Journal of Computational Interdisciplinary Sciences (2011) 2(3): 197-205
© 2011 Pan-American Association of Computational Interdisciplinary Sciences
Printed version ISSN 1983-8409 / Online version ISSN 2177-8833
http://epacis.net
doi: 10.6062/jcis.2011.02.03.0046

Network traffic characterization based on Time Series Analysis and Computational Intelligence

Adriana C. Ferrari Santos, José Demisio Simões da Silva[†],
Lília de Sá Silva and Milena Prado da Costa Sene

Manuscript received on September 15, 2010 / accepted on December 8, 2011

ABSTRACT

This paper presents an approach for computer network traffic characterization by using *Time Series Analysis and Computational Intelligence* techniques. HTTP network traffic datasets grouped into different periods of day were analyzed under Kurtosis, DFA and SOM-based clustering algorithms. The results obtained from the calculation of DFA and Kurtosis for each value of the attributes of the network session mapped a range of values of kurtosis and DFA regarded as the standard network. Any sessions of traffic whose attribute values when calculated with Kurtosis and DFA result values within the range mapped means the session is "normal" for that day and period. Were also obtained satisfactory results in the characterization of network traffic pattern through the application of clustering technique with rates of diversion and similarity of 10% and 70% respectively. The results have shown that, according to the observed datasets at certain time of day, the clusters may vary within a range of values, thus representing the traffic pattern behavior of the monitored network in specific period of the day and day of the week.

Keywords: computational mathematics, network traffic analysis, network security, time series analysis, computational intelligence application, data mining.

1 INTRODUCTION

Currently, given the growing use of computers connected to the Internet, concern about security, availability and integrity of stored data and systems is increasing significantly. Many essential benefits for companies are provided by computer networks, such as products and services exhibition through Web pages, messaging and systems available for different user profiles. However, the networks may present vulnerabilities that may expose them to the illegitimate actions. Successful attacks are capable of interrupting services operation, causing data loss, allowing the improper use of network resources, denigrating the company image and causing financial losses.

In order to detect attacks and maintain the correct operation of the computer networks, various preventive tasks have been developed over the years such as deploying anti-virus and anti-spyware applications, firewall systems and intrusion detection tools. However, for recognition of attack patterns in networks, it is necessary to use robust techniques to automate the process of analysis and mining of large and complex network traffic datasets over time. These techniques should provide adequate mapping of network behavior and to allow the detection of anomalous events accurately and fast.

This work presents results of a research carried out at INPE (National Institute for Space Research) that aims to characterize the behavior of network traffic by using Time Series Analysis and

Correspondence to: Adriana C. Ferrari Santos – E-mail: aferrarisantos@gmail.com
Instituto Nacional de Pesquisas Espaciais, São José dos Campos, SP, Brazil – E-mails: lilia@dss.inpe.br / milena@dss.inpe.br

[†] *In memoriam*

Computational Intelligence techniques. Network traffic data generated from Web services and grouped into different periods of the day were analyzed through the Kurtosis, DFA and SOM-based clustering techniques [10-16].

The theoretical basis relevant to the work, including definitions of modeling network traffic in sessions, session attributes, as well as anomalies in network traffic, are described in Section 2 of this article. The techniques used to perform time series analysis, such as DFA, Kurtosis and SOM-based clustering are discussed in Section 3. Section 4 presents the results of the analyzed series. Conclusion of this work and comments are addressed in Section 5.

2 NETWORK TRAFFIC DATA

During the network data communication process, packets are transferred between host pairs. Network traffic can be defined as large network packet datasets, which are generated during the data communications over time. Therefore, network traffic datasets can be analyzed as time series.

The data exchange between client and server machines provides a finite sequence of packets in a given time interval. As defined in [12] and adopted in this paper, the term "network traffic session" consists of any sequence of network packet data which characterizes the information exchange between two IP addresses during a defined time period, when accessing determined network service, providing information of beginning, middle and end of the data transmission process, even all data communication is contained in a single data packet.

Each network traffic session can be modeled in a unique way, through attributes contained in the packet header. Some "primitive attributes" include source IP, destination IP and application protocol. Semantically stronger Information named "derived attributes" can be extracted from the primitive attributes. For example, number of packets received by the host server at any time interval or number of bytes received by the host client.

In general, the network traffic shows a dynamic behavior [1]. Some factors that influence the network traffic behavior are: type of services provided, number of users and hosts connected, and periods of the day on which the services are accessed. Therefore, the activity of modeling the network traffic behavior can be made from analysis of network traffic session attributes, considering that attribute values will change over time with the changes in the factors mentioned above.

Network anomaly is that beyond the expected behavior. That is, what is outside the average. Possible events that cause network anomaly not necessarily consist of attacks, but may indicate misuse or acceptable deviation from network pattern behavior, including failure events in hardware or software resources, physical infrastructure or data collection problems, and others [8, 11]. Thus, network anomalies should be classified as anomalous sessions, so that immediate application of countermeasures can be implemented.

In order to map the network traffic behavior and classify events in network environments, datasets composed of attributes of network traffic sessions in a local computer network at INPE have been studied. The session attributes have been extracted from network packets collected in four periods of the day: 00:00 to 06:59h, 12:59 to 07:00h, 13:00 to 19:00h and 18:59 to 23:59h from March 5 to May 6, 2010.

Each session is represented by a set of nine (9) attributes, including: *psizeCL* (average size of packets received by the client), *psizeSV* (average size of packets received by the server), *pnumCL* (total packets number received by the client) and *pnumSV* (total packets number received by the server), *smallpkt* (percentage of small packets less than 130 bytes), *datadir* (traffic direction – if clients receive one packet, direction is incremented by 1; if server receives one packet, direction is decremented by 1), *brecvCL* (total bytes number received by the client), *brecvSV* (total bytes number received by the server) and *duration* (session length calculated by subtracting the first packet timestamp of the last packet timestamp in seconds).

Each network data packet was captured by the *tcpdump* software. For each session, a vector of nine attributes was mapped and all session vectors were recorded in a MySQL database using RECON – System for Reconstruction of TCP / IP Session [1].

3 APPLIED TECHNIQUES

Due to the large network traffic volume and the existence of some similar characteristics between normal and anomalous events, the characterization of network traffic behavior is a task that requires significant effort of data mining. Thus, computational tools to automate this process are essential. In this work, in order to achieve satisfactory results for characterization of the traffic behavior, time series analysis (Kurtosis and DFA) and SOM-based Clustering techniques were applied.

3.1 Kurtosis

Kurtosis is a measure of dispersion that characterizes the thinning or flattening of the characteristic curve of distribution of a population. It is normally defined by the expression:

$$K = \frac{m_4(\mu)}{\sigma^4} \tag{1}$$

where $m_4(\mu)$ is the fourth central moment and σ is the standard deviation.

According to [9], the kurtosis technique measures the divergence between the curves considered and agreed as normally flat, providing the concentration of data around its center, or average. The frequency distribution curves are classified by the kurtosis measure as illustrated in Table 1.

Table 1 – Time series classification according to kurtosis values.

Classification	$\langle K\rangle$	Curve flattening
Platykurtic	< 3	The curve is flatter than the normal distribution
Mesokurtic	$= 3$	The curve is equal to the normal distribution
Leptokurtic	> 3	The curve is highest (tapered) than the normal distribution

Curves presenting normal frequency distribution are unimodal (with only one peak) and symmetric (the areas under the curve are identical on both sides of the mean). These may have different standard deviations, causing varied levels of kurtosis.

3.2 DFA

DFA (*Detrended fluctuation Analysis*) is a tool proposed by Peng [9] that has been applied in various fields to determine the scale monofractal properties and to detect long-range correlations. This approach eliminates the tendency of time series at different scales by analyzing intrinsic fluctuations of the data. Fluctuations are seen as the measure of signal variability associated to the variance of each segment of the series at different scales [3].

According to [17] detrending methods for fluctuation analysis have been recently proposed and applied for detection of persistent correlations in non-stationary time series analysis (Bashan et al., 2008). The DFA algorithm considered in our approach is composed of six computational operations starting on a discrete time series of amplitudes $\{A_i\}$:

- Discrete Integration: Calculate the cumulative representation of $\{A_i\}$ as

$$C(k) = \sum_{i=1}^{k} (A_i - \langle A\rangle), \quad (k = 1, 2, \dots, N) \tag{2}$$

where $\langle A\rangle = \sum_{i=1}^{N} A$ is the average of $\{Ai\}$.

- Windowing: Using an arbitrary local window of length n, divide $C(k)$ into non-overlapping $N_n = \text{int}(N/n)$ sub-interval $c_j(j = 1, 2, \dots, N_n)$. Note that each sub-interval c_j has length n and N may not be the integer multiple of n. Then, the series $C(k)$ is divided once more from the opposite side to make sure all points are addressed, performing at the end of this operation $2N_n$ sub-intervals.
- Fitting: Get, in each sub-interval, the least-square fits as follows:

$$\begin{aligned} p_j^m(k) &= b_{j0} + b_{j1}k + \cdots + b_{jm-1}k^{m-1} \\ &\quad + b_{jm}k^m, \qquad m = 1, 2, \dots \end{aligned} \tag{3}$$

where m is interpreted as the order of the detrended trend, denoted here as DFA^m.

- Variance: Compute the cumulative deviation series in every sub-interval, where the trend has been subtracted: $C_j(k) = C(k) - p_j^m(k)$. Then, calculate the variance of the $2N_n$ sub-intervals:

$$\begin{aligned} F^2(j,n) &= \langle C_j^2(i)\rangle \\ &= \frac{1}{n}\sum_{i=1}^{n}\Big[C\big((j-1)n+i\big) - p_j^m(i)\Big]^2 \end{aligned} \tag{4}$$

for $j = 1, 2, \dots, N_n$, and

$$\begin{aligned} F^2(j,n) &= \langle C_j^2(i)\rangle \\ &= \frac{1}{n}\sum_{i=1}^{n}\Big[C\big(N-(j-N_n n+i)\big) - p_j^m(i)\Big]^2 \end{aligned} \tag{5}$$

for $j = N_n + 1,\ N_n + 2, \dots, 2N_n$.

- Fluctuation: Calculate the average of all the variances and the square root to get the fluctuation function of DFA $F(n)$:

$$F(n) = \left[\frac{1}{2N_n}\sum_{j=1}^{2N_n} F^2(j,n)\right]^{1/2} \tag{6}$$

- Scaling Exponent: Perform, recursively, the computation from windowing to calculate the corresponding $F(n)$ with different $n([N/4] > n \geq 2m + 2)$ box lengths. In general, in the presence of fluctuations in the form of power law: $F(n) = Kn^\alpha$, $F(n)$ increases linearly with n. Then, using the linear least-square regression on the double log plot log $F(n) = \log K + \alpha \log n$ one can get the slope α, which is the scaling exponent of the DFA method.

By using the value of alpha fluctuation exponent generated by the DFA function, a time series may be classified as shown in Table 2.

Table 2 – Time series classification according to values.

Classification	α (DFA)
Anti-correlated	$\alpha < 1/2$
Correlated	$\alpha > 1/2$
Uncorrelated	$\alpha \cong 1/2$

3.3 SOM-based Clustering

The technique of clustering considers that all data belonging to a same cluster (or class) present more characteristics in common among themselves than when compared with data belonging to other clusters. Data classification is different from data clustering. For classification, the available data must be assigned to previously known clusters, while in the clustering process, clusters are not defined previously, are discovered during the process [2, 5].

In this work, a clustering strategy is used to simulate the SOM (Self Organizing Map), a neural network based on a non-supervised and competitive learning process [7]. While the SOM network seeks a center to be a representative point of each cluster, the clustering strategy searches for the representative vector and groups similar data in this cluster.

The "dataclustering" algorithm analyzes the input vectors, representing the network traffic sessions with nine attributes, and groups them into cluster according to their similarity. The degree of similarity (ds) is a parameter that must be initially configured, since it influences the accuracy of the resulting clustering. For this work, a deviation of up to 10% between the vectors is adopted ($ds = d \geq 0.9$ and $d \leq 1.1$), i.e. the input vectors whose similarity score differs by up to 10% of the representative vector are classified as belonging to that cluster. During clustering, a weight matrix (w) is constructed as follows: each entry that defines the existence of a new cluster is inserted as a new row in the weight matrix. These clusters characterize the default behavior of network traffic over a given period of time.

4 DATA ANALYSIS AND RESULTS

In this work, 252 time series were analyzed, representing to 252 datasets of network traffic session records: each session record is described by nine attributes fields. Table 3 presents a sample (36 series) of the studied datasets, considering data from all Fridays collected during two months (from March 5 to May 6, 2010) in the periods: P1 (dawn – at 00:00 to 06:59), P2 (morning – 07:00 to 12:59), P3 (afternoon – 13:00 to 18:59) and P4 (night – 19:00 to 23:59).

The time series analyzed (shown in Table 3) are datasets of network sessions collected over time related to the default behavior of traffic (normal sessions), that vary over time and day of the week.

4.1 Kurtosis and DFA Results

The Kurtosis value was calculated to analyze the flattening of the frequency distribution curve for the studied series and the DFA fluctuation exponent (Alpha) was used to check if there is a correlation among samples. Figures 1, 2, 3 and 4 show the variation of Kurtosis (K) and DFA (Alpha) values calculated on the attributes *pnumCL*, *pnumSV*, *brecvCL* and *brecvSV* (36 series by attribute) in a sample of observed series.

Through the kurtosis values obtained for each series $(K > 3)$ it was observed that the frequency distribution having only one peak and it is more tapered than the normal one (leptokurtic curve). As this curve is close to the Gaussian curve, the set of analyzed data tend to be homogeneous, indicating that exist sessions with similar characteristics.

Through the DFA fluctuation exponent values (Alpha), it was noticed that the correlation exists among the samples from nine attributes, because alpha $> 1/2$. Thus, it was verified that there are repeated patterns in these data sets, i.e. the values of attributes in the sessions are not identical, but similar enough to permit analyzing and characterizing the sessions behavior in time.

From the images presented in Section 4.1, we can notice that when comparing a new value of kurtosis for the attributes *pnumCL*, *pnumSV*, *brecvCL* and *brecvSV* with that one frequently mapped to the traffic pattern, if this value is within the range $0 < k < 8000$, it means that the attribute belongs to a normal session. Similarly, if the value of DFA is within the range $0.4 < \alpha < 0.7$, the observed attribute also belongs to a normal session.

4.2 Som-based Clustering Results

The technique adopted clustering proved to be very useful because it facilitates the analysis of large datasets over time, providing the discovery of data patterns in the time series. The association of similar elements in one group was defined by the algorithm, so that the resulting number of clusters has become known only after the process of clustering. A sample of the size of clusters is presented in Table 4, illustrating the total number of clusters generated for each date and period.

Table 3 – Description of analyzed time series.

# Time Series	Date	P1 (dawn)	P2 (morning)	P3 (afternoon)	P4 (night)
		Total Sessions	Total Sessions	Total Sessions	Total Sessions
S05032010	03/05/2010	4127	76002	82664	3091
S12032010	03/12/2010	5121	83400	83010	3408
S19032010	03/19/2010	5747	63378	83898	3391
S26032010	03/26/2010	18207	78875	74005	13511
S02042010	04/02/2010	4629	3681	3987	2567
S09042010	04/09/2010	3716	74598	66848	4657
S16042010	04/16/2010	21420	68566	98742	34994
S23042010	04/23/2010	5029	85901	84543	2636
S30042010	04/30/2010	4200	76777	87296	12773

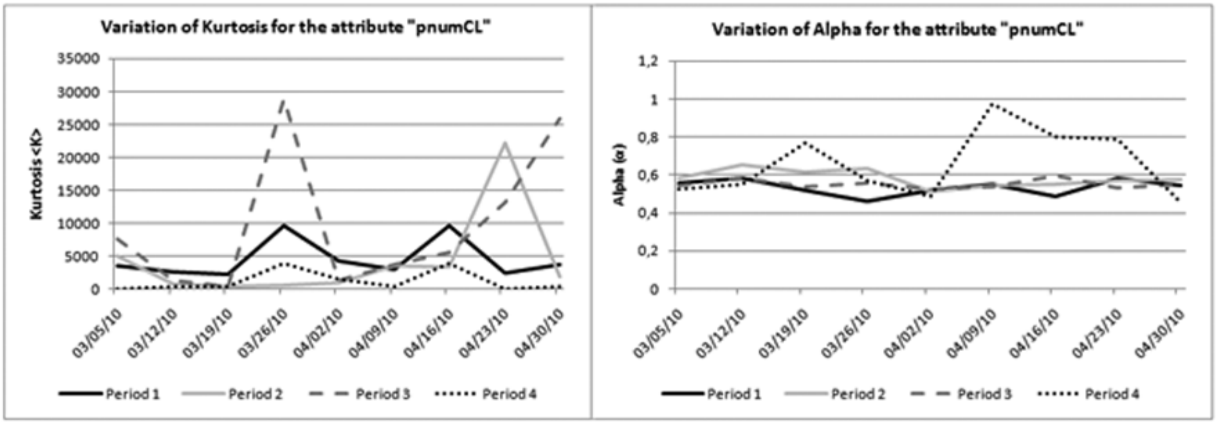

Figure 1 – Kurtosis and DFA for the attribute "pnumCL".

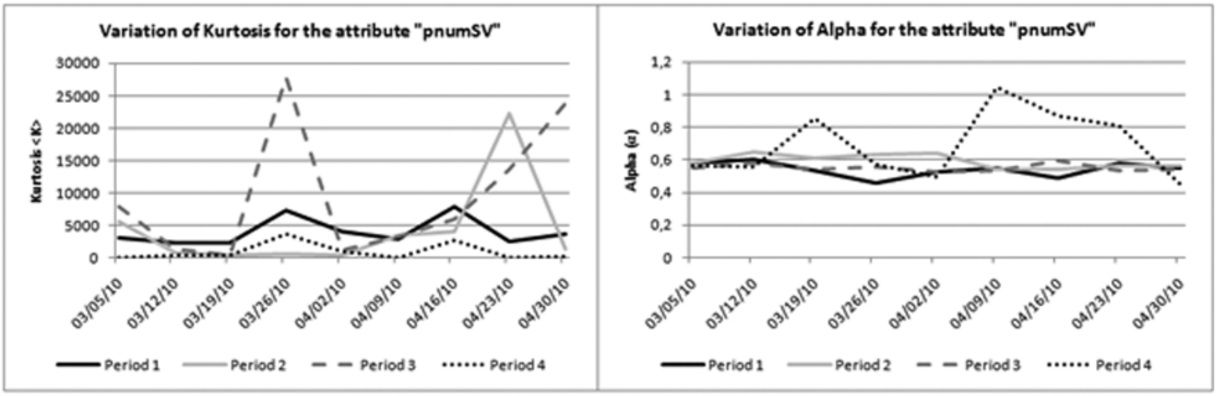

Figure 2 – Kurtosis and DFA for the attribute "pnumSV".

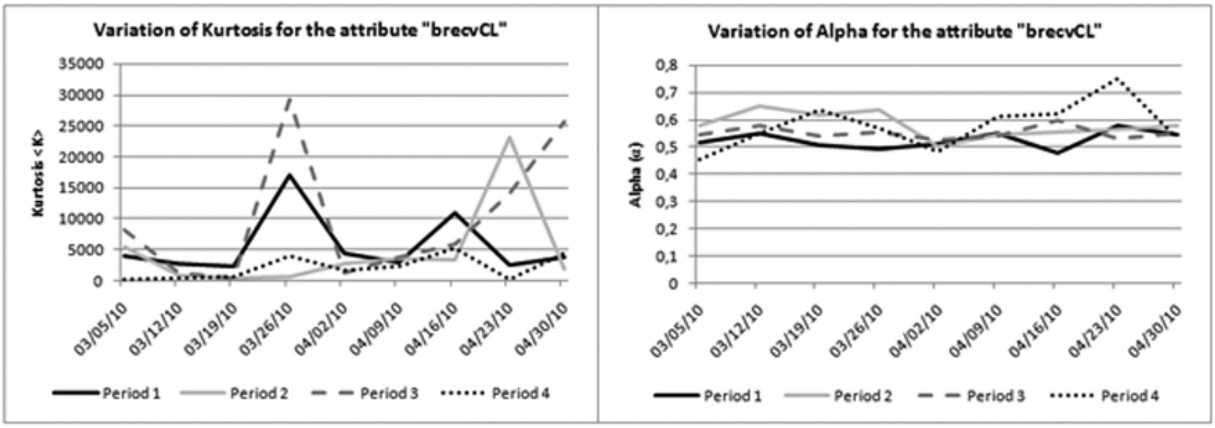

Figure 3 – Kurtosis and DFA for the attribute "brecvCL".

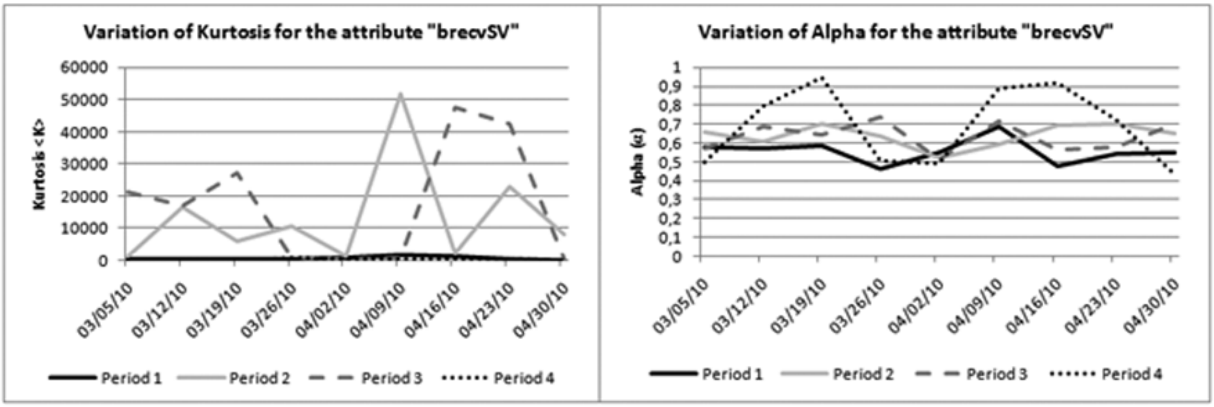

Figure 4 – Kurtosis and DFA for the attribute "brecvSV".

Table 4 – Total clusters generated for time series.

# Time Series	Date	P1 (dawn)		P2 (morning)		P3 (afternoon)		P4 (night)	
		Total Sessions	Total Clusters	Total Sessions	Total Clusters	Total Sessions	Total Clusters	Total Sessions	Total Clusters
S05032010	03/05/2010	4127	38	76002	6906	82664	8158	3091	181
S12032010	03/12/2010	5121	51	83400	8093	83010	7779	3408	422
S19032010	03/19/2010	5747	65	63378	6203	83898	5698	3391	264
S26032010	03/26/2010	18207	136	78875	7000	74005	5576	13511	51
S02042010	04/02/2010	4629	34	3681	34	3987	24	2567	22
S09042010	04/09/2010	3716	73	74598	7457	66848	6969	4657	153
S16042010	04/16/2010	21420	68	68566	7317	98742	7178	34994	313
S23042010	04/23/2010	5029	85	85901	7341	84543	6000	2636	169
S30042010	04/30/2010	4200	141	76777	7554	87296	7765	12773	115

The values in column "Total Clusters" indicates that the default behavior of the samples (sessions with nine attributes related to all Fridays from March to April 2010) varies within the ranges according to the period of the day. For P1, the range is 40-200 clusters; for P2, the range is 6000-8000 clusters, for P3, the range is 5500-8000 clusters and for P4, the range is 50-425 clusters. So, the traffic pattern behavior for other Fridays of the month to be analyzed should fall within their respective ranges. Otherwise, it is recommended that the network administrator make a more detailed analysis of the suspicious sample.

By analyzing columns P2 and P3 in Table 4, it was observed that the total clusters on April,02 has a value very different (outliers) from the other days. However, this traffic was classified as normal, because that day was a holiday (Good Friday), i.e., the traffic volume was lower than in normal days. This reflects an anomalous behavior of the network, but it does not represent an attack. Figures 5 and 6 illustrate the results of clustering of a randomly chosen data sample showing the number of sessions grouped into clusters in two monitored time period. Two parameters were used in the clustering process: deviation (10%) and similarity rate (70%).

As seen in Figures 5 and 6, over 98% of sessions were grouped into a single cluster (cluster 1) indicating that most sessions analyzed have similar characteristics. It was concluded, therefore, that the most populated cluster contains sessions that describe the behavior pattern of traffic. Namely, it is possible to characterize the behavior pattern of the traffic by analyzing only the knowledge base generated by larger clusters.

Thus, by using the SOM-based Clustering algorithm, the clustering problem of network traffic session considering different periods of the day is solved, maintaining certain homogeneity among sessions inside the clusters and heterogeneity among cluster values. The results have showed that, according to the observed period of the day, the clusters can vary within a range of values, thus representing the pattern behavior of the network traffic.

The advantage of using this technique is the ability to perform multivariate analysis of traffic, with nine session attributes are processed together to group similar sessions of the traffic, considering the intrinsic characteristics of sessions when their attributes are analyzed together. Multivariate analysis allows a better characterization of network behavior over time. Moreover, this technique provides benefits in performance and processing time.

Considering the large volume of network traffic data to be analyzed in just one day of the month – an average of 8,000 sessions per period of low traffic (night and dawn) and 70,000 sessions per period of increased traffic (morning and afternoon), the work with the largest clusters should allow for the reduction of the database, and consequently increased efficiency of the anomaly detection system.

5 CONCLUSION

In order to characterize the HTTP network traffic behavior with satisfactory precision and time, it is necessary to analyze large, multivariate and complex traffic datasets, containing thousands of data points distributed over time. In this study, network traffic datasets collected from a local network in four periods of the day, every Friday, for two months were analyzed.

The task of traffic characterization of a network is tedious and repetitive due to the large and complex volume of data points to process. Thus, performing this process manually is unfeasible and, therefore, computational techniques should be used to automate this activity, requiring minimal human supervision in the final stage of analysis.

By applying Kurtosis and DFA statistical technique, it was found that it is possible to characterize the behavior pattern of each of the nine attributes separately.

Satisfactory results were also obtained using the SOM – based clustering technique on to characterize the behavior of network traffic pattern, with benefits in performance and processing time. Allows multivariate analysis of the nine attributes of the sessions together, allowing the characterization of sessions of the network over time.

As future work, larger network traffic datasets will be studied, taking into account the every day of the week, in order to map the traffic behavior pattern all week. Also, the behavior of each cluster of sessions generated will be analyzed in more detail, and tests with other similarity degrees in the SOM-base Clustering technique will be conducted. Also, synthetic datasets containing anomaly events will be generated in a controlled network environment for analysis. Anomalous sessions collected from this simulated traffic will be rebuilt in attributes generating new datasets to be used to characterize the anomalous traffic behavior. As next steps, the current traffic sessions will be classified as normal or anomaly, based on historical traffic profile characterized over time.

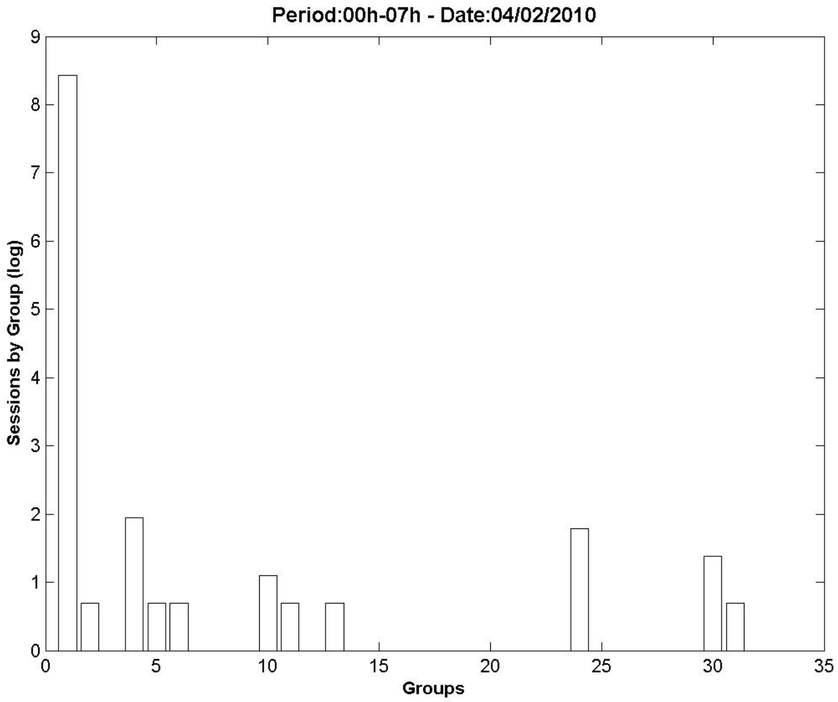

Figure 5 – Clustered sessions – Period P1: 00:00-07:00h (dawn).

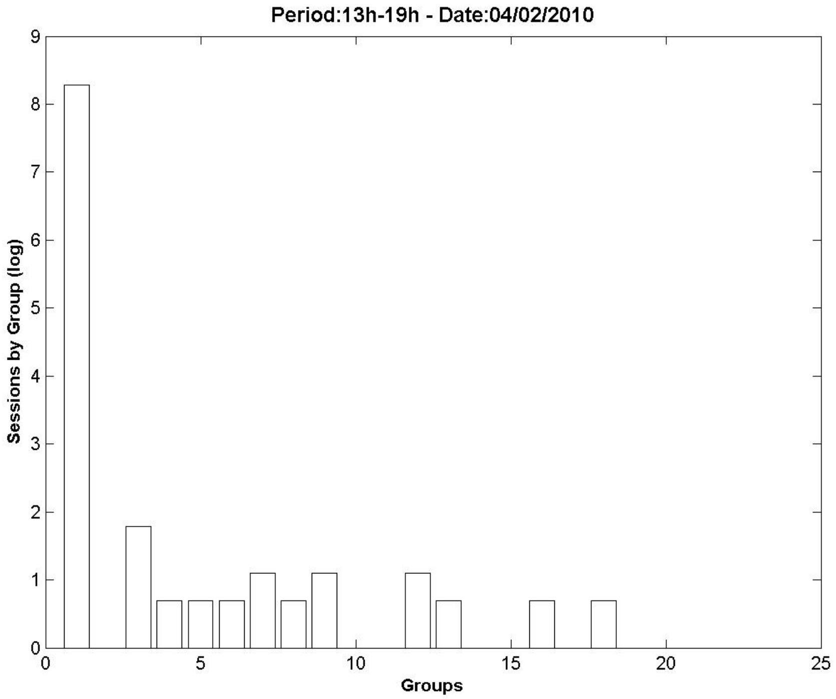

Figure 6 – Clustered sessions – Period P3: 13:00-19:00h (afternoon).

REFERENCES

[1] CHAVES MHP. 2002. Análise de Estado de Tráfego de Redes TCP/IP para Aplicação em Detecção de Intrusão. Dissertação de Mestrado em Computação Aplicada – INPE, set. 2002.

[2] ERTOZ L et al. 2003. Detection and summarization of novel network attacks using data mining. Technical Report. Minneapolis, USA: University of Minnesota. 20 p.

[3] FREITAS MR et al. 2009. Análise de anisotropia de imagens utilizando o método DFA: um estudo de caso na área de exploração de petróleo. Anais XIV Simpósio Brasileiro de Sensoriamento Remoto, Natal, Brasil, 25-30 abril 2009, INPE, p. 6463–6470.

[4] HAYKIN S. 2001. Redes neurais princípios e práticas, 2 ed. Porto Alegre: Bookman, 2001. 900 p. ISBN 8573077182.

[5] KAYACIK HG et al. 2003. On the capability of an SOM based intrusion detection system. In: IJCNN'2003 International Joint Conference on Neural Networks, 2003, Portland, Oregon, USA. Proceedings of... Piscataway, NJ, USA: IEEE, v. 3, p. 1808–1813.

[6] MILONE G. 2004. Estatística: geral e aplicada. São Paulo: Pioneira Thomson Learning.

[7] MUKKAMALA S & SUNG AH. 2003. Identifying significant features for network forensic analysis using artificial intelligence techniques. International Journal on Digital Evidence, 1(4).

[8] QAYYUM A et al. 2005. Taxonomy of Statistical Based Anomaly Detection Techniques for Intrusion Detection, IEEE International Conference on Emerging Technologies, Islarnabad, sept. 2005.

[9] PENG C. 1994. Mosaic organization of DNA nucleotides, Physical Review, 9(2), fev. 1994.

[10] SANTOS ACF, SILVA LS, SILVA JDS & ROSA RR. 2009. Aplicação de Técnicas de Análise de Séries Temporais em Dados de Tráfego de Rede. In: Workshop dos Cursos de Computação Aplicada, 9., 2009, INPE, São José dos Campos, SP. Anais... São José dos Campos: INPE.

[11] SILVA LS, SANTOS ACF, MANCILHA DT, SILVA JDS & MONTES A. 2008. Detecting attack signatures in the real network traffic with Annida. Expert Systems with Application: An International Journal, 34(4), p. 2326–2333, may 2008. ISSN:0957-4174.

[12] SILVA LS. 2007. Uma Metodologia para Detecção de Ataques no Tráfego de Redes baseada em Redes Neurais. 2007. 254 p. Dissertação (Doutorado em Computação Aplicada) – Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, SP.

[13] SILVA LS, SANTOS ACF, SILVA JDS & MONTES A. 2006. Hamming net and LVQ neural networks for classification of computer network attacks: a comparative analysis. In: SBRN'2006 Brazilian Neural Networks Symposium, 9., 2006, Ribeirão Preto, São Paulo. Anais... [S.l.]: IEEE Explore Digital Library, 2006. p.13. ISBN 0769526802
http://doi.eeeecomputersociety.org/10.1109/SBRN.2006.21.

[14] SILVA LS, MONTES A, SILVA JDS, MANCILHA TD & SANTOS ACF. 2006. A framework for analysis of anomalies in the network traffic. In: Workshop dos Cursos de Computação Aplicada, 6., 2006, INPE, São José dos Campos, SP. Anais... São José dos Campos: INPE, 2006. Disponível em: <eprint.sid.inpe.br/rep-/sid.inpe.br/ePrint@80/2006/12.20.23.21> Acesso em: 13 dez. 2006.

[15] SILVA LS, SANTOS ACF, SILVA JDS & MONTES A. 2005. ANNIDA: Artificial Neural Network for Intrusion Detection Application – Aplicação da Hamming Net para detecção por assinatura. In: CBRN'2005 Congresso Brasileiro de Redes Neurais, 7., 2005, Natal, RN, Brasil. Anais... [S.l.]: [s.n.], 2005.

[16] SILVA LS, SANTOS ACF, SILVA JDS & MONTES A. 2004. Neural network application for attack detection in computer networks. In: IJCNN'2004 International Joint Conference on Neural Networks, 2004, Budapeste, Hungria. Proceedings... Piscataway, NJ, USA: IEEE, 2004. (INPE-11626-PRE/7007).

[17] VERONESE TB, ROSA RR, BOLZAN MJA, ROCHA FERNANDES HS & KARLICKY M. 2010. Fluctuation analysis of solar radio bursts associated with geoeffective X-class flares. In: Journal of Atmospheric and Solar-Terrestrial Physics, doi:10.1016/j.jastp.2010.09.030.