Método Multifractal de Classificação de Tráfego

Jeferson Wilian de Godoy Stênico e Lee Luan Ling

***Resumo*—Este trabalho apresenta uma abordagem para a identificação do tráfego. Utilizando de uma nova forma de construção de cascata multiplicativa, fundamentada na expressão do Binômio de Newton, foram obtidos parâmetros dos tráfegos analisados. Em seguida foi aplicado o conceito de aprendizado de máquina com estatística de fluxo de pacotes para determinar a classe do tráfego. Os resultados demonstraram que o método proposto é viável e eficiente para a classificação de tráfego, conseguindo taxas de precisão bastante significativas.**

Palavras-Chave — Modelagem de Tráfego, Cascatas Multiplicativas, Classificação de Tráfego.

***Abstract*—In this paper we present an approach for the traffic identification. Using a novel construction scheme of multiplicative cascade, based on Newton Binomial expression, parameters of the traffics analyzed were obtained. Next we apply the concept of statistical machine learning with the packet flows to determine the traffic class. The results demonstrated that the proposed method is feasible and efficient to classify traffic, obtaining quite significant accuracy rates.**

Keywords— Traffic Modeling, Multiplicative Cascade, Traffic Classification.

I. INTRODUÇÃO

A classificação de tráfego é um mecanismo que ajuda a compreender a natureza do tráfego. Consiste em examinar os fluxos de dados com a finalidade de extrair algumas características específicas, respondendo questões relacionadas com a sua origem, conteúdo ou intenções dos usuários.

As informações fornecidas pela classificação do tráfego são extremamente valiosas, pois podem ser utilizadas para detectar padrões de ataques de negação de serviço ou identificar o mau uso dos recursos de rede, por parte de um usuário que, de alguma forma contraria os termos de serviço do operador [1]. Além disso, as tarefas de gestão de rede, tais como caracterização de carga de trabalho, planejamento de capacidade, provisão de rotas, modelagem e policiamento de tráfego, também dependem da identificação e classificação dos tráfegos de rede [2].

A importância de métodos adequados de classificação de tráfego continua a crescer. No entanto, os métodos tradicionais de classificação estão se tornando menos eficientes, isso porque, novos aplicativos estão utilizando de mecanismos sofisticados de camuflagem e uma grande quantidade de aplicações faz uso de criptografia para evitar verificações de segurança. Além disso, os aplicativos estão se adaptando rapidamente para neutralizar as tentativas de identificação de certos tipos de tráfego, criando dessa forma, novos desafios para os esquemas de classificação de tráfego.

Baseado nessa perspectiva, neste trabalho é proposto um novo método de classificação de tráfego. O mecanismo fundamenta-se em princípios multiplicativos advindo de uma nova forma de construção de cascata multiplicativa. As cascatas multiplicativas são uma mudança de paradigma dos tradicionais modelos baseados em sistemas lineares invariantes no tempo. A relativa simplicidade das cascatas e a flexibilidade que ela fornece a torna uma ferramenta atraente para modelar fenômenos não lineares que apresentam estruturas multiplicativas [3]. A cascata multiplicativa utilizada neste artigo é obtida através de expansões da expressão do Binômio de Newton, segundo o trabalho [4]. Após a extração de parâmetros de um grupo de fluxo de tráfego com o processo de cascata multiplicativa, utilizam-se esses parâmetros como entradas em um algoritmo de aprendizagem de máquina. Dessa forma, é determinado o desempenho e a viabilidade do método proposto.

O trabalho está organizado da seguinte forma: Na Seção II é descrito de forma resumida o novo processo de construção baseado na expressão do Binômio de Newton. Além disso, também será ilustrado como é obtido o processo inverso de uma cascata em relação a séries de tráfegos reais. A Seção III descreve a proposta para a classificação do tráfego. Na Seção IV são descritas as métricas que serão usadas para a validação da proposta. A Seção V é dedicada aos testes experimentais. Finalmente na Seção VI as conclusões são apresentadas.

II. NOVA PROPOSTA DE CONSTRUÇÃO DE CASCATA MULTIPLICATIVA

O processo de construção da cascata ocorre da seguinte forma: Inicialmente considera-se I para denotar o intervalo unitário $[0,1]$. Seja x uma variável aleatória real com distribuição uniforme no intervalo $[0,1]$. No $N-$ésimo estágio o intervalo I é dividido em b^N subintervalo, cada um assegurando uma medida proporcional a uma quantidade numérica, determinada pela seguinte expressão do Binômio de Newton:

$$\binom{b^N}{k}(x)^{b^N-k}(1-x)^k \quad (1)$$

Em outras palavras, no estágio N, aplica-se o fator de ponderação a seguir para o primeiro subintervalo:

$$W_{\underbrace{00\ldots0}_{N\ dígitos}} = (x)^{b^N}+(1-x)^{b^N} \quad (2)$$

Enquanto que para os demais subintervalos os fatores de ponderação são os seguintes:

$$W_{\eta_1\ldots\eta_N} = \binom{b^N}{i}(x)^{b^N-i}(1-x)^i|_{i=1,\ldots,b^N-1} \quad (3)$$

onde $\eta_1 \ldots \eta_N$ são a representação binária do número decimal i.

Denotados por R, os multiplicadores da cascata restritos em $[0,1]$ e com densidade de probabilidade $f_R(x)$, de forma que $E[R] = 1/b$. Com isso, para $t = 0.\eta_1\eta_2 \ldots \eta_k = \sum_{i=1}^{k} \eta_i b^{-i}$, seja $R(\eta_1 \ldots \eta_k) = W_{\eta_1\ldots\eta_k}$, representando o novo multiplicador aleatório incorporado para o subintervalo $[t, t+\Delta t_k]$ no $k-$ésimo estágio da cascata. Desse modo, a medida do intervalo $[t, t+\Delta t_k]$ pode ser expressa como:

$$\mu(\Delta t_k) = \mu[t, t+\Delta t_k] = R(\eta_1)R(\eta_1\eta_2) \ldots R(\eta_1 \ldots \eta_k) \quad (4)$$

Para uma melhor ilustração da nova regra de construção da cascata conservativa, na Figura 1 são apresentados os estágios 0 – 11 da construção de uma cascata multiplicativa

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

considerando $b = 2$, gerando dessa forma uma cascata binomial. Para maiores detalhes sobre esse processo ver [4]. A Figura 1 nos dá a ideia de como se pode aproximar uma cascata conservativa com a forma de operação dos mecanismos de uma rede em pequenas escalas de tempo, como por exemplo, para um tráfego TCP ao longo da duração de uma conexão real.

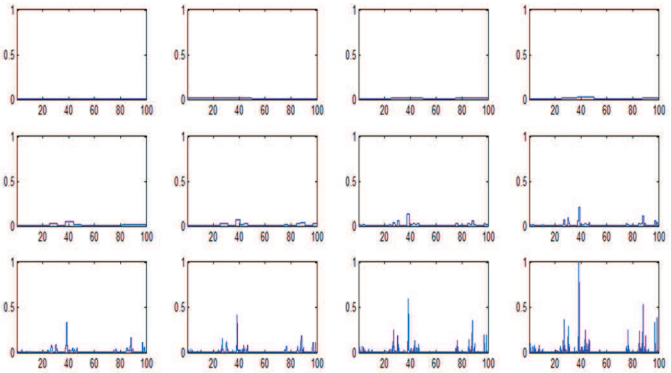

Fig. 1 Estágio 0 -11 da Cascata Conservativa Segundo o Método Proposto

A. Cascata multiplicativa inversa

O principal objetivo da construção da cascata inversa é verificar se os tráfegos de redes satisfazem ou não a regra conservativa na redistribuição de massa de um intervalo inicial para os subintervalos e se assim for, inferir as propriedades estatísticas pertinentes do gerador da cascata conservativa.

Seja X_i^N os dados de tráfego no estágio N obtido através do processo de construção de uma cascata com tempo de resolução de b^{-N}. Os valores das variáveis x_i, para a nova forma de construção de cascata multiplicativa, utilizando a expressão do Binômio de Newton serão estimados da seguinte forma:

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

$$X_i^{N-j-1} = X_{bi-1}^{N-j} + X_{bi}^{N-j} \quad (5)$$

para $i = 1, \ldots, b^{N-j-1}$. Esse procedimento termina quando a agregação dos valores forma apenas um ponto na última escala da cascata. Esse processo é ilustrado na Figura 2, considerando $b = 2$.

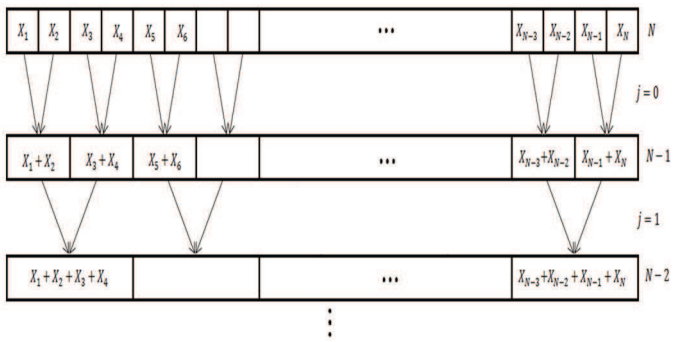

Fig. 2. Diagrama do Processo de Agregação de Dados.

Uma maneira versátil e simples de modelar X_i^{N-j-1} é considerar uma aproximação pela distribuição beta, cuja função de densidade de probabilidade pode ser expressa da seguinte forma [5]:

$$f(w) = \frac{1}{(v-u)} \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} \left(\frac{w-u}{v-u}\right)^{\alpha-1} \left(1 - \frac{w-u}{v-u}\right)^{\beta-1}, \quad (6)$$

onde u e v correspondem ao menor e maior valor respectivamente da série de dados X_i^{N-j-1}, $\Gamma(.)$ corresponde à função Gama, α e β são parâmetros da distribuição Beta e w será considerado como a média da série analisada. Para a estimativa dos valores de ocorrência de probabilidade, por meio da distribuição Beta, é necessário que a Equação (6) seja transformada para um intervalo compreendido entre [0,1]. Dessa forma, segundo o trabalho proposto em [5], a variável de transformação x_i toma então a seguinte forma:

$$x_i = \frac{w-u}{v-u} \quad (7)$$

com isso a função de densidade da distribuição beta assume a seguinte forma:

$$f(x_i) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} (x_i)^{\alpha-1}(1-x_i)^{\beta-1} \quad (8)$$

onde $0 \leq x_i \leq 1$, para $\alpha > 1$ e $\beta > 1$.

A integração numérica da Equação (8) conferem os valores da probabilidade de ocorrência para um valor de x_i qualquer dentro de intervalo [0,1].

Desse modo, através da obtenção das variáveis x_i, agora é possível extrair os multiplicadores do tráfego real para a nova forma de construção de cascata multiplicativa proposta utilizando o seguinte procedimento do estágio j para o estágio $j+1$ dado por:

Para os $b's$ primeiros intervalos os multiplicadores são obtidos pelas equações:

$$R_j^{i=1} = \frac{(x_i)^{b^{N-j}} + (1-x_i)^{b^{N-j}}}{(x_{i-1})^{b^{N-j-1}} + (1-x_{i-1})^{b^{N-j-1}}} \quad (9)$$

e

$$R_j^{i=2,\ldots,b} = \frac{(x_i)^{b^{N-j}} + (1-x_i)^{b-j}}{\binom{b^{N-j-1}}{k} (x_{i-1})^{b^{N-j-1}} (1-x_{k-1})^{b^{N-j-1}}} \quad (10)$$

onde $k = 1, \ldots b-1$.

Para os demais intervalos tem-se:

$$R_j^{i=b+1,\ldots,b^{N-j-1}} = \frac{\binom{b^{N-j}}{k} (x_i)^{b^{N-j}} + (1-x_i)^{b^{N-j}}}{\binom{b^{N-j-1}}{k} (x_{i-1})^{b^{N-j-1}} + (1-x_{i-1})^{b^{N-j-1}}} \quad (11)$$

onde $k = b, \ldots, b^N - 1$.

Pode-se considerar $R_j^{(i)}$ como amostras da distribuição de multiplicadores no estágio j. A distribuição dos multiplicadores na escala j pode ser obtida pelos histogramas de $R_j^{(i)}$.

Na Figura 3 é apresentado o histograma para uma série de tráfego real, representada por X_i^{N-j-1}, assim como a aproximação pela distribuição beta dada pela Equação (8). A série de tráfego utilizada é proveniente de uma rede móvel, coletada no 62º encontro *Internet Engineering Task Force* (IETF) disponível em [6], essa série será denotada por "TraflETF".

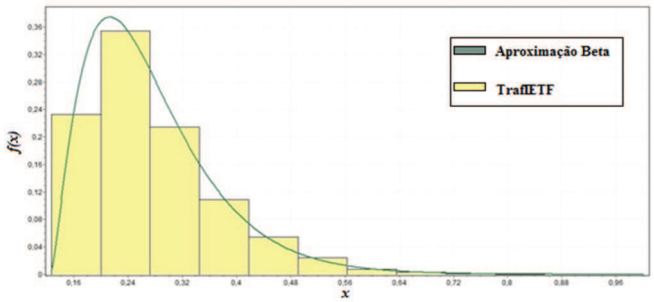

Fig. 3. Aproximação pela Distribuição Beta para a série de tráfego TraffETF quando N=7.

Analisando a Figuras 3 é possível observar que a utilização da aproximação adotada para X_i^{N-j-1} é uma alternativa eficaz, o que nos impulsiona a adotar a distribuição beta para a variável aleatória x.

Baseado nessa nova técnica de construção de cascata multiplicativa conservativa, na próxima seção será apresentado uma nova metodologia para a classificação de tráfego.

III. PROPOSTA PARA A CLASSIFICAÇÃO DO TRÁFEGO

O estabelecimento da base de dados de referência é uma etapa critica de qualquer método de classificação de tráfego que se utiliza de aprendizagem de máquina (*machine learning*). Isso ocorre por que o desempenho da classificação depende da precisão na identificação dos fluxos que serão usados como referências [7].

Foram utilizadas nas fases de treinamento, como nas fases de testes, várias séries de tráfego distintas advindas de dois diferentes tipos de fluxos, denotados por "Dados", extraídos de [8][9] e "Ataque" disponíveis em [10]. O formato das séries de tráfego consiste de um arquivo de texto simples de forma que cada linha apresenta diversas informações relacionadas ao tipo de tráfego. Foram utilizadas apenas informações referentes aos tamanhos dos pacotes. O processo de rotulação dos fluxos foi realizado pelo *software livre L7—filter* [11]. O *software* L7-filter é do tipo DPI (*Deep Packet Inspection*), o *software* procura por padrões característicos no *payload* dos pacotes e os rotula com a aplicação correspondente.

Neste trabalho foi utilizado o algoritmo de aprendizado de máquina C4.5 [12] em combinação com o processo de cascata para extração de características de grupos de séries de tráfego. Esse processo extrai as características de um grupo de fluxos por meio da aplicação do método da cascada inversa como enunciada na Seção II.

O objetivo da utilização de cascada inversa está na obtenção dos multiplicadores ou geradores das cascatas associados a um grupo de fluxos analisados. As variâncias obtidas em cada nível da cascata seguem uma característica exponencial, tal afirmação pode ser verificada através da Figura 4. 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 depositados em um vetor que será denotado por "vetor de atributos".

Na Figura 5 é apresentada a fase de treinamento da metodologia proposta, a qual se inicia com a coleta das séries de tráfego. O conjunto de dados que serão usados no treinamento é rotulado com o nome da aplicação que o gerou, para isso utiliza-se a ferramenta de *software livre* L7-filter.

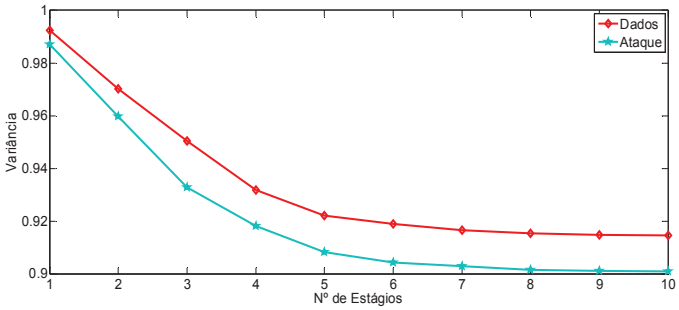

Fig. 4. Característica Exponencial das variâncias dos Multiplicadores das cascatas multiplicativas.

Em seguida, continua-se com os passos do processo de cascatas descrito na Seção II, obtendo as variâncias dos multiplicadores para cada estágio.

Os valores das variâncias extraídas formam um conjunto de dados para treinamento que 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* [13]. Finalmente esse modelo de decisão construído será usado no processo de classificação.

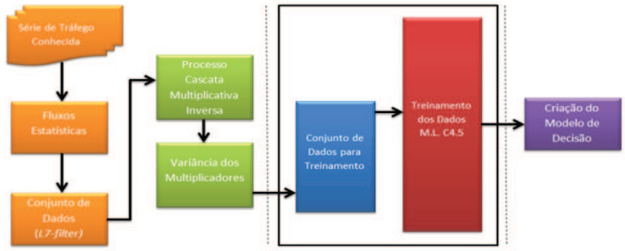

Fig. 5. 1ª Fase de Treinamento.

O esquema de classificação é mostrado na Figura 6. Inicialmente a série tráfego a ser classificada é agrupada em fluxos, depois obtêm-se estatísticas das variáveis de tráfego usadas para a análise. Através dessas estatísticas cria-se o conjunto de dados respectivo à série inicial. O próximo passo é extrair as variâncias dos multiplicadores do conjunto de dados aplicando o processo de cascatas inversa enunciado na Seção II, gerando dessa forma o "vetor de atributos". De posse do "vetor de atributos" aplica-se o modelo de decisão construído na fase de treinamento. Finalmente obtêm-se a predição da classificação do tráfego.

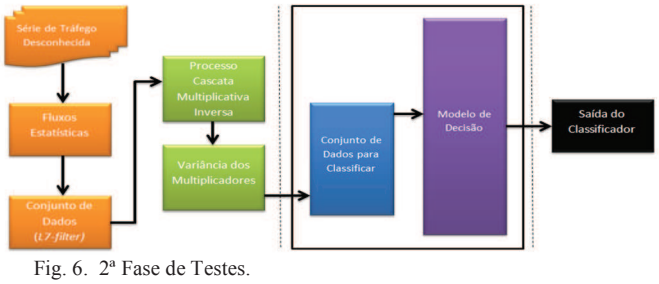

Fig. 6. 2ª Fase de Testes.

IV. MEDIDAS DE DESEMPENHO

O desempenho da metodologia proposta para a classificação de tráfego foi medido através de métricas bastante conhecidas e utilizadas na literatura. As métricas são: *Precision, Recall*, e *F-Measure* [7] [14].

A métrica *Precision* é uma medida de exatidão e denota o percentual de acerto em relação a todos os objetos considerados como positivos, ou seja, 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:

$$Precision = \frac{TP}{TP+FP} \quad (12)$$

A métrica *Acurácia* é o acerto do sistema considerando a proporção de instâncias corretamente classificadas no total dos registos classificados, apresenta a mesma expressão de *Precision*, 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.

A métrica *Recall* é definida 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). A expressão para a métrica *Recall* é dada por:

$$Recall = \frac{TP}{TP+FN} \quad (13)$$

A métrica *F-Measure* tem como característica a sintetização das informações das métricas *Precision* e *Recall*, conseguindo dessa forma uma média harmônica entre as mesmas. A expressão é a seguinte:

$$F - Measure = \frac{(1+\theta)Precision.Recall}{\theta.Precision+Recall} \quad (14)$$

onde θ é um coeficiente que ajusta a importância relativa de *Precision* versus *Recall*, sendo normalmente $\theta = 1$ [15].

V. TESTES EXPERIMENTAIS

Nesta seção serão apresentados os resultados obtidos nos testes experimentais utilizando a metodologia proposta para dois tipos de fluxos de tráfegos:

- "Dados": Séries de tráfego TCP/IP, além de séries HTTP. Essas séries foram extraídas de [8][9].
- "Ataque": Séries de tráfego geradas pela ferramenta de ataque TfnDos - (*Tribe Flood Network denial of service tool* [16]). Essas séries foram extraídas de [10].

Nas figuras 7 e 8 são apresentados os resultados da metodologia proposta referente à métrica *Precision* para as respectivas séries de tráfego: "Dados" e "Ataques". É possível observar que para todos os tipos de tráfego, o método proposto alcança resultados bastante expressivos à medida que a quantidade de estágios utilizados pelas cascatas multiplicativas aumenta. Esse fato é constatado tanto na fase de treinamento como na fase de teste onde a taxa *Precision* obtêm estimativas bem próximas a 100% na classificação do tráfego.

Nas figuras 9 e 10 são apresentados os resultados da metodologia proposta referente à métrica *Recall*, para as respectivas séries de tráfego: "Dados" e "Ataques". Novamente os resultados obtidos nos testes experimentais mostraram taxas de acerto na classificação do tráfego superior a 90% para estágios das cascatas acima de 6.

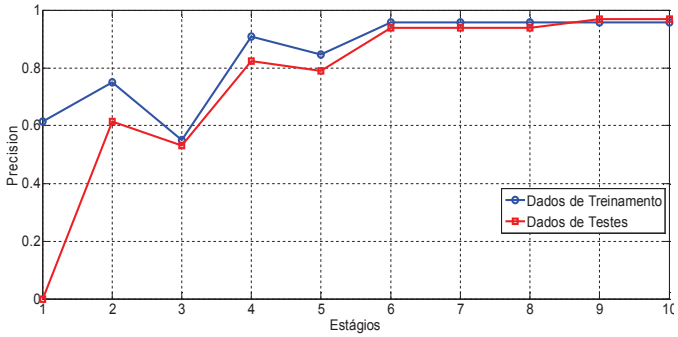

Fig. 7. Métrica *Precision*: Dados de Treinamento e Testes para séries de tráfego de Dados.

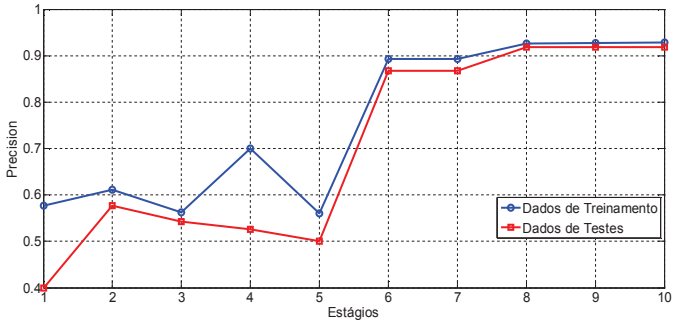

Fig. 8. Métrica Precision: Dados de Treinamento e Testes para séries de tráfego de Ataques.

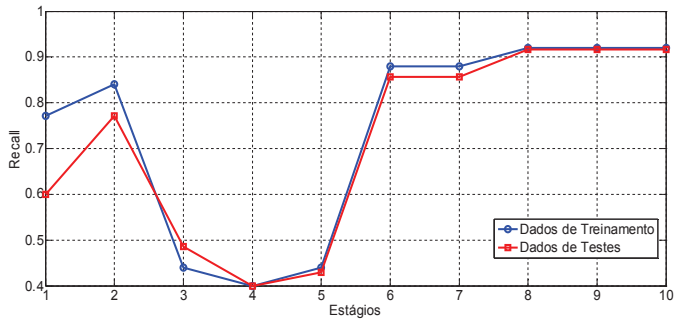

Fig. 9. Métrica *Recall*: Dados de Treinamento e Testes para séries de tráfego de Dados.

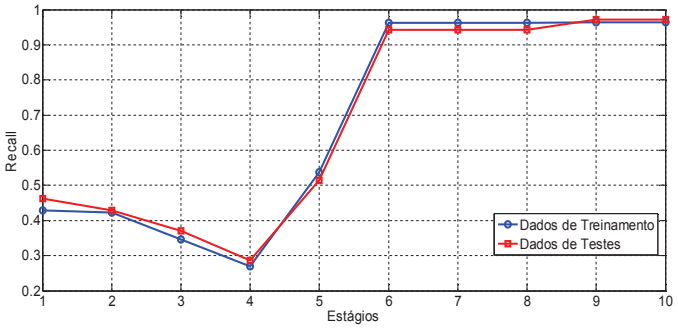

Fig. 10. Métrica Recall: Dados de Treinamento e Testes para séries de tráfego de Ataques.

Finalizando os testes experimentais da metodologia proposta para a classificação do tráfego, foi utilizada a métrica *F-Measure*. Essa métrica pode ser interpretada como uma média ponderada das métricas *Precison* e *Recall*. Os resultados obtidos pela métrica *F-Measure* é um indicativo de que, quanto mais próximo de 1, melhor é a classificação do tráfego e resultados próximos de 0, evidenciam que as classificações são ruins.

Nas figuras 11 e 12 são apresentados os resultados da métrica *F-Measure*. É possível notar que os indicies de classificação correta são bastante relevantes em todos os experimentos realizados. Isso ocorre quando são considerados os estágios das cascatas igual ou superior a 6. Acreditamos que para os estágios iguais ou inferiores a 5 os resultados sempre serão baixos ou insignificantes, devido a pouco quantidade de informações usadas pelas cascatas multiplicativas para cada tipo de tráfego.

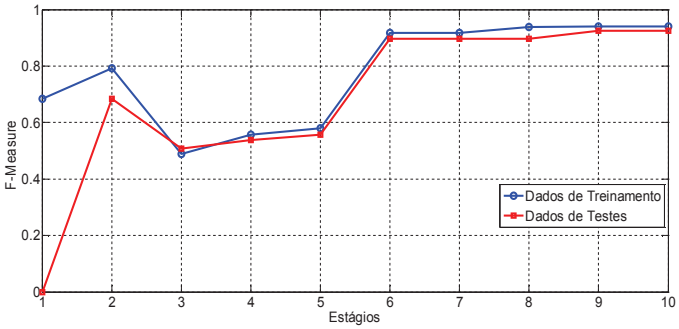

Fig. 11. Métrica *F-Measure*: Dados de Treinamento e Testes para séries de tráfego de Dados.

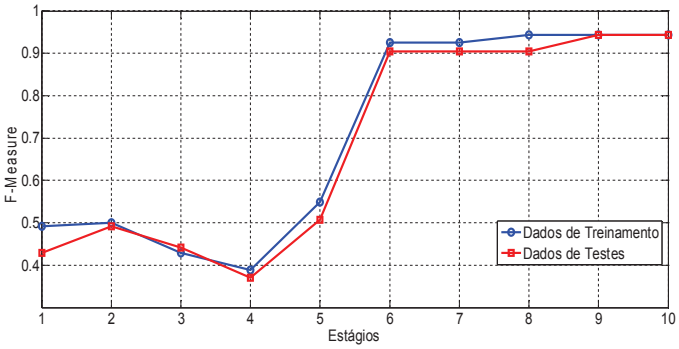

Fig 12. Métrica F-Measure: Dados de Treinamento e Testes para séries de tráfego de Ataques.

Com a finalidade de validação da nova metodologia, os resultados obtidos com as séries de tráfego denotadas por "Dados" e "Ataques" foram comparados com outro método existentes na literatura. O método usado na comparação foi proposto por [17]. Os autores desse modelo utilizam das correlações entre os protocolos relacionados (por exemplo, IMAP, POP, SMTP e webmail) e entre os hosts compartilhando uma base de clientes semelhante, além de explorar e identificar o tempo de introdução de novas características em webmail para a classificação de tráfego HTTP.

Para essa comparação foram utilizados os resultados obtidos da metodologia proposta para as informações na fase de teste no estágio 10 das cascatas multiplicativas. Além disso, considerou-se como medida de conferência a métrica *Acurácia*. Os resultados estão dispostos na Tabela 1, e mostram mais uma vez que o método proposto para a classificação de tráfego é eficiente e robusto.

TABELA 1. COMPARAÇÃO DE MÉTODOS

Série de Tráfego	Método proposto	Método proposto por [17]
Dados	96,9%	93,2%
Ataques	92,7%	90,8%

VI. CONCLUSÃO

Este trabalho apresentou uma nova metodologia para a classificação de tráfego. Utilizando de uma nova abordagem para a construção de cascata multiplicativa conservativa, fundamentada na expressão do Binômio de Newton, foi possível obter parâmetros das séries de tráfego. De posse desses parâmetros aplicou-se um algoritmo de aprendizagem de máquina para a criação uma árvore de decisão ou modelo de classificação. Em seguida testes experimentais foram realizados com a finalidade de comprovar a eficiência da proposta. Os resultados obtidos demonstraram que a metodologia usando cascatas multiplicativas é eficiente e robusta, alcançando classificações do tráfego em níveis de precisão bastante significativos. Acreditamos que essa técnica possa ser melhorada se conseguirmos analisar de forma mais detalhada os padrões de comportamento para os diferentes tipos de tráfego existentes na rede.

REFERÊNCIAS

[1] 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.

[2] Hurley,J.; Garcia-Palacios, E. and Sezer, S. Classifying Network Protocols: A 'Two-Way' Flow Approach, Communications, IET, vol. 5, pp. 79-89, 2011.

[3] Waymire, E. and Williams, S. Multiplicative Cascades: Dimension Spectral and Dependence. Journal Fourier Anal. and Appl.(Kahane Special), pages 589–609, 1995.

[4] Stênico, J. W. G.; Lee, L. L. A New Binomial Conservative Multiplicative Cascade Approach for Network Traffic Modeling. In: 27th IEEE International Conference on Advanced Information Networking and Applications - IEEE AINA 2013,Vol. 1 Pages 794-801, Barcelona, Spain 2013.

[5] Falls, L. W. The Beta Distribution: A Statistical Model for World Cloud Cover. Vol. 79, Issue 9, pp. 1261-1264, 1974.

[6] Jardosh, A., Ramachandran K. N., Almeroth K. C. and Belding, E. "CRAWDAD Data Set UCSB / IETF – 2005 out 2005". http://crawdad.cs.dartmouth.edu/ucsb/ietf2005.

[7] 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.

[8] http://ita.ee.lbl.gov/html/traces.html

[9] http://loadshedding.ccaba.upc.edu/trafic _classification

[10] http://lever.cs.ucla.edu/ddos/traces

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

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

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

[14] 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.

[15] Van Rijsbergen, C. J. Information Retrieval. 2nd Butterworths Heinemann Newton, MA, USA ISBN: 0408709294, 1979.

[16] http://www.iss.net/security _center/reference/vuln/tfn-dos.htm

[17] Schatzmann, D., Mühlbauer, W., Spryropopulos, T. and Dimitropoulos, X. Digging into HTTPS: Flow-Based Classification of Webmail Traffic. Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement, pp. 322-327, 2010.