Graph-based Correlation of SNMP Objects for Anomaly Detection

Bruno Bogaz Zarpelão[1], Leonardo de Souza Mendes[1] and Mario Lemes Proença Jr.[2],

[1] School of Electrical and Computer Engineering, State University of Campinas (UNICAMP), Campinas, SP, Brazil
[2] Computer Science Department, State University of Londrina (UEL), Londrina, PR, Brazil

Summary
Anomaly detection is essential, because it allows a rapid reaction to the problems and helps assuring performance and security in computer networks. This paper presents an anomaly detection system based on: (i) the traffic characterization performed by the BLGBA model, which is responsible for the DSNS generation; (ii) an alarm system that compares the DSNS and the real movement obtained in SNMP objects, sending the alarms to a correlation system when a behavior deviation is detected; (iii) a correlation system based on a directed graph which represents the possible paths of anomaly propagation through the SNMP objects in a network element. Three years of data collected from the State University of Londrina network were used to evaluate this anomaly detection system. The results were encouraging and confirmed that our system is able to detect anomalies on the monitored network elements, avoiding the high false alarms rate.

Key words:
Anomaly Detection, SNMP, DSNS, Correlation, Directed Graph

1. Introduction

Computer networks are of vital importance nowadays for modern society, comparable to essential services like piped water, electricity and telephone. Their functionality cannot be interrupted due to their importance for the people that use their services. In this context, the automation of the network management became fundamental for reducing costs, early detection of network failures and avoiding performance bottlenecks. Anomaly detections allow the administrators to answer appropriately to the problems, thus ensuring networks reliability and throughput [1][4][11][12].

Despite the latest advances in the development of technologies related to networks monitoring, traffic characterization and intrusions detection, to identify anomalies correctly is still a challenging task. Anomalies can arise from different situations, thus making it difficult to develop techniques to detect them. Among the various situations that can cause anomalies we can mention flash crowds, malfunctioning, network elements failures, vendor implementation bugs, misconfigurations, transfer of very big files, outages and malicious attacks such as DoS (Denial of Service), DDoS (Distributed Denial of Service) and worms [6][7][12][14][16][17][18].

The anomaly detection techniques known as profile-based or statistical-based do not require any previous knowledge about the nature and properties of the anomalies to be detected. Their main advantages are the effectiveness in detecting unknown anomalies and the easiness to adapt to new environments. This method establishes a profile for the normal behavior of the network by studying the history of its movements. The detection is accomplished by searching for significant behavior changes that are not coherent with the previously established profile [5][6][8][14][17].

The first difficulty met when using this method is the fact that there is no consensus about an effective model to characterize network traffic. Factors such as the human working hours create a dynamic network behavior, making the traffic characterization more difficult [1][4][5]. An efficient traffic characterization model must be able to deal with these factors. This work deals with the employment of the BLGBA (Baseline for Automatic Backbone Management) model for the calculation of the DSNS (Digital Signature of Network Segment) [10][11] as a suggestion to solve this issue.

The definition of which events represent an anomaly and therefore must be reported to the network administrators is still an open question. The difficulty resides on the non-stationary behavior of the network traffic [5][7][16]. Because of these natural variations that occur in the traffic, normal events can be considered anomalous by the anomaly detection system that will generate a false alarm, also known as false positive. Thus, besides using a well-succeeded traffic characterization, we must possess means to avoid the generation of false positives and false alarms when comparing real traffic to the profile established by the DSNS.

Besides identifying the occurrence of an anomaly, the anomaly detection system must offer additional information about the situation detected thus helping the network administrator to find the origin and solution of the problem quickly. The amount of problems notifications that get to the network administrators must also be observed in order not to overload them [16][18].

An important resource to be used in anomalies detection is the monitoring of different SNMP objects, trying to correlate the results obtained from the analysis performed for each one of these objects. Each one of them offers a particular perspective of the problem. After the correlation these perspectives converge for a single notification containing the additional information useful to the

Manuscript received May 5, 2006.
Manuscript revised May 25, 2006.

localization of the anomaly. Besides, the correlation causes a reduction of the amount of notifications generated. This work proposes the correlation of SNMP objects based on a directed graph that represents the possible courses of anomalies propagation through the objects. This correlation graph is used aiming to verify the occurrence of an anomaly and to generate a map of its behavior related to the network element analyzed, thus increasing the semantic power of the notifications set to the network administrator.

The anomaly detection system presented in this work performs in the first place the comparison between the real traffic and the profile of the normal operations obtained from the traffic characterization. This comparison is based on the identification of behavior deviations in each SNMP object monitored through the BLGBA model. After the comparison, the deviations detected are analyzed using the correlation graph and the occurrence of an anomaly is verified. The anomalies detected can be classified in one of the following categories: *input flow*, *output flow* or *forwarding flow* anomaly. This classification is based on the anomaly behavior map obtained with the aid of the correlation graph.

This work is organized as follows: Section 2 summarizes some work related to the anomaly detection area. Section 3 describes the network environment used to obtain the results. Section 4 deals with the concepts about traffic characterization and presents the BLGBA model and DSNS. Section 5 will present the *Anomaly Detection System* and the results of its application to the previously described network environment. Finally, section 6 relates some final considerations and discusses some possible future work.

2. Related Works

Anomaly detection has been studied by many researchers. The first works were related mainly to security issues. Usually, techniques based on the signatures of the attacks were used instead of characterizing traffic normal operations. Considering the need to detect unknown anomalies the authors initiated the development of techniques that used the characterization of the normal network operations.

It has been recently discovered that besides being necessary to detect the occurrence of anomalies it is important to offer additional information about the problem to facilitate the identification of its origin.

Other works such as [2], [8] and [16] also explore the properties of SNMP (Simple Network Management Protocol) [15] and MIB-II (Management Information Base) [9] aiming to detect anomalies. Cabrera *et al.* [2] presented the possibility of detection of Distributed Denial of Service attacks using data from SNMP objects. Li *et al.* [8] approached the detection of Denial of Service attacks using SNMP objects. Thottan *et al.* [16] used the correlation of some SNMP objects face to the anomalies in order to increase the effectiveness of their detection mechanism.

Roughan *et al.* [12] assumed a simple approach to correlate the generated alarms with the use of two data sources: the SNMP management protocol and the BGP external routing protocol. Based on the premise that the false alarms found in the two data sources are not related, i.e., are not simultaneous, the system detects anomalies only when it finds behavior deviations in the two data sources for the same situation.

The study of traffic matrices represents another branch in the area of detection and diagnosis of anomalies. The global view of the network offered by the matrices can be useful to infer the cause of the anomalies.

Zhang *et al.* [18] presented a framework that uses traffic matrices to perform *network anomography*. The name of this technique comes from the union of the words anomaly and tomography. The *anomagraphy* process is divided in two main steps: anomalies detection and inference about their origin. The different algorithms used at the framework are based on the ARIMA model (Autoregressive Integrated Moving Average), Fourier transform, wavelets and PCA (Principal Component Analysis).

Soule *et al.* [14] have also used the traffic matrices. In the present approach matrices are used to obtain a panoramic view of the network where the Kalman filter is applied. Data resulting from the filtering are analyzed by four different methods that include, for example, statistical techniques to detect sudden behavior changes and wavelet algorithms. These methods are responsible for pointing anomalous situations. A very interesting point of this work is the comparison performed between the results obtained from the application of the four methods.

3. Network Environment Studied

Tests were performed at the backbone of the network of the State University of Londrina (UEL). The network elements used in the experiments were:

- S_1**:** is the Firewall server from the State University of Londrina;
- S_2**:** is the main Web server from the State University of Londrina;
- S_3**:** is responsible for interconnecting the ATM router to the other backbone segments of the State University of Londrina network; it gathers the traffic of approximately 3000 computers;

4. Traffic Characterization

The first step considered as fundamental for anomaly detection is the traffic characterization. The model used must be efficient at establishing a profile for the network traffic normal behavior, which presents self-similar characteristics and a lot of noise. The complete control of this normal behavior profile will lead to a precise diagnosis of anomalies.

In this work, traffic characterization is performed by the BLGBA model (Baseline for Automatic Backbone Management), which is responsible for the generation of the DSNS (Digital Signature of Network Segment). The BLGBA model and the DSNS it generates were both proposed by Proença *et al.* [10][11].

DSNS is the result of traffic characterization. It can be defined as a set of basic information that constitutes the traffic profile of a network element. This information includes data such as traffic volume, number of errors, types of protocols and the services that are carried along the network element during the day.

The BLGBA model was developed based on statistical analyses. It performs analyses for each second of the day, each day of the week, respecting the exact moment of the collection, second by second for twenty-four hours, preserving the characteristics of the traffic based on the time variations along the day. Therefore the goal of the traffic characterization performed by BLGBA is that the resulting DSNS can reflect the normal behavior expected for the network traffic along the day.

The BLGBA algorithm is based on a variation in the calculation of *mode*, which takes the frequencies of the underlying classes as well as the frequency of the modal class into consideration. The calculation takes the distribution of the elements in frequencies, based on the difference between the greatest G_{aj} and the smallest S_{aj} element of the sample, using only 5 classes. This difference is divided by five to form the amplitude h between the classes according to equation (1):

$$h = \frac{\left(G_{aj} - S_{aj}\right)}{5} \quad (1)$$

Then, the limits of each L_{Ck} class are obtained. They are calculated according to equation (2) where Ck represents the k class $(k=1\ldots5)$:

$$L_{Ck} = S_{aj} + h * k \quad (2)$$

The proposal of the calculation of the DSNS for each B_{li} second is to obtain the element that represents 80% of the analyzed samples. The B_{li} will be defined as the greatest element inserted in class with accumulated frequency equal to or greater than 80%. The purpose is to obtain the element that would be above most samples, respecting the limit of 80%. More information about the BLGBA model and DSNS can be found at [10] and [11].

Figure 4.1 illustrates in the form of a histogram the daily movement of S_2, and its respective DSNS, generated by the BLGBA model. In this figure some graphs are shown concerning a week of September 2005, with the DSNS in blue and the real movement that occurred on the day in green and red. It is possible to observe a great adjustment between the real movement and the DSNS.

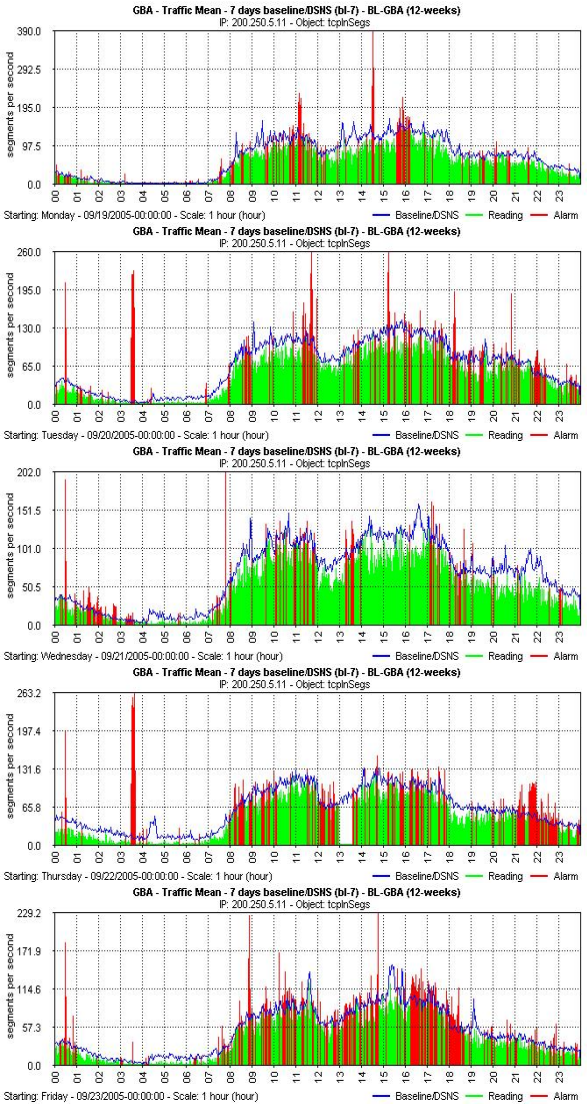

Figure 4.1 Real traffic and DSNS at S_2, SNMP object *tcpInSegs*

5. Anomaly Detection

Anomalies detection is performed by comparing the traffic normal operations profile to the real movement, in order to identify anomalous behaviors in the network. The

Anomaly Detection System must be effective and present a low rate of false positives, besides generating a reduced amount of notifications that do not overload the network administrators and have additional information useful to the search of the cause of the anomaly.
The first objective of this stage is to compare the data obtained through the SNMP objects monitored with its respective DSNS in the search for significant behavior deviations. Deviations detected by each SNMP object bring different perspectives over the present event. They are later correlated, leading to a more precise diagnosis, which will indicate the existence of an anomaly or not. The correlation is based on a directed graph that explains the existing relations between the monitored SNMP objects according to figure 5.1.

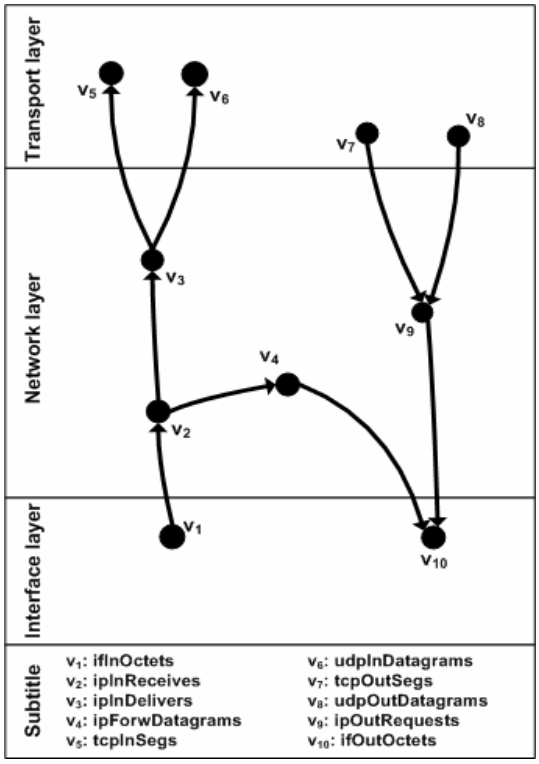

Figure 5.1 Correlation graph

Figure 5.2 presents the reference model of the *Anomaly Detection System*. The GBA tool (Automatic Backbone Management) [11] is responsible for collection and storage of samples and the execution of the BLGBA model for the generation of the DSNS. The *Alarm system* reports the deviation detected through the comparison between the DSNS and the real movement pictured by the SNMP objects. The *Correlation system* gathers these alarms and analyzes them using the correlation graph. Its function is to verify the occurrence of an anomaly and to offer a map of its behavior for the network administrator aiming to help him on the search of the origin and solution of the problem.

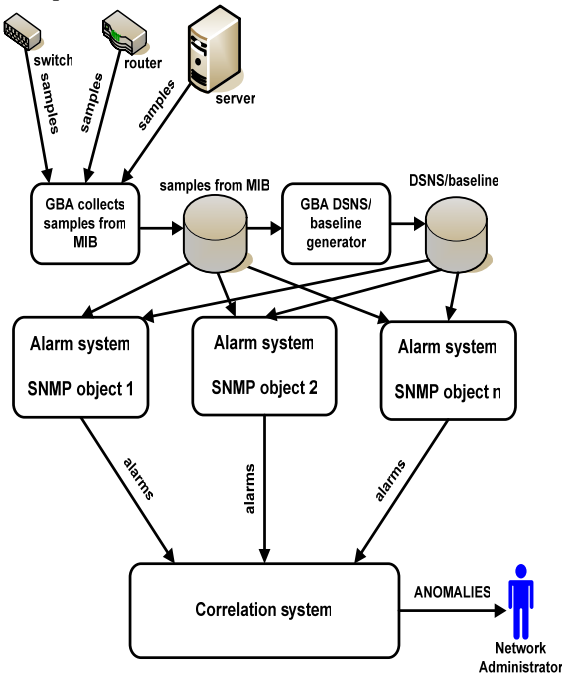

Figure 5-2 Reference model of the *Anomaly Detection System*

5.1 Alarm System

The *Alarm system* indicates the occurrence of behavior deviation in a specific SNMP object, generating an alarm when the three following facts happen simultaneously:

- Fact 1: the real sample analyzed deviates from the limit established by the DSNS and the hysteresis interval *t* is initiated.
- Fact 2: the current sample analyzed overcomes the previous one concerning the occurrence of fact 1 in the hysteresis interval *t*.
- Fact 3: the number of occurrences of fact 2 in the hysteresis interval *t* overcomes the value of δ.

The occurrence of these three facts is required to characterize a significant behavior deviation aiming to avoid the generation of false alarms. The hysteresis interval *t* is of 60 seconds. The value of δ is 25. These conventions have been defined after a great amount of practical and analytical tests in various situations.
The emission of alarms does not generate a straight notification for the administrator, since they indicate not the occurrence of an anomaly but of a behavior deviation in a SNMP object. However, the alarms generated are available in log files and in graphics referring to the

network movements so that the administrators can perform a more precise analysis about the event occurred in case it is necessary. Information such as the moment of the generation, number and frequency of the alarms and values of the DSNS and real traffic can be useful for network planning so that likely preventable future anomalous situations are avoided.

The operation of the *Anomaly Detection System* is based on constant time frames of 5 minutes. The comparison of DSNS to the real movement and the correlation of the alarms are performed in these time frames. For each five-minute time frame, various hysteresis interval *t* can exist. Figure 5.3 presents an example of the behavior of the hysteresis interval *t* at the five-minute time frame during the operation of the *Alarm system*. The hysteresis interval is initiated only when a real sample deviates from the limit established by the DSNS. The five-minute frame however is fixed and independent of any other factor. Once the hysteresis interval is started, if the number of occurrences of fact 2 overcomes δ an alarm is generated and sent to the correlation system.

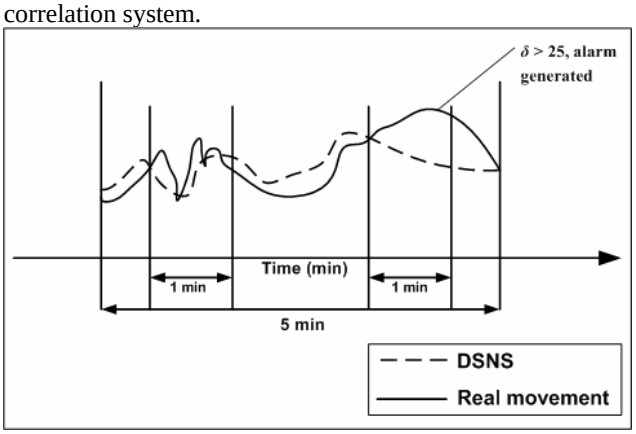

Figure 5.3 Five-minute frame and hysteresis interval *t*

5.2 Correlation System

The *Correlation system* is based on the correlation directed graph presented in figure 5.1. A graph *G* is a data structure defined by $G = (V, E)$, where *V* represents the set of vertices of the graph and *E* the set of edges that link vertices respecting a specific relation between them. For directed graphs, edges express a unidirectional relationship between two vertices and are represented by ordered pairs (x, y) [3]. In correlation graph, an ordered pair (x, y) defines that an anomaly can propagate from the SNMP object represented by vertex *x* to the SNMP object represented by vertex *y*.

The relations of the correlation graph were built based on the characteristics of the information available at each SNMP object monitored. The correlation graph aims to assemble in its scope the possible courses of propagation of anomalies along the SNMP objects, mapping their behavior at the network element analyzed. The analysis and correlation of the SNMP objects belonging to four different groups of the MIB-II [9], *interface*, *ip*, *tcp* and *udp*, allow the detection of a very diversified set of anomalies behaviors.

The correlation graphs helped the identification of three data flow at network elements in general. The first one is the *input flow*, formed by the SNMP objects *ifInOctets*, *ipInReceives*, *ipInDelivers*, *udpInDatagrams* and *tcpInSegs*. The second one is the *output flow* formed by the objects *tcpOutSegs*, *udpOutDatagrams*, *ipOutRequests* and *ifOutOctets*. The third and last one is the *forwarding flow*, presenting the objects *ifInOctets*, *ipInReceives*, *ipForwDatagrams* and *ifOutOctets*.

Figure 5.4 shows the behavior of the data flows face to the layers of the TCP/IP set of protocols. The *input flow* crosses all the layers until it reaches the application layer where all the data will be used. The *output flow* follows the inverse course, starting at the application layer and sending data to the network. The *forwarding flow* gets to the network layer where it is defined the forwarding of data to other points of the network in a process typical of routing equipments.

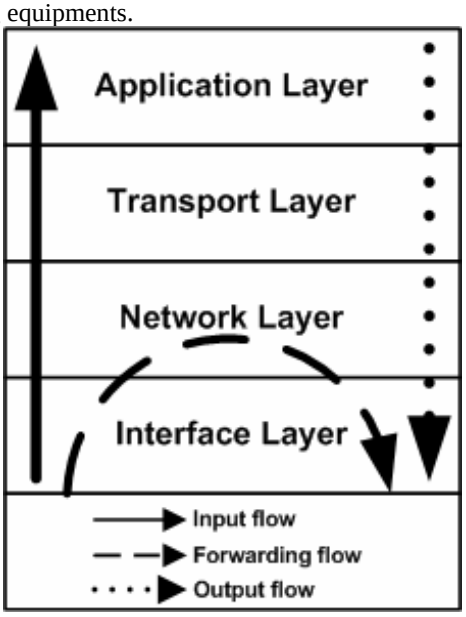

Figure 5.4 TCP/IP protocol layers and the three flows

The algorithm that gathers all the alarms generated and verifies the occurrence of an anomaly through the correlation graph was built based on the depth search algorithm [3]. The difference is that in the depth search algorithm the graph is processed going from a vertex to its adjacent, while in the algorithm used at the correlation system the graph is processed going from a vertex to its

correlated. Two vertices are correlated when they are adjacent and there are alarms generated for both SNMP objects in the same five-minute time frame.

The algorithm developed requires the definition of the initial and final vertices in order to perform the search. The choice of these vertices is based on what we call initial and final monitoring point for *input*, *output* and *forwarding flows*. The initial monitoring point of the *input flow* is the object *ifInOctets* and the final monitoring points are the objects *udpInDatagrams* and *tcpInSegs.* The initial points of the *output flow* are the objects *udpOutDatagrams* and *tcpOutSegs* and the final point is the object *ifOutOctets*. The initial point of the *forwarding flow* is the object *ifInOctets* and the final point is object *ifOutOctets.*

The correlation algorithm is presented in table 5.1. The *depthFirstSearch* routine is recursive and is in charge of processing the correlation graph searching for the course followed by the supposed anomaly, verifying its occurrence and preparing the map to be presented to the network administrator in case the anomaly is detected. The situation is considered anomalous when the search process at the correlation graph reaches a final monitoring point.

5.3 Evaluation and Results

The parameters used to evaluate the performance of the *Anomaly Detection System* are the rate of false positives and the rate of anomalies detected compared to the total of occurrences. The following variables are necessary to calculate these parameters:

- *amount_of_detected*: gives the total number of anomalies that were correctly detected by the *Anomaly Detection System*.
- *amount_of_missed*: gives the total number of anomalies that occurred and were not detected;
- *amount_of_false*: gives the total number of anomaly notifications that don't correspond to an anomaly.

The following rates can be calculated based on these variables:

$$\det ection\_rate = \frac{amount\_of\_\det ected}{amount\_of\_\det ected + amount\_of\_missed} \quad (3)$$

$$false\_rate = \frac{amount\_of\_false}{amount\_of\_\det ected + amount\_of\_false} \quad (4)$$

Figures 5.5 and 5.6 present histograms with the results of the evaluation of the *Anomaly Detection System*. These results were calculated for each month of the second semester of 2005 for the three network elements analyzed in this work: S_1, S_2 and S_3.

Table 5.1 Correlation algorithm

Input data of the algorithm*:*

- $G = (V, E)$: correlation graph where *V* is the set of vertices that represent the SNMP objects and *E* is the set of edges that explicit their relationships;
- O_i *:* set of initial objects of the three flows;
- O_f *:* set of final objects of the three flows;
- *a*: alarm sent to the *Alarm system*;
- S *:* stack used in the depth search algorithm;

Output data of the algorithm:

- anomaly notification that includes the anomaly behavior map shown in subgraph $g \in G$;

Functions:

- $C(o)$ *:* function that returns the set of objects correlated to object *o;*
- $F(a)$*:* function that identifies the flows related to alarm *a* and returns the set of objects belonging to these flows;

```
/*main program*/
begin
   Correlation system receives alarm a;
   for each o ∈ (O_i ∩ F(a)) do
      depthFirstSearch(o);
end;
```

```
procedure depthFirstSearch(o)
begin
  mark o as visited;
  push o on the stack S;
  if ( o ∈ O_f ) then
      send anomaly notification;
  for each (o' ∈ C(o)) do
    begin
       if o' not marked then
          depthFirstSearch(o');
    end for;
  pop S;
end;
```

Figure 5.5 shows the rates of the anomalies correctly detected calculated according to equation (3). Only the months of July and December for S_1 and July and September for S_2 presented a detection rate under 85%. The other results in figure 5.5 present rates near 90%, which indicates the effectiveness of the *Anomaly Detection System*.

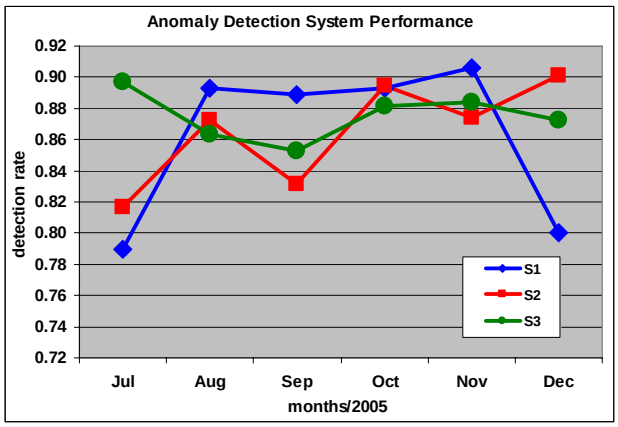

Figure 5.5 Detection rate of *Anomaly Detection System* for S_1, S_2 and S_3

Figure 5.6 shows the rate of false positives calculated with equation (4). All the rates of false positives found are under 4%. Element S_2 presents various incidences of short-duration traffic peaks that can lead the *Anomaly Detection System* to generate false positives. Elements S_1 and S_3 do not present so many occurrences of this type and for this reason their rates of false positives are in general lower than those presented by S_2. This difference of behavior between the network elements analyzed did not influence the detection rates presented in figure 5.5.

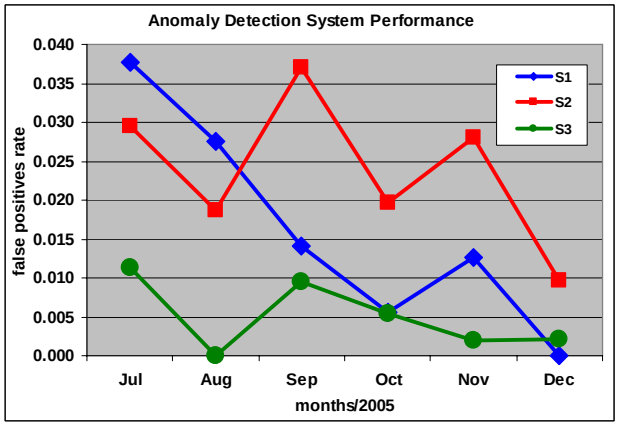

Figure 5.6 False positives rate of *Anomaly Detection System* for S_1, S_2 and S_3

The results obtained indicate that the *Anomaly Detection System* is able to adapt to the different network elements presenting low rates of false positives and high rates of successful detection.

The amount of anomalies found in each of the three data flows in a network element is closely related to the characteristics of its operation. S_1 is a firewall that concentrates its operations in filtering and forwarding packets. For this reason, most of the anomalies detected in S_1 were present at the *forwarding flow*. S_2, which is responsible for final user services through TCP connections and concentrates its operations on the application layer, had its anomalies detected in the *input* and *output flows*. Finally, S_3 is a router and therefore offers services that are important from the operational point of view and that are transparent to the final user. Its main function is related to data forwarding and it is performed at the *forwarding flow*, where most of the anomalies for this element were detected. The proportions of anomalies found in each flow for the network elements are presented in table 5.2.

Table 5.2 Classification of anomalies occurred during the second semester of 2005

	Input flow	**Output flow**	**Forwarding flow**
S_1	0.00	0.04	0.96
S_2	0.50	0.50	0.00
S_3	0.03	0.02	0.95

Figure 5.7 presents the graphics related to the occurrence of an anomaly at S_1 *output flow*. There was a great behavior deviation in three SNMP objects: *ifOutOctets*, *ipOutRequests* and *udpOutDatagrams*. The *Alarm system* generated alarms that were sent to the *Correlation system*, which executed the search at the correlation graph and detected the occurrence of the anomaly at the *output flow*. The initial object of the search at the correlation graph was *udpOutDatagrams* and the final object was *ifOutOctets*. The notification sent to the network administrators informed the SNMP objects involved, building an anomaly behavior map. Considering that the anomaly is at the *output flow*, it was possible to conclude that S_1 was injecting anomalous traffic at the network and could be causing the anomalies that would be detected in other network elements.

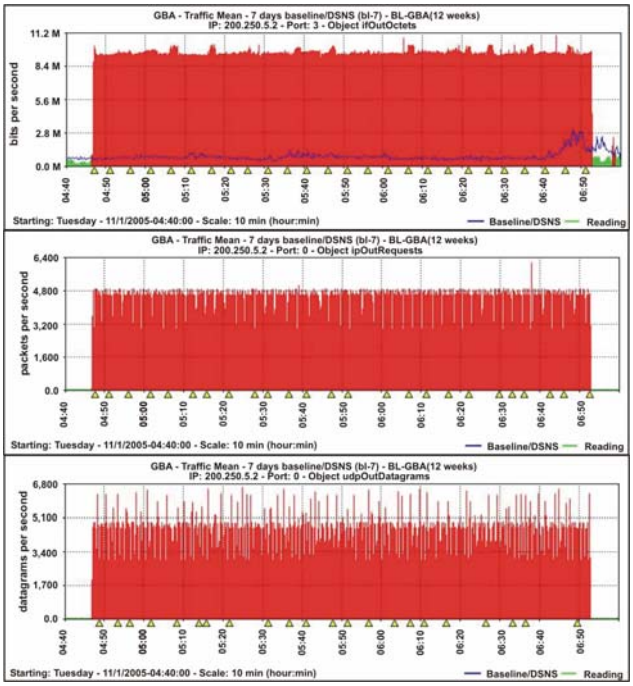

Figure 5-7 Anomaly detected for *output flow* at S_1, Firewall

6. Conclusions

This work reconfirms such as in [10] and [11] that the DSNS generated by the BLGBA model presented good results for traffic characterization, thus accomplishing their main purpose, which is the creation of baselines for various network elements. The effectiveness of the traffic characterization is essential for a good throughput of the anomaly detection system, since it is the first and fundamental step that must be accomplished in this kind of system.

It was possible to observe that the behavior of SNMP objects is intimately related to the characteristics of its operations. At elements S_1 and S_3 that deal with packets forwarding, the anomalies have appeared most of the times in objects related to the *forwarding flow*. At element S_2, which offers services to the final user and whose actions are concentrated in the application layer, the anomalies appeared at the SNMP objects belonging to the *input* and *output flow*.

The good results presented by the rates of false positives and of detection in the three elements analyzed show that the *Anomaly Detection System* is able to adapt to network elements with different characteristics maintaining a good performance. Besides, it is possible to conclude that the system carries out its function effectively, notifying the network administrators about the occurrence of unexpected movements in the traffic. The notifications sent present, among other information, a map of the anomaly behavior obtained from the correlation graph, which facilitates the intervention of the network administrators on the problem.

The method presented here fulfilled an important requirement that had not been approached in [17]: to offer additional information to the network administrator to facilitate the search of origin and solution of the problem. The correlation graph proposed in this paper was responsible for this gain related to the semantic of notifications sent to network administrators.

Future works include increasing the variety of SNMP objects monitored for each one of the MIB-II groups approached in this work, always searching for the behavior correlation between them. The inclusion of SNMP objects related to the packets discard and to errors can enhance even more the diagnosis offered by the tool. The other step is related to the localization of the origin of theses anomalies, facilitating the determination of the cause and solution of the problem.

7. Acknowledgements

Our thanks to The State of São Paulo Research Foundation (FAPESP) that supports this work.

References

[1] Z. U. M. Abusina, S. M. S. Zabir, A. Ashir, D. Chakraborty, T. Suganuma and N. Shiratori. “An Engineering Approach to Dynamic Prediction of Network Performance from Application Logs”. International Journal of Network Management, v. 15, p. 151-162, feb. 2005

[2] J. B. D. Cabrera, L. Lewis, X. Qin, W. Lee, R. K. Prasanth, B. Ravichandran, R. K. Mehra. “Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables – A Feasibility Study”. Integrated Network Management Proceedings, 2001 IEEE/IFIP International Symposium on, p. 609-622, 14-18 maio 2001.

[3] J. L. Gersting “Mathematical Structures for Computer Science”. 5 ed., W H Freeman, 2002.

[4] H. Hajji “Baselining Network Traffic and Online Faults Detection”. IEEE International Conference on Communications, 2003 (ICC '03). v.: 1, p. 301-308, may 2003.

[5] J. Jiang, S. Papavassiliou “Detecting Network Attacks in the Internet via Statistical Network Traffic Normally Prediction” Journal of Network and Systems Management, v. 12, p. 51-72, mar. 2004.

[6] B. Krishnamurthy, S. Sen, Y. Zhang, Y. Chen. “Sketch-based change detection: methods, evaluation, and applications”, Internet Measurement Workshop Proceedings of the 2003, ACM SIGCOMM conference on Internet measurement; Miami Beach, Pages: 234 – 247, ISBN:1-58113-773-7.

[7] Lakhina, M. Crovella, C. Diot "Diagnosing Network-Wide Traffic Anomalies". ACM SIGCOMM Computer Communication Review, Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications, v. 34, p. 219-230, aug 2004
[8] J. Li, C. Manikopoulos. "Early Statistical Anomaly Intrusion Detection of DOS Attacks Using MIB Traffic Parameters." Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, p. 53-59, jun. 2003.
[9] K. McCloghrie, M. Rose "Management Information Base for Network Management of TCP/IP-based internet: MIB-II". RFC 1213, mar 1991.
[10] M. L. Proença Jr., B. B. Zarpelão, L. S. Mendes. "Anomaly Detection for Network Servers using Digital Signature of Network Segment". IEEE Advanced Industrial Conference on Telecommunications 2005, Lisbon, Portugal, week of 7/17/2005. Advanced ICT Proceedings.
[11] M. L. Proença Jr., C. Coppelmans, M. Bottoli, L. S. Mendes. "The Hurst Parameter for Digital Signature of network Segment". 11th International Conference on Telecommunications (ICT 2004), 2004, Fortaleza. Springer-Verlag in the LNCS series. p. 772-781 aug 2004.
[12] M. Roughan, T. Griffin, Z. M. Mao, A. Greenberg, B. Freeman "IP Forwarding Anomalies and Improving their Detection Using Multiple Data Sources" Proceedings of the ACM SIGCOMM workshop on Network troubleshooting: research, theory and operations practice meet malfunctioning reality, p. 307-312, sep. 2004.
[13] V. A. Siris, F. Papagalou. "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks". IEEE Communications Society Globecom 2004. p. 2050-2054.
[14] Soule, K. Salamatian, N. Taft. "Combining Filtering and Statistical Methods for Anomaly Detection". Proceedings of ACM SIGCOMM Internet Measurement Conference 2005 (IMC'05), p. 317-330, October 19-21, 2005, Berkeley, CA, USA.
[15] W. Stallings "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, 3". Addison-Wesley, 1998.
[16] M. Thottan, C. Ji "Anomaly Detection in IP Networks" IEEE Transactions in Signal Processing, v. 51, n. 8, p. 2191-2204, aug. 2003
[17] B. B. Zarpelão, M. L. Proença Jr., L. S. Mendes. "Anomaly Detection Aiming Pro-Active Management of Computer Based on Digital Signature of Network Segment". 4th IEEE Latin American Network Operations and Management Symposium, Porto Alegre, Brazil, August 29-31, 2005. Lanoms Proceedings.
[18] Y. Zhang, Z. Ge, A. Greenberg, M. Rhoughan. "Network Anomography". Proceedings of ACM SIGCOMM Internet Measurement Conference 2005 (IMC'05), p. 317-330, October 19-21, 2005, Berkeley, CA, USA.

Bruno Bogaz Zarpelão received his B.S. degree in Computer Science from State University of Londrina, Brazil. He is currently pursuing his Ph.D. in Electrical Engineering at School of Electrical and Computer Engineering from State University of Campinas, Brazil. His research interests include Computer Network Management and Operations and Anomaly Detection using SNMP and MIB-II.

Leonardo de Souza Mendes received his B.S. degree in 1985 from the Gama Filho University, Rio de Janeiro, his M.S. degree in 1987 from the Catholic University of Rio de Janeiro, and his Ph.D. degree in 1991 from Syracuse University, all in Electrical Engineering. In 1992 he joined the School of Electrical Engineering of the State University of Campinas, Brazil. Prof. Mendes's recent R&D focus is in the studies and development of Communications Engineering applications for metropolitan IP networks. Prof. Mendes created, at UNICAMP, the Laboratory of Communications Network (LaRCom), from which he is now the Director and also the main coordinator. At LaRCom , Prof. Mendes and his group have developed or are developing the following projects: 1) an optical system simulator to help in the analysis of optical networks; 2) an environment for the simulation of systems using event driven technique which allows the development of ATM, IP and CDMA simulators; 3) development of Internet set top boxes using J2ME for small devices; 4) communications description of Internet devices using CORBA component modules for Telecommunications; 5) development of e-Learning objects for the PGL project.

Mario Lemes Proença Jr. received his M.Sc degree in Computer Science from the Computer Science Institute of Federal University of Rio Grande do Sul, Porto Alegre, Brazil, in 1998 and his Ph.D. degree in Electrical Engineering from School of Electrical and Computer Engineering of State University of Campinas, Brazil in 2005. Also, he is a computer science professor since 1991 in State University of Londrina, Brazil. His research interests include Computer Network, Network Operations and Management and Security. He currently is leader of the group of research in computer networks of Computer Science Department of State University of Londrina.