Journal on Select Areas on Communications*, v. 9, n. 3, p. 325-334, apr., 1991.
- RIEDI, R. H.; VÉHEL, J. L., TCP Traffic is multifractal: A numerical study. INRIA Research Report, n.3129, 1997.
- RIEDI, R. H., CROUSE, M. S., RIBEIRO, V. J., BARANIUK, R. G., “Multifractal *Wavelet* Model with Application to Network Traffic” *IEEE TRANSACTIONS ON INFORMATION THEORY*, V. 45, No. 3, Abril de 1999.
- RIBEIRO, V. J., RIEDI, R. H., CROUSER, M. S. e BARANIUK, R. G., “Multiscale queueing analysis of long-range dependent traffic”, in *IEEE INFOCOM*, Tel Aviv, Israel, pp. 1026–1035, Março de 2000.
- ROH, W. e YANOVER, V., Introduction to WiMAX Technology. Introduction to WiMAX Technology, em *WiMAX Evolution: Emerging Technologies and Applications* (eds M. D. Katz and F. H. Fitzek), John Wiley & Sons, Ltd, Chichester, UK, 2009.
- ROCHA, F. G. C., VIEIRA, F. H. T., SANTOS Jr, J.A., “A Multifractal Based Approach for Loss Probability Estimation for OFDM/TDMA Based Systems” In: *The 13th*

International Symposium on Wireless Personal Multimedia Communications, Recife-PE / Brasil, 2010.

- SILVA, A. J. S., As Tecnologias de Redes Wireless. RNP V.2 No.5. 15 de maio de 1998. Disponível em: <http://www.rnp.br/newsgen/9805/wireless.html> (último acesso: 09/01/2011 - 11:34h).
- SILVA FILHO, A. C. e LIMA, F. G.; A Função De Autocorrelação e a Escolha do Passo da Reconstrução. IX Encontro de pesquisadores: Comunicações. Uni-FACEF, Franca de 5 a 9 de maio de 2008.
- SILVESTER, J. A. The effectiveness of multi-level policing mechanisms in ATM traffic control. In: IEEE INTERNATIONAL TELECOMMUNICATIONS SYMPOSIUM, Acapulco, 1996.
- SOHRABY, K., SIDI, M. On the performance of bursty modulated sources subject to leaky bucket rate-based access control schemes. IEEE Transactions on Communications, v.42, n. 234, p. 477-487, feb./apr., 1994.
- SOTTINEN, T. e VALKEILA, E. Fractional Brownian motion as a model in finance. University of Helsinki, Department of Mathematics, Preprint 302, 16 p., 2001.
- TAKADA, H. H.; Design of High-Speed Networks Considering Monofractal and Multifractal Traffic Models. Tese doutorado ITA/CTA, São José dos Campos, 2007.
- TAKADA, H. H.; ANZALONI, A.; A Multifractal Traffic Policing Mechanism. IEEE COMMUNICATIONS LETTERS, pp. 120-122, vol. 10, n. 2, fevereiro de 2006.
- TANENBAUM, A S. Redes de Computadores. 4.ed. São Paulo: Campus, 2003.
- UNINA - Universita' degli Studi di Napoli -"Federico II" (Italy) (2004). Disponível em: <http://www.grid.unina.it/Traffic/> (último acesso em 08/09/2011 – 22:55h).
- USC - The University of Southern California Wireless LAN Traces (2006). Disponível em : http://nile.cise.ufl.edu/MobiLib/USC_trace/ (último acesso em 08/01/2011 – 15:00h).
- VALE, M. S. C.; COSTA, D. C.; ALVES JR., N.; Internet: Histórico, Evolução e Gestão. CBPF-NT-005/01, 2001.
- VECIANA, G. De, July 1996. Private Communication.
- VIEIRA, F. H. T.; Contribuições ao cálculo de banda e de probabilidade de perda para tráfego multifractal de redes. Tese doutorado - UNICAMP. Campinas, SP: [s.n.], 2006.
- VIEIRA, F. H. T. e GARCEZ, S. G.; Estimação de Probabilidade de Perda de Dados em Redes Através de Modelagem Multifractal de Tráfego e Teoria de Muitas Fontes. pp 13-30, RITA, v. 18, n. 1, 2011.
- VIEIRA, F. H. T. e LING, L.L., MULTIFRACTAL TRAFFIC MODELING USING A MULTIPLICATIVE CASCADE WITH GENERALIZED MULTIPLIER DISTRIBUTIONS. Proceedings of IEEE International Conference on Communications, Istanbul, June 11-15, pp: 509-514, 2006.
- VIEIRA, F. H. T., LING, L. L., Limitantes de Desempenho de Fila para Tráfego Multifractal de Redes. Infocomp, p.100-109, Volume 6, n. 4, 2007.
-
- _____, Modelagem de Tráfego de Redes Utilizando Cascata Multifractal Generalizada, Revista de Informática Teórica e Aplicada, pp 87-104 v.15 n. 2, 2008.

- _____, An admission control approach for multifractal network traffic flows using effective envelopes. *AEU - International Journal of Electronics and Communications*. Agosto de 2009.
- YAGHOUBI, H.; Scalable OFDMA Physical Layer in IEEE 802.16 WirelessMAN. *Intel Technology Journal*, Volume 8, Issue 3, 2004.
- WALKE, B. H., MANGOLD, S. BERLEMANN, L., *Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence*, Hardcover, 402 pages, Wiley 2006.
- Wi-Fi *Alliance*. Disponível em <http://www.wi-fi.org> (último acesso em 7 de julho de 2011 – 12:00h).
- Wi-Fi *Alliance*, Wi-Fi CERTIFIED™ n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks, 2009.
- WIERSEMA, U. F., *Brownian Motion Calculus*. Wiley, John & Sons, Incorporated, dezembro de 2008.
- WILLINGER, W., TAQQU, M. S., LELAND, W. E. e WILSON, D. V. Self-Similarity in High-Speed Packet Traffic: Analysis of Modeling of *Ethernet* Traffic Measurements. *Statistical Science*, 10, n.1, pp. 71 – 86, Dezembro de 1995.
- WiMAX.COM, último acesso em 28/09/2010.
- WiMAX FORUM; Position Paper for WiMAX™ Technology in the 700 MHz Band. Março de 2008.
- ZENG, Q.-A.; AGRAWAL, D. P.; Handoff in Wireless Mobile Networks, in *Handbook of Wireless Networks and Mobile Computing* (ed I. Stojmenović), John Wiley & Sons, Inc., New York, USA, 2002.

APÊNDICE A

Princípios Básicos de Cálculo Min-Plus

Apresenta-se em detalhes os fundamentos do Cálculo de Rede Min-Plus. Um tratamento detalhado da álgebra Min-Plus é fornecido em Baccelli et al. (1992). Muitos dos resultados abaixo também podem ser encontrados em Chang (2000) com o ajuste de tempo discreto.

A.1 Cálculo Min-Plus

Na álgebra convencional, as duas operações mais comuns para elementos do conjunto \mathbb{Z} ou \mathbb{R} é a sua adição e sua multiplicação. Na verdade, o conjunto de números inteiros ou reais dotado com estas duas operações verifica um número de axiomas conhecidos que definem as estruturas algébricas: $(\mathbb{Z}, +, \times)$ é um anel¹¹ comutativo, enquanto que $(\mathbb{R}, +, \times)$ é um campo¹². Aqui se considera outra álgebra, onde as operações são alteradas da seguinte forma: adição se torna o cálculo do mínimo, a multiplicação torna-se adição. Verifica-se que isto define outra estrutura algébrica, mas primeiramente verificar-se-á noções de mínimo e ínfimo.

A.2 Mínimo e Ínfimo

Seja S um subconjunto não vazio de \mathbb{R} . S é o limite inferior se houver um número M tal que $s \geq M$ para todo $s \in S$. Adotou-se chamar de ínfimo de S , e denotada por $\inf S$. Por exemplo, os intervalos fechados e abertos $[a, b]$ e (a, b) tem o mesmo ínfimo, que é a . Agora, se S contém um elemento que é menor do que todos os seus outros elementos, esse elemento é chamado de mínimo de S , e é denotado por $\min S$. Note que o mínimo de um conjunto, nem sempre existe. Por exemplo, (a, b) não tem mínimo desde que $a \notin (a, b)$. Por outro lado, se o mínimo de um conjunto S existe, é idêntico ao seu ínfimo. Por exemplo, $\min [a, b] = \inf [a, b]$

¹¹ Anel – representa uma estrutura algébrica que consiste em um conjunto com duas operações binárias (adição e multiplicação), onde cada operação combina dois elementos para formar um terceiro elemento (BEACHY, 1999).

¹² Campo – representa uma classe de um conjunto que é anel mas é também fechada relativamente à operação de complemento (MARQUES DE SÁ, 2003).

$= a$. É facilmente mostrado que todo subconjunto não vazio finito de \mathbb{R} tem um mínimo. Finalmente, define-se a notação \wedge para denotar ínfimo (ou, quando existe, o mínimo).

Por exemplo, $a \wedge b = \min\{a, b\}$. Se S é vazio, adota-se a convenção que $\inf S = +\infty$. Se f é uma função de S para \mathbb{R} , denota-se por $f(S)$ a sua gama (LE BOUDEC; THIRAN, 2004):

$$f(S) = \{t \text{ desde que } t = f(s) \text{ para algum } s \in S\}$$

Será denotado o ínfimo deste conjunto por notações equivalentes:

$$\inf f(S) = \inf_{s \in S} \{f(s)\} \quad (\text{A.1})$$

Seja S um subconjunto não vazio de \mathbb{R} e f uma função de S para \mathbb{R} . Seja $\{S_n\}_{n \in \mathbb{N}}$ é uma coleção de subconjuntos de S , cuja união é S , então:

$$\inf_{s \in S} \{f(s)\} = \inf_{n \in \mathbb{N}} \{\inf_{s \in S_n} [f(s_n)]\} \quad (\text{A.2})$$

A.3 Álgebra Dióide $(\mathbb{R} \cup \{+\infty\}, \wedge, +)$

A álgebra tradicional está habituada a trabalhar com a estrutura algébrica $(\mathbb{R}, +, \times)$, isto é, com o conjunto dos reais dotado com as duas operações usuais, adição e multiplicação. Estas duas operações possuem um número de propriedades (associatividade, comutatividade, distributividade, etc) que fazem $(\mathbb{R}, +, \times)$ um campo comutativo. Como mencionou-se anteriormente, na álgebra min-plus, a operação de adição torna-se o cálculo do ínfimo (ou do mínimo se existir), ao passo que a de multiplicação se torna a operação clássica de adição. Incluir-se-á no conjunto de elementos o $+\infty$ para as operações realizadas com \min , de modo que a estrutura de interesse seja $(\mathbb{R} \cup \{+\infty\}, \wedge, +)$. A maioria dos axiomas (mas não todos) que definem um campo se aplicam a essa estrutura (CAVALCANTE, 2008).

Facilmente verifica-se que \wedge e $+$ satisfazem as seguintes propriedades (LE BOUDEC; THIRAN, 2004) :

- (Encerramento de \wedge) - Para todos $a, b \in \mathbb{R} \cup \{+\infty\}$, $a \wedge b \in \mathbb{R} \cup \{+\infty\}$.
- (Associatividade da \wedge) - Para todos $a, b, c \in \mathbb{R} \cup \{+\infty\}$, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
- (Existência de um elemento de zero para \wedge) - Há algum $e = +\infty \in \mathbb{R} \cup \{+\infty\}$

tal que para todo $a \in \mathbb{R} \cup \{+\infty\}$, $e \wedge a = a$.

- (Idempotente de \wedge) - Para todos $a \in \mathbb{R} \cup \{+\infty\}$, $a \wedge a = a$.
- (Comutatividade de \wedge) - Para todos $a, b \in \mathbb{R} \cup \{+\infty\}$, $a \wedge b = b \wedge a$.
- (Encerramento de $+$) - Para todos $a, b \in \mathbb{R} \cup \{+\infty\}$, $a + b \in \mathbb{R} \cup \{+\infty\}$.
- (Associatividade de $+$) - Para todos $a, b, c \in \mathbb{R} \cup \{+\infty\}$, $(a + b) + c = a + (b + c)$.
- (O elemento zero para \wedge é absorvido para $+$) - Para todo $a \in \mathbb{R} \cup \{+\infty\}$, $a + e = e = e + a$.
- (Existência de um elemento neutro para $+$) - Existe algum $u = 0 \in \mathbb{R} \cup \{+\infty\}$ tal que para todo $a \in \mathbb{R} \cup \{+\infty\}$, $u + a = a = a + u$.
- (Distributiva de $+$ em relação a \wedge) - Para todos $a, b, c \in \mathbb{R} \cup \{+\infty\}$, $(a \wedge b) + c = (a + c) \wedge (b + c) = c + (a \wedge b)$.

A.4 Convolução Min-Plus

Seja $f(t)$ um valor para a função real, com zero para $t \leq 0$. Se $t \in \mathbb{R}$, a integral desta função na álgebra convencional $(\mathbb{R}, +, \times)$ é (LE BOUDEC; THIRAN, 2004):

$$\int_0^t f(s) ds \quad (\text{A.3})$$

No qual se torna, para a sequência $f(t)$ onde $t \in \mathbb{Z}$,

$$\sum_{s=0}^t f(s) \quad (\text{A.4})$$

Na álgebra Min-Plus $(\mathbb{R} \cup \{+\infty\}, \wedge, +)$, a adição é \wedge e a multiplicação é $+$, uma integral da função f se torna, portanto:

$$\inf_{s \in \mathbb{R} | 0 \leq s \leq t} \{f(s)\} \quad (\text{A.5})$$

No qual se torna, para a sequência $f(t)$ onde $t \in \mathbb{Z}$,

$$\min_{s \in \mathbb{Z} | 0 \leq s \leq t} \{f(s)\} \quad (\text{A.6})$$

Muitas vezes, adota-se uma notação mais curta para as duas expressões anteriores:

$$\inf_{0 \leq s \leq t} \{f(s)\} \quad (\text{A.7})$$

com $s \in \mathbb{Z}$ ou $s \in \mathbb{R}$ dependendo do domínio de f .

Uma operação chave na teoria do sistema linear convencional é a convolução entre duas funções, que é definida como:

$$(f \otimes g)(t) = \int_{-\infty}^{+\infty} f(t-s)g(s)ds \quad (\text{A.8})$$

e torna-se, quando $f(t)$ e $g(t)$ são duas funções que são zero para $t < 0$,

$$(f \otimes g)(t) = \int_0^t f(t-s)g(s)ds \quad (\text{A.9})$$

No Cálculo Min-Plus, a operação de convolução é a extensão natural da definição:

Definição A.1 (Convolução Min-Plus). Sejam f e g duas funções ou sequências de F . A convolução Min-Plus de f e g é a função:

$$(f \otimes g)(t) = \inf_{0 \leq s \leq t} \{f(t-s)g(s)\} \quad (\text{A.10})$$

[se $t < 0, (f \otimes g)(t) = 0$].

Teorema A.1 (LE BOUDEC; THIRAN, 2004) (Propriedades gerais de \otimes). Seja $f, g, h \in F$

- Regra 1 (**Encerramento de \otimes**) - $(f \otimes g) \in F$.
- Regra 2 (**Associatividade de \otimes**) - $(f \otimes g) \otimes h = f \otimes (h \otimes g)$.
- Regra 3 (**O elemento zero para \wedge é absorvido por \otimes**) - O elemento zero para \wedge pertencentes a F é a função de ε , definido como $\varepsilon(t) = +\infty$ para todo $t \geq 0$ e $\varepsilon(t) = 0$ para todos $t < 0$. Tem-se $f \otimes \varepsilon = \varepsilon$.
- Regra 4 (**Existência de um elemento neutro para \otimes**) - O elemento neutro é δ_0 , como $f \otimes \delta_0 = f$.
- Regra 5 (**Comutatividade de \otimes**) - $f \otimes g = g \otimes f$.
- Regra 6 (**Distributiva de \otimes com relação a \wedge**) - $(f \wedge g) \otimes h = (f \otimes h) \wedge (g \otimes h)$.

- Regra 7 (**Adição de uma constante**) - Para qualquer $K \in \mathbb{R}^+$, $(f + K) \otimes g = (f \otimes g) + K$.

Teorema A.2 (Propriedades de \otimes para funções Côncovas/Convexas) (LE BOUDEC; THIRAN, 2004). Seja $f, g \in F$.

- Regra 8 (**Funções passando pela origem**) - Se $f(0) = g(0) = 0$ então $f \otimes g \leq f \wedge g$. Além disso, se f e g são em forma de estrela, então $f \otimes g = f \wedge g$.
- Regra 9 (**Funções convexas**) - Se f e g são convexas, então, $f \otimes g$ é convexa.

Em particular, se f, g são convexas e linear por partes, $f \otimes g$ é obtida colocando um ponto-a-ponto em diferentes conjuntos lineares de f e g , classificado por aumento gradual.

Se f e g são lineares por partes, pode-se construir o conjunto $S = S_1 + S_2$, que é a epígrafe de $f \otimes g$, colocando em um ponto-a-ponto os diferentes conjuntos lineares de f e g , classificados por aumento gradual (VECIANA, 1996).

A.5 Operadores Min-Plus

Observa-se que grande parte da estrutura formal do Cálculo da Rede pode ser escrita em uma álgebra Min-Plus (BACCELLI et al., 1991), com operadores para as funções de convolução e deconvolução. Geralmente, as funções apresentadas não são negativas, não-decrescente e contínua à esquerda, definida em intervalos de tempo $[0, t]$. Assume-se um f para determinada função $f(t) = 0$ se $t \leq 0$.

A convolução $f * g$ de duas funções f e g , é definida como (LE BOUDEC; THIRAN, 2004):

$$f * g(t) = \inf_{\tau \in [0, t]} \{f(t - \tau) + g(\tau)\} \quad (\text{A.11})$$

A deconvolução $f \otimes g$ de duas funções f e g , é definida como:

$$f \otimes g(t) = \sup_{\tau > 0} \{f(t + \tau) - g(\tau)\} \quad (\text{A.12})$$

Para $\tau \geq 0$, a função impulso δ_τ é definida como:

$$\delta_\tau(t) = \begin{cases} \infty, & \text{se } t > \tau \\ 0, & \text{se } t \leq \tau \end{cases} \quad (\text{A.13})$$

Se f é não decrescente, tem-se as fórmulas:

$$\begin{aligned} f(t - \tau) &= f * \delta_\tau(t) \\ f(t + \tau) &= f \otimes \delta_\tau(t) \end{aligned} \quad (\text{A.14})$$