Classificação de Fluxos de Tráfego Utilizando Cascatas Multiplicativas

Yulios Zavala, Jeferson Wilian de Godoy Stênico, Lee Luan Ling

***Resumo*—Neste trabalho, propomos um novo método de classificação de tráfego baseado no uso de cascatas multiplicativas para o desenvolvimento de um método de classificação confiável, eficiente e sem análise da carga útil (*payload*) dos pacotes ou dos (*well-known*) números de portas das aplicações. Nós ampliamos o conceito de utilização de aprendizado de máquina junto com estatística de fluxo de pacotes para determinar a classe de tráfego. Os resultados mostram a viabilidade e eficiência do nosso novo método que classifica os tipos de tráfego com precisão acima de 90%.**

Palavras-Chave— Tráfego de Rede, Classificação de Tráfego, Processos Multifractais.

Abstract—In this paper we propose a new method for classification of traffic based on the use of multiplicative cascades for the development of a classification method reliable, efficiently and without analysis of the payload (*payload*) of the packages or the (*well-known*) port numbers of applications. We expanded the concept of using statistical machine learning with the packet flows to determine the class of traffic. Our results show the feasibility and efficiency of our new method achieving detection rates above 90%.

Keywords—Network Traffic, Traffic Classification, Multifractal Processes.

I. INTRODUÇÃO

A classificação do tráfego é uma parte essencial dos sistemas de administração de redes. Os métodos de classificação devem superar cada vez mais novos desafios como uso de portas imprevisíveis e criptografia para disfarçar o tipo de tráfego. O tráfego mundial de dados na internet aumentou rapidamente e deve quadruplicar nos próximos anos [1], impulsionado principalmente pelo maior número de dispositivos (*tablets e smartphones*), o crescimento de usuários, a maior velocidade de banda larga e o incremento de vídeos nas redes. Neste cenário, a correta classificação dos tipos de tráfegos desempenha um papel importante.

As tarefas de gestão de rede, tais como caracterização de carga de trabalho, planejamento de capacidade, provisão de rotas, modelagem e policiamento de tráfego, dependem da identificação e classificação do tráfego de rede [2]. Os métodos de classificação de tráfego são parte essencial dos Sistemas de Detecção de Intrusão. A intercepção legal do tráfego de dados IP tornou-se mais uma obrigação dos ISP, porque assim como as empresas de telefonia devem oferecer suporte para a intercepção da utilização do telefone, os provedores de serviços de internet estão cada vez mais sujeitos aos pedidos do governo para obter informações sobre o uso da rede pelos usuários em determinados pontos no tempo [3]. Para satisfazer esta obrigação as soluções dos ISP têm como parte essencial a classificação de tráfego.

Por causa de sua grande importância, diferentes técnicas têm sido estudadas e utilizadas para classificar o tráfego de redes. Neste trabalho, será proposto um novo método de classificação de fluxos, baseado no uso de cascatas multiplicativas para o desenvolvimento de um classificador de tráfego de internet confiável. Depois de extrair as características de um grupo de fluxos de tráfego com o processo de cascata inversa, utilizam-se, essas características como entradas de um algoritmo de aprendizagem de máquina para assim determinar o desempenho e viabilidade do método proposto. O trabalho está organizado da seguinte forma: Inicialmente na Seção II será feita uma breve revisão de vários trabalhos importantes relacionados com classificação e identificação de tráfego, realizados nos últimos anos, em seguida, na Seção III será introduzido o conceito de cascatas multiplicativas. Na Seção IV apresenta-se a metodologia proposta. A Seção V mostra os resultados dos experimentos e finalmente na Seção VI conclui-se o trabalho.

II. TRABALHOS RELACIONADOS

Existe um número considerável de trabalhos que estudam mecanismos de classificação de tráfegos de redes e internet.

Muitos métodos de classificação de tráfego têm sido propostos para superar os problemas associados com as classificações de porta e tráfego criptografado. Esses incluem a análise de atividade *host* para determinar a possível origem de fluxos ligados ao esse *host* [4][5] ou analisar as diferentes camadas de funcionalidade entre os *hosts* e os fluxos em uma rede [6]. Métodos mais ativos de classificação de tráfego incluem a adição de um *host* isca na rede para determinar mais endereços IP e números de porta que estão executando uma determinada aplicação [7].

Vários estudos existentes na literatura mostram diversas técnicas de classificação de tráfego baseadas em máquinas de aprendizagem (ML – *Machine Learning*). Nguyen et. al. [3] estudaram e compararam a literatura completa no campo da classificação de tráfego baseada em ML. O uso de aprendizado de máquina baseado em estatística tem-se mostrado promissora no processo de classificação de tráfego [3][7]. Moore et. al. [8] propuseram 249 discriminadores de fluxo e de aprendizagem de máquina, usada para selecionar os melhores para classificar novos fluxos.

Embora haja um amplo trabalho relacionado com o campo da classificação de tráfego, a maioria das técnicas baseadas em ML tem relativamente um limitado sucesso na pratica entre os operadores de rede.

Yulios Zavala, Jeferson Wilian de Godoy Stênico e Lee Luan Ling, Departamento de Comunicação da Faculdade Engenharia Elétrica e Computação ,Unicamp, Campinas Brasil E-mails: {yulios,jeferson,lee}@decom.fee.unicamp.br

III. O TRÁFEGO DE REDES COMO CASCATAS

O tráfego nas redes de comunicações é analisado mediante processos probabilísticos que representam o uso que os usuários impõem sobre os recursos da rede. Assim consideram-se variáveis como o tempo entre chegadas dos pacotes, tempo entre conexões, duração das conexões, comprimentos dos pacotes, duração entre sessões. No início, considerava-se, que os tempos entre chegadas eram independentes entre si, assim como a quantidade da demanda. Posteriormente, foi preciso incluir um efeito de correlação existente entre elas, assim começou a utilização de modelos de tráfego Poissonianos onde a correlação cai exponencialmente com o tempo.

Conceitos teóricos importantes para a análise das redes aparecem com Kolmogorov [9] quem introduziu o conceito de auto-similaridade para nomear processos escalonados sem alterações de suas propriedades estatísticas e em 1977 Mandelbrot [10] propõe o termo fractal para descrever objetos muito irregulares. Com esses conceitos é que Leland et. al., [11] pesquisadores de *Bellcore Morristown Research and Engineering Center*, mostraram que o tráfego sobre redes LAN e WAN é estatisticamente auto-similar possuindo comportamento fractal.

A partir do trabalho de Leland et. al., ocorreu uma intensificação nos estudos dos fractais, autores como [12] mostraram características multifractais do tráfego TCP, em [13] se mostrou o comportamento multifractal do tráfego de redes por meio do fenômeno escala e em 2002, Krishina et al. [14] propuseram o modelo VVGM (*Variable Variance Gaussian Multiplier*) baseado em cascata multiplicativa.

A. Cascatas Multiplicativas

Definição 1: Uma cascata multiplicativa é um processo iterativo que fragmenta um determinado conjunto em partes menores de acordo com alguma regra geométrica, e ao mesmo tempo, distribui a massa total do conjunto dado de acordo com outra regra.

A cascata denominada binomial, ou seja, onde a divisão de um determinado conjunto ocorre de dois em dois, é a forma mais simples de se obter um processo multifractal, constituindo de um procedimento iterativo no intervalo fechado $[0,1]$. Sejam m_0 e m_1 denominados multiplicadores da cascata, dois números positivos, cuja soma é 1. No estágio $k = 0$ da cascata, obtêm-se a medida inicial μ_0 do processo com valor aleatório entre o intervalo fechado $[0,1]$. No estágio $k = 1$ a medida μ_1 distribui-se massa, sendo, m_0 no subintervalo $[0,1/2]$ e massa igual a m_1 em $[1/2,1]$. Já para o estágio $k = 2$, o intervalo $[0,1/2]$ é novamente dividido em dois subintervalos $[0,1/4]$ e $[1/4,1/2]$, da mesma forma é repetido o procedimento para o intervalo $[1/2,1]$, obtendo então as seguintes medidas: [10]

$$\mu_2[0,1/4] = m_0 m_0 \quad \mu_2[1/4,1/2] = m_0 m_1$$
$$\mu_2[1/2,/3/4] = m_1 m_0 \quad \mu_2[3/4,1] = m_1 m_1 \qquad (1)$$

Repetindo esse procedimento, pode-se gerar uma sequência de medidas μ_k convergindo para um processo multiplicativo, ou multifractal μ.

A Figura 1 é apresentado o processo de construção de uma cascata conservativa multiplicativa como descrito acima.

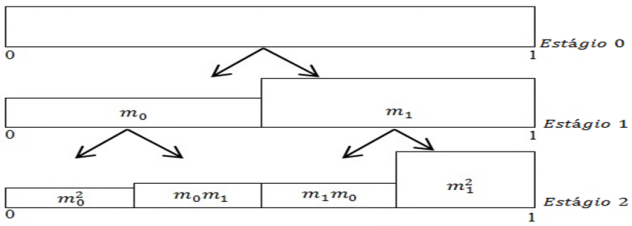


Fig. 1. Processo de Construção da Cascata Multiplicativa.

B. Estimação da Densidade de Probabilidade dos Multiplicadores

Nesta seção, será apresentado o algoritmo para a estimação dos multiplicadores propostos por [13] e uma extensão sugerida com a qual, podem-se obter funções analíticas para as densidades de probabilidade dos multiplicadores.

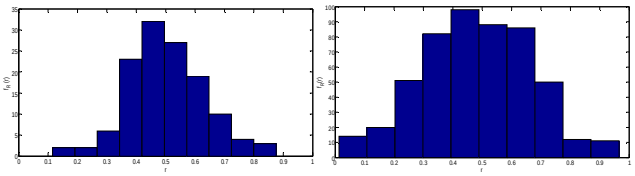
Dessa forma, sejam os dados de tráfego no estágio N da cascata X_i^N, A série de tráfego no estágio $N-1$ da cascata pode ser obtida agregando valores consecutivos do estágio posterior em blocos não sobrepostos de tamanho 2. De forma análoga, dada à série na escala, $(N-j)$, X_i^{N-j}, $(i = 1, \dots, 2^{N-j})$ obtêm-se os dados na escala $(N-j-1)$ pela soma consecutiva dos valores do estágio $(N-j)$ da seguinte forma:

$$X_i^{N-j-1} = X_{2i-1}^{N-j} + X_{2i}^{N-j} \qquad (2)$$

para $i = 1, \dots, 2^{N-j-1}$. Esse procedimento termina quando a agregação dos valores forma apenas um ponto na última escala da cascata. Uma estimativa $r_j^{(i)}$ dos multiplicadores pode ser obtida pela seguinte equação adaptada de [13]:

$$r_j^{(i)} = \frac{X_i^{N-j}}{X_{2i-1}^{N-j-1}} \qquad (3)$$

para $i = 1, \dots, 2^{N-j-1}$. Pode-se considerar $r_j^{(i)}$ como amostras da distribuição de multiplicadores $f_{R_j}(r)$ no estágio j. A distribuição dos multiplicadores na escala j pode ser obtida pelos histogramas de $r_j^{(i)}$. O modelo multiplicador Gaussiano de variância variável (*Variable Variance Gaussian Multiplier,VVGM*) proposto por [14], é uma cascata multiplicativa que aproxima os histogramas obtidos por gaussianas. A distribuição dos multiplicadores $f_{R_j}(r)$ nesse modelo é gaussiana, com média 0.5 e com variâncias que mudam a cada escala. Essas variâncias são estimadas a partir dos histogramas para processos de tempo de chegada de pacote. Na Figura 2 mostra os histogramas para uma série de tráfego HTTP, para os estágios N = 5 e N = 8. Pode-se observar que a distribuição dos multiplicadores é aproximadamente gaussiana.



(a) (b)

Fig. 2. (a) Estágio N = 5, (b) Estágio N = 8

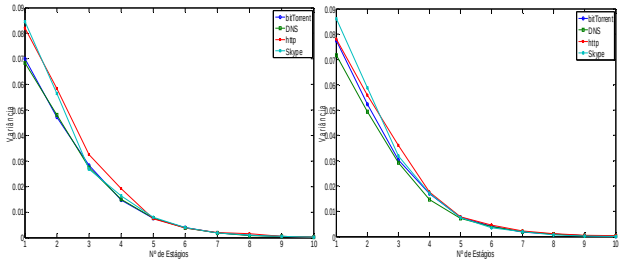
IV. METODOLOGIA

Nessa seção, será apresentada a metodologia proposta para classificação dos fluxos de tráfego de rede baseada em cascatas multiplicativas. Também será descrito o conjunto de dados usados nos experimentos.

A. *Método de Classificação Proposto*

Nesse trabalho, foi utilizado o algoritmo de aprendizado de máquina C4.5 [15] em combinação com um processo de cascata para extração de características de grupo de fluxos. Este processo extrai as características por meio da aplicação do método de estimação de densidade de probabilidade dos multiplicadores como citado na Seção 3.

O objetivo disso está na obtenção dos multiplicadores associados a um grupo de fluxos analisados. Os valores dos multiplicadores de acordo com [14] assume uma distribuição normal com média igual a 0.5, como visto na Figura 2 e as variações dos estágios possuem característica exponencial, o que de fato pode ser comprovado na Figura 3, dessa forma, a quantidade do número de variâncias, será igual à quantidade do número de estágios da cascata. Finalmente os valores obtidos das variâncias são colocados em um vetor que será denotado por "vetor de características".



(a) (b)

Fig. 3. Medida das Variâncias dos Multiplicadores para as Características (a) Tempo de Duração, (b) Quantidade de Bytes.

A Figura 4 é apresentado a fase de treinamento da metodologia proposta, a qual se inicia com a coleta dos traços de tráfego. Depois são extraídos os fluxos de acordo com as informações obtidas a partir dos seus cabeçalhos <protocolo, ip origem, ip destino, porta origem, porta destino >. Dessa forma, é construído o conjunto de dados de treinamento rotulando cada fluxo com o nome da aplicação que o gerou, para isso utiliza-se a ferramenta de *software* livre *L7-filter*. Em seguida, continua-se com os passos do processo de cascatas descrito anteriormente, obtendo as variâncias dos multiplicadores para cada estágio.

Os valores das variâncias extraídas são usados pelo algoritmo C4.5 para criar uma árvore de decisão ou modelo de classificação, utilizando a implementação J48 feita com java do algoritmo C4.5, essa implementação forma parte do *software open source Weka* [16]. Finalmente esse modelo de decisão construído será usado no processo de classificação. O esquema de classificação é mostrado na Figura 5, inicialmente o traço de tráfego a ser classificado é agrupado em fluxos, depois obtêm-se estatísticas das variáveis de tráfego usadas para a análise, com estas estatísticas cria-se o conjunto de dados

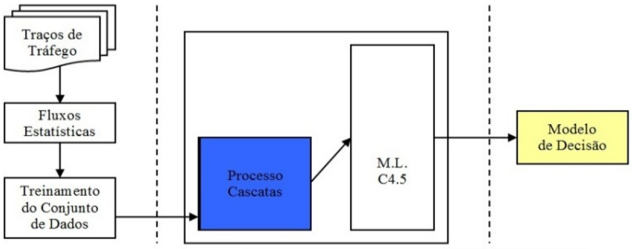


Fig. 4. Fase de Treinamento.

respectivo ao traço inicial. O próximo passo é extrair as variâncias dos multiplicadores do conjunto de dados aplicando o processo de cascatas enunciado no início desta seção. Finalmente obtêm-se a predição da classificação.

O intuito de nossa metodologia é mostrar uma classificação sem análise da carga útil (*payload*) ou dos números de portas *Well-Known*. Nossa metodologia está baseada especificamente na análise com cascatas multiplicativas de três variáveis dos fluxos: número de pacotes, total de bytes e tempo de duração.

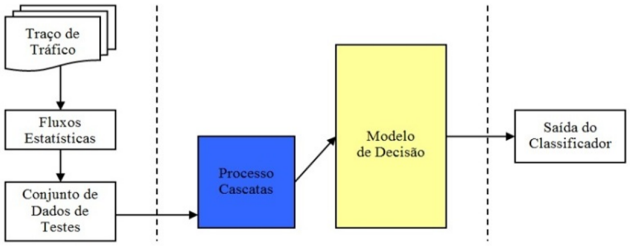


Fig. 5. Esquema de Classificação

B. *Base de Referência (Base-truth)*

Estabelecimento da *Base-truth* ou base de dados de referência é uma fase critica de qualquer método de classificação de tráfego que use *machine learning* – (ML), porque todo o desempenho da classificação depende da precisão na identificação dos fluxos que serão usados como referências [17].

A Tabela I mostra os traços de tráfego que foi utilizado nesse trabalho, traços II e IV do conjunto de dados de avaliação utilizados no trabalho de [17]. Esses traços foram recolhidos no link de acesso Gigabit da Universidade Politécnica da Catalunha (UPC)[18], que conecta cerca de 25 faculdades e 40 departamentos (geograficamente distribuídas em 10 campus) à Internet através da rede espanhola de pesquisa e educação (RedIRIS).

TABELA I. CONJUNTO DE DADOS DE AVALIAÇÃO

Nome Traço	Data	Fluxos Utilizados	Classe	Fluxos x Classe
UPC-II (Treinamento)	11-12-08	1314284	P2P	414829
			DNS	260595
			HTTP	194086
			VoIP	444774
UPC-IV (Teste)	12-12-08	1495302	P2P	380320
			DNS	286337
			HTTP	129994
			VoIP	698651

Nos experimentos, foram analisados 1.314.284 fluxos do traço UPC-II como conjunto de dados de treinamento, esses fluxos analisados são os fluxos das quatro maiores classes existentes no traço, de igual maneira, foram utilizados 1.495.302 fluxos das maiores classes do traço UPC-IV como conjunto de dados de testes. O formato dos traços consiste em um arquivo de texto simples onde cada linha contém diversas informações relacionadas a um fluxo, utilizou-se de apenas três informações as quais são mostradas na Tabela II, assim os conjuntos de dados ficaram com o seguinte formato: <duração, pacotes, *bytes*, rotulo>.

O processo de rotulo dos fluxos foi feito com uma ferramenta baseada no *software* livre [19]. O *software* L7-filter é do tipo DPI (*Deep Packet Inspection*), assim ele procura por padrões característicos no *payload* dos pacotes e os rotula com o aplicativo correspondente.

TABELA II. VARIÁVEIS CARACTERÍSTICAS DOS FLUXOS

Características	Descrição
Duração	Duração do Fluxo em Segundos
Pacotes	Número Total de Pacotes no Fluxo
Bytes	Total de *Bytes* por Fluxo

C. *Métricas de Desempenho*

Caracteriza-se o desempenho do método de classificação proposto, com as seguintes métricas de uso frequente na literatura: Precisão, *Acurácia* e *Recall*, [17][20].

Precisão é o número de verdadeiros positivos TP *(True Positives* ou número de itens corretamente classificados como pertencentes à classe positiva), dividido pelo número total de elementos classificados como pertencentes à classe positiva, ou seja, a soma de verdadeiros positivos TP e falsos positivos FP (*False Positives* ou número de itens incorretamente rotulados como pertencentes à classe positiva). Essa medida é calculada através da seguinte expressão:

$$Precisão = \frac{TP}{TP+FP} \quad (4)$$

Acurácia é o acerto do sistema considerando a proporção de instâncias corretamente classificadas no total dos registos classificados, apresenta a mesma expressão de Precisão, mas com a diferença de que a precisão refere-se a apenas uma classe de fluxo e acurácia refere-se a todas as classes de fluxos.

Recall é definido como o número de verdadeiros positivos TP dividido pelo número total de elementos que realmente pertencem à classe positiva, ou seja, a soma dos verdadeiros positivos TP e falsos negativos FN (*False Negatives* ou número de itens que não foram identificados como pertencentes à classe positiva, mas deveria ter sido). Sua expressão é a seguinte:

$$Recall = \frac{TP}{TP+FN} \quad (7)$$

V. RESULTADOS

Nesta seção serão apresentados os resultados utilizando a metodologia proposta para quatro classes de tráfegos:

1. P2P (*bittorrent*), protocolo para troca de arquivos;
2. DNS sistema usado para resolver os nomes de domínio em endereços de rede;
3. HTTP, protocolo utilizado para a passagem de documentos de hipertexto como paginas web;
4. VoIP (*Skype*) telefonia sobre internet.

Além disso, os resultados obtidos pela proposta apresentada nesse trabalho, forma comparados com o método proposto por [20] que utiliza uma abordagem baseada nas estatísticas dos conteúdos de carga útil (*payload*) e em estatísticas das características dos pacotes, para os seguintes traços de tráfego HTTP e DNS. É importante mencionar que a comparação de taxas HTTP e DNS está grandemente limitada devido ao uso de diferentes conjuntos de dados, a falta de um traço de referência comum é uma dificuldade para as pesquisas nesta área.

Na Tabela III são apresentados os resultados referentes à métrica *Precisão* para os tráfegos analisados. Pode-se observar que a classe de tráfego HTTP apresenta a melhor taxa de 98% quando se utiliza cascatas com 9 estágios. Para o método proposto por [20] está precisão é de 91%. Como se observa na Tabela IV. Já o tráfego do tipo DNS o método proposto apresenta uma taxa de 99%, sendo que o método proposto por [20] obtém uma taxa de 80% (vide Tabela IV).

TABELA III. PRECISÃO DOS RESULTADOS NO CONJUNTO DE DADOS TESTE

Applicação	N=6	N=7	N=8	N=9	N=10
Bittorrent	0.873	0.916	0.929	0.965	0.944
DNS	0.879	0.943	0.977	0.991	0.996
HTTP	0.885	0.948	0.957	0.981	0.913
Skype	0.975	0.989	0.999	0.999	0.999

Na Tabela IV são mostrados os resultados referentes ao nível $N = 9$ de uma cascata, onde formam obtidos os melhores resultados através do método proposto, como se pode observar a metodologia proposta apresenta resultados superiores ao método comparado [20], para os traços de tráfegos HTTP e DNS, sendo uma alternativa eficiente na classificação de tráfego.

TABELA IV. COMPARAÇÃO DE MÉTODOS (*PRECISÃO)*

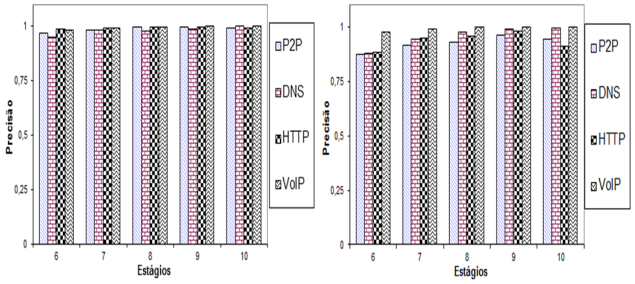
Tráfego/Método	Proposto (N = 9)	Proposto por [20]
HTTP	0.981	0.910
DNS	0.991	0.800

Nas Figuras 6 e 7 mostram as métricas *Precisão* e *Recall* na classificação dos quatro tipos de classes, utilizando 6, 7, 8, 9 e 10 estágios. Observa-se que as taxas de treinamento e teste são todas próximas a 100%, no entanto, a melhor precisão para todas as classes é alcançada com o uso de cascatas com 9 estágios.

A Tabela V mostra os resultados da comparação da classificação para a métrica *Recall*, na fase de testes, em relação ao método proposto em [20]. Mais uma vez, observa-se que o método proposto apresenta melhores resultados.

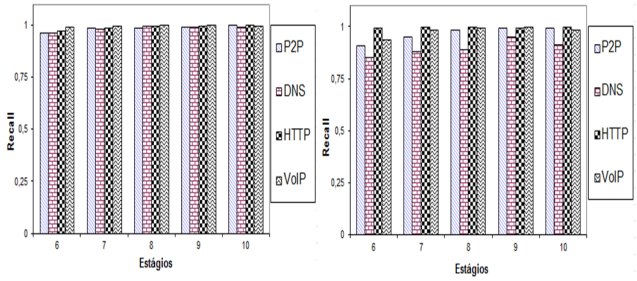
TABELA V. COMPARAÇÃO DE MÉTODOS (RECALL)

Tráfego/Método	Proposto (N = 9)	Proposto por [20]
HTTP	0.996	0.931
DNS	0.950	0.832



(a) (b)

Fig. 6. Precisão: (a) Dados de Treinamento, (b) Dados de Testes.



(a) (b)

Fig. 7. Recall: (a) Dados de Treinamento, (b) Dados de Testes.

Pode-se notar também na Tabela VI, que a metodologia proposta baseada nas variâncias dos multiplicadores dos tráfegos, consegue taxas de *Acurácia* tanto no conjunto de dados de treinamento como no conjunto de dados de testes acima dos valores usando apenas o algoritmo C.45 [15], o que mostra que o método proposto é robusto e eficiente.

TABELA VI. ACURÁCIA TOTAL EM %

Conjuto de Dados	C.45	N=6	N=7	N=8	N=9	N=10
Treinamento	93.7	97.2	98.8	99.2	99.4	99.6
Teste	91.1	92.1	95.8	97.2	98.7	97.5

VI. CONCLUSÕES

Este trabalho mostrou a viabilidade e eficiência de uma nova técnica de classificação baseado nas cascatas multiplicativas. Utilizou-se de um algoritmo de aprendizado de máquina como o C4.5, com este foram realizados vários testes, obtendo taxas de classificação acima de 90%. Ao mesmo tempo, foram comparados os resultados do método proposto com os resultados obtidos por outro método existente na literatura, mostrando a eficiência da metodologia. A técnica mostrou um bom desempenho na tarefa de classificar os registros dos tráfegos estudados, tanto nos experimentos com 6, 7, 8, 9 e 10 estágios. Acreditamos que o desempenho dessa técnica pode ser refinado através da seleção de um número ideal de estágios das cascatas utilizadas para a análise.

REFERÊNCIAS

[1] Cisco.(June 2011). Global Internet Traffic Projected to Quadruple by 2015.Available: http://newsroom.cisco.com/dlls/2011/prod_060111.html

[2] Alshammari, R. and Zincir-Heywood, A. N. A Flow Based Approach for SSH Traffic Detection. In Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference on, 2007, pp. 296-301.

[3] Nguyen,T.T.T. and Armitage,G. A Survey of Techniques for Internet Traffic Classification Using Machine Learning, IEEE Communications Surveys & Tutorials, vol. 10(4), pp. 56-76, 2008.

[4] Karagiannis, T.; Broido, A.; Faloutsos, M. and Claffy, K. Transport Layer Identification of P2P Traffic. In Proceeding IMC'04 ACM SIGCOMM Conference on Internet Measurement (IMC 2004),Italy, October 2004, pp. 121–134.

[5] Constantinou,F. and Mavrommatis, P. Identifying Known and Unknown Peer-To-Peer Traffic. In Proceedings NCA'06 Proceedings of the Fifth IEEE International Symposium on Network Computing and Applications, 2006, pp. 93–102, 2006.

[6] Karagiannis,T.; Papagiannaki, K. and Faloutsos,M. Blinc: Multilevel Traffic Classification in the Dark. proc. 2005 conf. On Applications, Technologies, Architectures, and Protocols for Computer Communications, Philadelphia,Pennsylvania, USA, 22–26 August 2005.

[7] Moore, A.W. and Zuev,D. Internet Traffic Classification Using Bayesian Analysis Techniques.SIGMETRICS Perform. Eval. Rev., vol. 33, pp. 50-60, 2005.

[8] Moore, A.; Zuev, D. and Crogan, M. Discriminators for Use in Flow-Based Classification. technical report, intel research, 2005.

[9] Kolmogorov, A.N. A Refinement of Previous Hypothses Concerning The Local Structure of Turbulence in a Viscous Incompressible Fluid a High Reynolds number, 13, 82–85, 1962.

[10] Mandelbrot, B.B. The Fractal Geometry of Nature. Nova York: W.H.Freeman e Co. 1977.

[11] Leland W., Taqqu M., Willinger W. and Wilson D., On the self-similar nature of Ethernet traffic (extended version), IEEE/ACM Transactions on Networking, v.2, n.1, pp 1-15, Feb 1994.

[12] Riedi,R.H. and Véhel,J.L. Multifractal Properties of TCP Traffic: "A Numerical Study", Technical Report 3129, INRIA Rocquencourt, March 1997.

[13] Feldmann,A. Gilbert,A. Willinger,W. and Kurtz,T.G. The Changing Nature of Network Traffic: Scaling Phenomena. ACM Computer Communication Review, v.28, p.5-29. Group, Tech.1 Rep.Disas-STP-93-30, 1998.

[14] Krishna, P. M. Gadre, V. M. and Desai, U. B. Multifractal based network traffic modeling, Kluwer Academic Publishers, Boston, MA, 2003.

[15] Quinlan,J.R. C4.5: Programs for Machine Learning. Morgan Kaufmann Publishers, 1993.

[16] Weka, http://www.cs.waikato.ac.nz/ml/weka/

[17] Carela-Español,V.; Barlet-Ros, P.;Cabellos-Aparicio, A. and Solé-Pareta, J. Analysis of the Impact of Sampling on NetFlow Traffic Classification, Computer Networks, vol. 55, pp. 1083-1099, 2011.

[18] UPC. Traffic Classification at the Universitat Politècnica de Catalunya (UPC). <http://loadshedding.ccaba.upc.edu/trafic_classification>.

[19] L7-filter. Application Layer Packet Classifier. <http://l7-flter.sourceforge.net/>.

[20] Dehghani, F.; Movahhedinia, N.; Khayyambashi, M.R.; Kianian, S. Real-Time Traffic Classification Based on Statistical and Payload Content Features, Intelligent Systems and Applications (ISA), 2010 2nd International Workshop on , vol., no., pp.1-4, 22-23 May 2010.