The 7th International Telecommunications Symposium (ITS 2010)

A Traffic Policing Mechanism for Wimax Systems Based on Multifractal Modeling

Josemar A. Santos Jr / Flávio G. C. Rocha
Dep. Electrical and Computer Engineering at
Federal University of Goiás
Goiânia - Goiás, Brazil
josemarjr@gmail.com / flavio.geraldo@gmail.com

Flávio H. T. Vieira
Dep. Electrical and Computer Engineering at
Federal University of Goiás
Goiânia - Goiás, Brazil
flavio@eee.ufg.br

***Abstract*— In this paper, we analyze the queueing performance in terms of loss rate of an OFDM (Orthogonal Frequency-Division Multiplexing)/TDMA(Time Division Multiplexing Access) based Wimax system taking into account the multifractal behavior of the wireless traffic flows. To this end, first, we show evidences of multifractal characteristics on wireless traffic traces. These findings motivated us to propose a traffic policing and control scheme based on a multifractal envelope process in order to maintain the traffic flows well-behaved, i.e., in accordance to the desired parameters. Simulations and comparisons to other methods are carried out to verify the efficiency of the proposed traffic policing.**

Keywords Multifractal Traffic, IEEE 802.16, Policing algorithms, Wireless Traffic

I. INTRODUCTION

Efficient models that provide better understanding of network traffic behavior are very important in the design and optimization of communication networks. Numerous traffic models and analysis techniques have been developed for communication networks [13]. Among them, we can include renewal models, Markov-based models, fluid models, autoregressive models, self-similar models, multifractal models, etc. [8].

Some researches have revealed that multifractal models are adequate in describing different network traffic characteristics [22]. In fact, analyzes have been conducted to various real network traffic types. The examples of such traffic types are video traffic [10], Local Area Network (LAN) traffic [21], Wide Area Network (WAN) traffic [11] and World Wide Web (WWW) application traffic [8].

Wireless communication systems are designed to support a diverse range of services and applications and the policing mechanism became required. The most commonly discussed policing mechanism based on traffic modeling in the literature is the Leaky Bucket (LB). However, the Leaky Bucket does not work well when the traffic input process is bursty, once this kind of traffic quickly fills the bucket/buffer and the resulting overflow forces the algorithm to discard even well-behaved packet [16]. This situation can be observed when the incoming traffic is monofractal and multifractal. A traffic flow is considered well-behaved when its parameters are in accordance to those stipulated in the service level agreement (SLA).

A traffic regulator called Fractal Leaky Bucket (FLB) was introduced in [12] to deal with monofractal traffic. The FLB approach proved to be an efficient mechanism to police monofractal traffic sources. Aiming to develop a more accurate model, we propose a traffic policing algorithm that takes into account the multifractal properties of the network traffic, being more general than the fractal approach and adequate for real wireless network traffic as we will demonstrate.

OFDM based Wireless LAN traffic may exhibit singular properties related to multifractal characteristics on small time scale due to the IEEE 802.11 MAC protocol mechanisms. Fixed broadband access systems, e.g. IEEE 802.16a, may present such singularities as we verify in this work. In this work, we found that most of the considered wireless traffic *traces* presents some multifractal characteristics leading us to argue that multifractal analysis can enhance the wireless traffic analysis and control. Regarding loss rate control, we apply the proposed multifractal traffic policing algorithm to an OFDM/TDMA based Wimax system, comparing its performance to other traffic model based policing approaches.

The paper is organized as follows: In section II, we discuss about traffic policing mechanisms. More specifically, on subsection E, we propose a multifractal traffic model based policing scheme. In section III, we evaluate the application of traffic policing mechanisms to the Wimax system and in section IV we conclude.

II. TRAFFIC POLICING MECHANISMS BASED ON NETWORK TRAFFIC MODELING

The multifractal characteristics encountered in wireless traffic traces motivated us to investigate traffic policing mechanisms that consider such characteristics. A policing algorithm is intended to allow a certain number of packets entering into the network only if the traffic flow connection is well-behaved. Otherwise, incoming packets must be discarded or marked as low priority.

A. Leaky Bucket Traffic Regulator

The traditional Leaky Bucket (LB) can be interpreted as a sequential test to analyze the behavior of an incoming traffic flow. In this test, the packets go through an analysis

of traffic behavior to determine if they are in accordance to the service level agreement (SLA), i.e., if they can be considered well-behaved. In this paper, we follow The Leaky Bucket (LB) algorithm described in [6].

The Leaky Bucket (LB) algorithm is often illustrated using the scheme outlined in fig. 1 and can be seen as a "bucket" with *S* bytes or packets in which incoming packets are stored and then sent to network with constant rate.

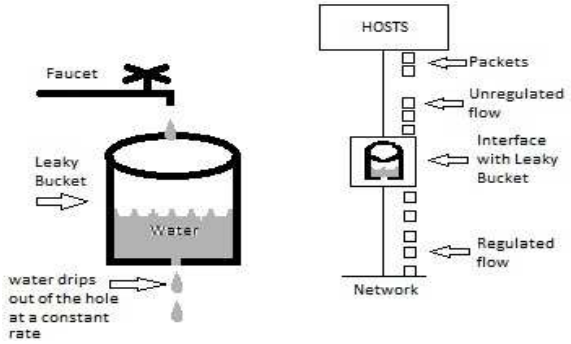

Fig. 1 The Leaky Bucket Algorithm [8].

The LB algorithm is a simple single-server queuing system with constant service time [8]. Apparently, the Leaky Bucket (LB) algorithm directly transfers to its output all traffic with average ρ and maximum capacity *S*, and the maximum accumulated traffic (traffic envelope) is:

$$\hat{L}_{LB}(t) = \rho t + S \tag{01}$$

However, this conclusion is not always valid and well-behaved incoming traffic may present an additional delay and packet loss caused by the algorithm when the packet traffic is bursty.

B. Fractal Leaky Bucket Traffic Regulator

The Fractal Leaky Bucket (FLB) is a policing mechanism that was introduced in [12]. The FLB is based on the concept of fBm modeling (Fractional Brownian Motion) of packet traffic process. It has been verified that the FLB accurately polices monofractal traffic flow with mean ($\bar{a}$), standard deviation (σ) and Hurst parameter (H) [4] of the process X_n.

The packet arrival process is considered a random sequence X_n (n = 1,2,3,…). That is, X_n represents the cumulative number of packets that arrive at buffer's Leaky Bucket (LB) during a time interval Δ.

The FLB algorithm can be described as a sequential test as the LB algorithm and it is described by the following equations:

$$E_n = \max\{0, E_{n-1} + X_n - \bar{a}\Delta\} \tag{02}$$

$$K_n = \begin{cases} S, & E_n = 0 \\ k\sigma\Delta^H\left[n^H - (n-1)^H\right] + K_{n-1} \end{cases} \tag{03}$$

$$J_n = \begin{cases} 0, & E_n \le K_n \\ X_n - \bar{a}\Delta - k\sigma\Delta^H\left[n^H - (n-1)^H\right] \end{cases} \tag{04}$$

The sequence J_n represents the number of packets marked as low priority or discarded. It is straightforward to notice that E_n is a test sequence, K_n is an adaptive decision threshold for E_n and J_n is the control applied to the incoming random sequence X_n. *S* is a constant variable, analogous to the bucket size in the LB algorithm and *k* is the constant related of probability of violation of the envelope process ($\mathcal{E}$) [21].

The maximum amount of work accepted by the FLB algorithm is:

$$\hat{L}_{FLB}(t) = \bar{a}t + \kappa\sigma t^H + S \tag{05}$$

We observed that the FLB envelope process has higher values than the real traffic envelope. This causes the network traffic to be weakly policed, i.e., packets marked as bad-behaved can travel through the network without being dropped. This behavior was also observed in [12].

C. Fractal Gaussian Noise Traffic Regulator

The previous model (FLB) is appropriate when the traffic obeys a normal distribution with zero mean and variance 1. The Fractal Gaussian Noise (fGn) is the first-order increment of the sampled fBm, that can be described by the following equation [2]:

$$G_H(k) = \Delta B_H(k;1) = B_H(k) - B_H(k-1), k \in \mathbf{Z} \tag{06}$$

The main difference between the fGn and FLB policing algorithms is the traffic type that they are able to regulate. The fGn is a stationary self-similar process, whose auto-correlation function decays hyperbolically [2]. On the other hand, fBm may not be stationary.

A drawback of using a fGn traffic regulator is the fact that the fGn model can produce negative values. However, the Gaussian structure of the fGn model can make it more adequate for aggregate traffic due to the Central Limit Theorem. The maximum amount of work accepted by the fGn policing algorithm is [5]:

$$\hat{L}_{fGN}(t) = \bar{a}t + \kappa\sigma t^H + S \tag{07}$$

The parameters $\bar{a}$ and σ represents the mean and the standard deviation of the process Z_n, respectively. Where:

$$Z_n = X_{n+1} - X_n \tag{08}$$

D. Gaussian Multifractal Leaky Bucket Traffic Regulator

The Gaussian Multifractal Leaky Bucket (GMLB) algorithm is based on the mBm (multifractal Brownian motion) envelope process. The GMBL algorithm is defined by the following equations [23]:

$$E_n = \max\{0, E_{n-1} + X_n - \bar{a}\Delta\} \tag{09}$$

$$K_n = \begin{cases} S, & E_n = 0 \\ k\sigma \int_{\Delta(n-1)}^{\Delta n} H(x)x^{H(x)-1}dx + K_{n-1} \end{cases} \tag{10}$$

$$J_n = \begin{cases} 0, & E_n \le K_n \\ X_n - \bar{a}\Delta - k\sigma \int_{\Delta(n-1)}^{\Delta n} H(x)x^{H(x)-1}dx & \end{cases} \quad (11)$$

It is easy to see that K_n, E_n and J_n have the similar functions as in the FLB policing algorithm. However, in these equations, the Hurst parameter is substituted by the Hölder exponent (computed through the method described in [15]) that has a corresponding value for each traffic sample. The insertion of the Hölder exponent is the main difference between the algorithms FLB and GMLB. The maximum work amount accepted by the algorithm GMLB is given by:

$$\hat{L}_{GMLB}(t) = \bar{a}t + \kappa\sigma \int_0^t H(x)x^{H(x)-1}dx + S \quad (12)$$

E. Multifractal Arrival Policing Mechanism Traffic regulator

We argue that network traffic presenting more complex properties (e.g. multifractal characteristics) will not be accurately described by monofractal or simpler models. In this section, we present a more general and sophisticated policing algorithm, namely Multifractal Arrival Policing Mechanism (MAPM) that is based on multifractal modeling.

In order to develop our policing algorithm, we start from the concept known as Multifractal Bounded Arrival Process (MFBAP) [23]. The envelope process MFBAP is able to represent the accumulated traffic of a multifractal process without assuming a particular marginal distribution. The envelope process MFBAP (L_{MFBAP}) is given by the following equations:

$$\hat{L}_{MFBAP}(t) = \bar{a}t + \kappa\sigma\hat{C}(t) \quad (13)$$

$$\hat{C}(t) = t^{H(t)} \quad (14)$$

$$H(t) = H_0 + \sigma_H \exp\left\{-\frac{[\ln(t) - \bar{a}_H]}{2\sigma_H^2}\right\} \quad (15)$$

where $H(t)$ is the Hölder exponent, t the time instant, $\bar{a}$ is the mean value of the input traffic, σ is the standard deviation of the input traffic, k is the constant related of probability of violation of the envelope process (ε) and Δ the time interval [21].

Incorporating the multifractal envelope process into a policing algorithm, we obtain the equations for the proposed MAPM algorithm:

$$E_n = \max\{0, E_{n-1} + X_n - \bar{a}\Delta\} \quad (16)$$

$$K_n = \begin{cases} S, & E_n = 0 \\ k\sigma\Delta^{H(n)}\left[n^{H(n)} - (n-1)^{H(n)}\right] + K_{n-1} & \end{cases} \quad (17)$$

$$J_n = \begin{cases} 0, & E_n \le K_n \\ X_n - \bar{a}\Delta - k\sigma\Delta^{H(n)}\left[n^{H(n)} - (n-1)^{H(n)}\right] & \end{cases} \quad (18)$$

The J_n sequence represents the number of packets marked with low priority or discarded. The parameters K_n and E_n have the same meaning as that of the GMLB algorithm. However, J_n is computed based on the MFBAP envelope.

F. Comparison of Envelope Processes

In this section, we compare the envelope processes obtained from the different policing algorithms described in subsections A until D. Fig. 2 shows the envelope process for the Real traffic input (Real), the Leaky Bucket traffic regulator (LB), the Fractal Leaky Bucket (FLB), the Gaussian Multifractal Leaky Bucket (GMLB), the Fractal Gaussian Noise (fGn) and the proposed Multifractal Arrival Policing Mechanism (MAPM).

The *traces* are collected of USC (University of Southern California) from the raw WLAN log file with users appeared during Jan. 25, 2006 to Apr. 28, 2006 [1].

Note that once the envelope process obtained for the Fractal Gaussian Noise (fGn) is very high, it is straightforward to conclude that the corresponding fGn policing algorithm will allow the passage of all incoming traffic, without discarding packets.

The LB and FLB envelopes are closer to the Real envelope than the fGn envelope. However, they are still not accurate. On the other hand, the GMLB envelope provides a more precise envelope. For this reason, the GMLB has a greater number of packets being dropped or marked as bad-behaved, as we will show.

The MAPM envelope values are located between the Real envelope and the GMLB. Therefore, the input traffic presented less marked or dropped packets then with the GMLB. Notice that the real aggregated traffic is closer to the MAPM envelope process than the others traffic envelopes.

III. TRAFFIC POLICING APPLIED TO THE WIMAX SYSTEM

In this paper, we intend to evaluate the proposed policing approach for an OFDM/TDMA based Wimax system. To

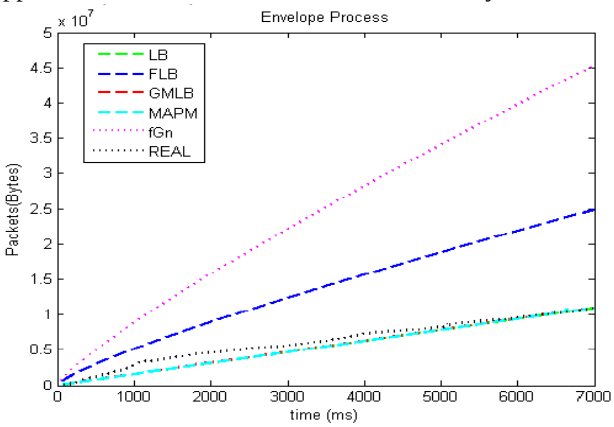

Fig. 2 Envelope Processes (wireless traffic *trace*).

this end, we consider an OFDM transmission scheme similar to the scenario presented in [17], with N users and total M traffic channels (i.e., subcarriers) as represented by fig. 3. The packet arrivals are assumed to be multifractal processes, since we have verified that wireless traffic traces can present those multifractal characteristics.

In the considered Wimax system, data traffic for each user is buffered into a separate queue and the buffer size is finite. We consider a scenario with characteristics of TDMA-based multiple access with round-robin scheduling. The central idea of the round robin algorithm is as follows. A small unit of time, called *quantum*, is defined.

All processes are stored in a circular queue, or in a set of queues as showed in the Fig. 3. The round robin scheduler goes through the queues, allocating the resources to each process for a *quantum*. During all the service time new processes are inserted at the end of the queues, as expected. Due to its characteristics, the round robin system model is extensively used especially for time-sharing systems.

We also assume that the channel state information (i.e., signal-to-noise ratio (SNR) is available at the transmitter system, and the total transmission bandwidth is *B*. Then, each subcarrier has a bandwidth of $\Delta f = B/M$ Hz.

By using adaptive modulation and coding (AMC), the maximum number of bits per symbol (per Hz), denoted by $c_{m,n}(t)$ that subcarrier m for user n can transmit per time unit during time slot t can be expressed as a function of SNR and target bit error rate (BER). Although, there are several approximations for this function (e.g., [9]), all of them are upper bounded by the following capacity expression [20]:

$$C_{m,n}(t) = \left\lfloor \log_2\left(1 + \frac{-1.5}{\ln(5P_{ber})}\gamma_{m,n}(t)\right)\right\rfloor \qquad (19)$$

where $\gamma_{m,n}(t)$ is the instantaneous SNR at time slot t for subcarriers m corresponding to user n and P_{ber} is the target bit error rate (BER).

The transmission power is fixed and the channel undergoes Rayleigh fast fading. The time-invariant average SNR of subcarrier m for user n is denoted by $\gamma_{m,n}$. For a Rayleigh fast fading channel, the received SNR $\gamma_{m,n}$ is a random variable with probability density function (pdf) given as follows:

$$p_\gamma(\gamma_{m,n}) = \frac{1}{\overline{\gamma}_{m,n}} \exp\left(\frac{\gamma_{m,n}}{\overline{\gamma}_{m,n}}\right) \qquad (20)$$

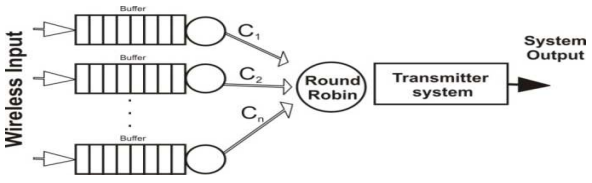

Fig. 3 OFDM/TDMA system model round-robin scheduling.

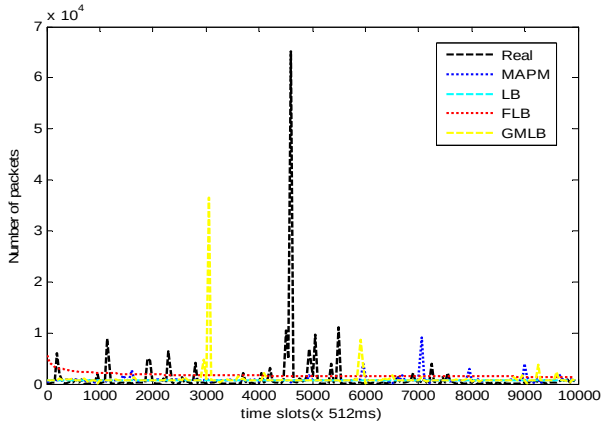

Fig. 4 Buffer occupation

We aim to compare the performance of the MAPM, GMLB and FLB policing algorithms for wireless traffic under the considered Wimax scenario. In the simulations, we considered for each user in the system illustrated by fig. 3, the same *trace* as traffic input to analyze, but with a different traffic policing algorithms for each user. Besides, we set the following parameters to the policing mechanism: Δ was set to 512 ms, S to 10,000 bytes and $\mathcal{E}$ equal to 10^{-4}.

A multifractal process exhibits highly irregular patterns as a function of time and this characteristic degrades the performance of policing mechanisms. There are two characteristics that should be taken into consideration when analyzing policing traffic mechanisms, the number of packets that are well-behaved and are punished (packets dropped or marked as low priority) and the number of packets bad-behaved that are not punished by the algorithm. The FLB performance was superior to that of the LB policing algorithm regarding these two characteristics, as was also pointed out in [12], because FLB allow all well-behaved packets to be transmitted and punish almost all packets bad-behaved of the incoming traffic. The simulation results confirm that the values of the envelope FLB for the packets in the buffer is also higher than those of the LB and those of the multifractal approaches.

Regarding buffer occupation, one can see that the proposed MAPM policing algorithm provides a queuing process almost smooth as that of the LB algorithm. As shown in fig. 4, a comparison to other policing algorithms reveals that MAPM is efficient in controlling the traffic flows.

When the incoming traffic envelope is higher than that established by the policing algorithm, the traffic is considered bad-behaved and is discarded (punished).

To quantify the traffic policing algorithm punishments, we estimate the probability (P_b) of a packet be considered bad-behaved or dropped for real wireless traffic processes [23]. Compared to other policing algorithms, the MAPM algorithm presented some important characteristics: an

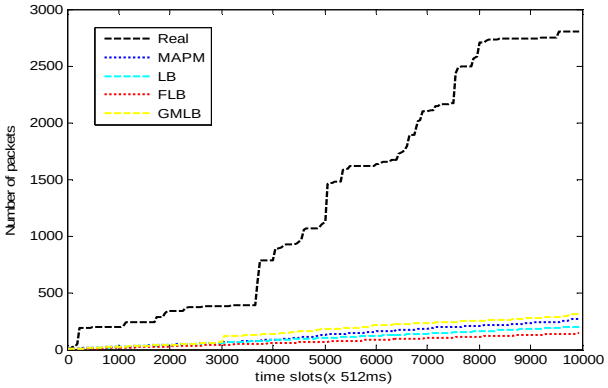

Fig. 5 Aggregated Number of Dropped Packets

envelope process as precise as that of the GMLB but discarding a less number of packets as it can be seen by fig. 5.

In summary, the MAPM tends to mark or drop packets only when the traffic is really bad-behaved, not affecting the traffic that is consistent to the required traffic characteristics (with traffic bursts below an upper limit).

IV. CONCLUSION

The characteristics of traffic flows especially in wireless networks, as long-range dependence and bursts at multiple scales make traffic modeling a difficult and challenging task.

In order to traffic policing mechanisms in wireless networks, we considered a simplified IEEE 802.16 scenario operating with an OFDM/TDMA scheme, where a round robin scheduling controls the data transmission.

In this paper, we propose a more general traffic policing algorithm, namely, the MAPM. For the considered wireless traffic traces, the multifractal GMLB and the proposed MAPM policing algorithms showed to be more efficient than the fractal fGn and FLB. The FLB algorithm presented a better policing performance than the fGn for the considered traffic traces because the traces are not adequately described by the fGn model. Among the policing algorithms, we verified a better performance to the MAPM than those of the GMLB FLB and fGn algorithms. In fact, the MAPM envelopes are closer to the real traffic envelope processes than the other considered envelopes. From our analysis, we conclude that the proposed policing algorithm is able to efficiently police real traffic data.

References:

[1] The USC Wireless LAN Traces. http://nile.cise.ufl.edu/MobiLib/USC_trace/ (last access 2010-02-14).

[2] H. H. Takada. Design of High-Speed Networks Considering Monofractal and Multifractal Traffic Models. São José dos Campos – 2007.

[3] V. A. Aquino e J. A. Barria. “Multiresolution FIR neural-network-based learning algorithm applied to network traffic prediction”. IEEE Transactions on Systems, Man and Cybernetics-C, vol. 36, no.2, pp.208-220, March 2006.

[4] P. Abry, R. Baraniuk, P. Flandrin, R. Riedi, and D. Veitch, “The multiscale nature of network traffic: discovery, analysis and modelling,” IEEE Signal Processing Mag., vol. 19, pp. 28-46, May 2002.

[5] NORROS, I. A storage model with self-similar inputs. Queueing Systems, v.16, p.387- 396, 1994..

[6] A. K. Parekh; R.G. Gallager. A generalized processor sharing approach to flow control in integrated services networks: the single-node case. IEEE/ACM Trans. Networking, v. 1, n. 3, jun., 1993.

[7] M. S. Crouse e R. G.Baraniuk V. J. Ribeiro, R. H. Riedi. “Multiscale queueing analysis of long-range dependent traffic”. Proc. IEEE INFOCOM, vol.2, pp. 1026-1035, March 2000.

[8] Tanenbaum, A. S., Computer Networks. 4th ed. Prentice Hall. New Jersey, 2002.

[9] A. Czylwik, “Adaptive OFDM for wideband radio channels,” in Proc. IEEE GLOBECOM’96, vol. 1, pp. 713-718, Nov. 1996.

[10] H. Fei and W. Zhimei, “Multifractal analysis and model of the MPEG-4 video traffic,” in Performance, Computing, and Communications Conf.,vol. 9–11, Apr. 2003, pp. 463–467.

[11] A. Feldmann, A. C. Gilbert e W. Willinger. “Data networks as cascades: Investigating the multifractal nature of Internet WAN traffic”. pp. 25-38. ACM/SIGCOMM'98, Vancouver, 1998.

[12] N. L. S. Fonseca.; G. S. Mayor; C. A. V. Neto. On the equivalent bandwidth of self-similar sources. ACM Transactions on Modeling and Computer Simulation, v. 10, n. 2, p. 104-124, apr., 2000.

[13] V. S. Frost and B. Melamed. Traffic Modeling for Telecommunications Networks. In IEEE Communications Magazine, March 1994.

[14] S. Haykin, M. Moher. Modern Wireless Communications, 1st ed., Prentice-Hall, 2004.

[15] INRIA, Fractales project <http://fraclab.saclay.inria.fr> (last access 2010-06-18).

[16] J. A. Silvester. The effectiveness of multi-level policing mechanisms in ATM traffic control. In: IEEE INTERNATIONAL TELECOMMUNICATIONS SYMPOSIUM, 1996, Acapulco. Proceedings. Acapulco: IEEE, 1996. p. 98-102.

[17] D. Niyato, E. Hossain. “Queueing Analysis of OFDM/TDMA Systems”. IEEE Globecom 2005 Proceedings. 2005.

[18] Y. C. Ouyang, C.-W. Yang e W. S. Lian. “Neural networks based variable bit rate traffic prediction for traffic control using multiple leaky bucket”. Journal of High Speed Networks. vol. 15, no.2, pp.11-122, 2006.

[19] K.Park e W. Willinger. Self-similar Network Traffic and Performance Evaluation. John Wiley and Sons, New York, 2000.

[20] X. Qiu and K. Chawla, “On the performance of adaptive modulation in cellular systems,” IEEE Trans. Commun., vol. 47, no. 6, pp. 884-895, June 1999.

[21] F. H. T. Vieira, L. L. Lee. An Admission Control Approach for Multifractal Network Traffic Flows Using Effective Envelopes. AEU – International Journal of Electronics and Communications, In Press, Corrected Proof, Availabel online 8 August 2009.

[22] F. H. T. Vieira, L. L. Ling, “Modelagem de Tráfego de Redes Utilizando Cascata Multifractal Generalizada”. RITA, Vol.15, No. 2, 2008.

[23] F. M. Pereira, N. L. S. Fonseca, D. S. Arantes. Fractal Traffic Modeling and Policing using Envelope Process. Technical Report. State University of Campinas, 2006.