Anomaly Detection Aiming Pro-Active Management of Computer Network Based on Digital Signature of Network Segment*

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

[1] State University of Campinas (UNICAMP) – School of Electrical and Computer Engineering (FEEC) – Communications Department – Campinas, SP, Brazil.
{bzarpe, lmendes}@decom.fee.unicamp.br
[2] State University of Londrina (UEL), Computer Science Department, Londrina, PR, Brazil.
{proenca}@uel.br

Abstract. Detecting anomalies accurately is fundamental to rapid problems diagnosis and repair. This paper proposes a novel anomaly detection system based on the comparison of real traffic and DSNS (Digital Signature of Network Segment), generated by BLGBA model, within a hysteresis interval using the residual mean and on the correlation of the detected deviations. Extensive experimental results on real network servers confirmed that our system is able to detect anomalies on the monitored devices, avoiding the high false alarms rate.

1 Introduction

Computer networks lately appear as an important base of information technology. They form systems that go under constant evolution and are composed of devices such as routers, switches and software from different natures. These factors turned the networks management into a challenging task for human operators leading to a demand for automation of many management functions [3][13][16].

Nowadays many services are offered to the users integrated to the network, using data, voice and video transmission. This fact is contributing for an increasing probability of occurrence of anomalies of many different types. These anomalies became very common and can be caused by servers' overload, Denial of Service and worm attacks, equipment failures, software bugs, and configuration errors among others [4][7][14][16].

In this context, the existence of a pro-active approach for management is essential, so that these problems can be detected and solved in the fastest way possible, avoiding the anomalies to cause grave consequences to the execution of the services offered by the network. Anomaly detection is thus a fundamental point to reliability assurance, which is a common goal to most of the networks [1][13][14].

* This work was made with support of CNPq

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 movement. The detection is accomplished by searching for significant behavior changes that are not coherent with the previously established profile [4][6][10][13][16][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 [3][10][16]. This work deals with the employment of the BLGBA (Baseline for Automated Backbone Management) model proposed by Proença *et. al.* [11][12], for the calculation of the DSNS (Digital Signature of Network Segment) to detect anomalies as a suggestion to solve this issue.

DSNS can be defined as a set of basic information that constitutes the traffic profile of a segment or a server. This information includes data such as traffic volume, number of errors, types of protocols and the services that are carried along the segment or server during the day [11][12].

Even with a reasonably effective traffic characterization there is still another difficult to solve issue on the anomaly detection: which behavior deviations must be taken as anomalies? The difficulty to answer this question resides on the non-stationary behavior of the network traffic. 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 when comparing real traffic with the profile established by the DSNS.

The anomaly detection system presented at this work is based on the comparison of the real traffic with the DSNS in a hysteresis interval, on the residual mean resulting from this comparison and on the later correlation of the behavior deviations detected in each SNMP object. The idea is to notify the network administrator only about the events that really present some risk to the services reliability.

The results of the employment of this system at the network servers of the State University of Londrina will be presented as well as a case study about the occurrence of a specific class of anomalies named flash crowd.

This work is organized as follows: Section 2 presents some work related to the anomaly detection area. Section 3 describes the servers used to obtain the results. Section 4 deals with the concepts about the BLGBA model and DSNS. Section 5 will present the anomaly detection system and the results of its application to the previously described servers. 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. Recently the need for detecting unknown anomalies caused the method addressed at this paper, based on the characterization of traffic normal operations, to be present in various works such as [1][3][4][7][14][16][17].

The need for an effective traffic characterization for successful anomaly detection was addressed by Hajji [3]. The traffic characterization model presented at his work requires the dataset used as history when establishing the traffic profile to be pure. The BLGBA model used in this work presents as an advantage the absence of this kind of requirements.

The properties of the SNMP protocol (Simple Network Management Protocol) and of MIB-II (Management Information Base) were explored by Thottan *et. al.* [16] who has used the behavior correlation of some SNMP objects face to anomalies aiming to increase the effectiveness of his anomaly detection mechanism. In [2] was presented the possibility to detect Distributed Denial of Service attacks by using data coming from the SNMP objects. This work also uses the SNMP protocol and searches for a correlation on the behavior of some SNMP objects found at the MIB-II, addressing also a SNMP object related to the TCP protocol which is not present at Thottan *et. al.* [16].

Roughan *et. al.* [14] worked with another source of data besides the SNMP protocol: the routing protocol BGP (Border Gateway Protocol). From the correlation of behavior deviations found at both data sources he showed a reduction on the false positives rate.

Lakhina *et. al.* [7] analyzed anomalies based on a study of packets flow samples. This work has discovered the need for a complete diagnosis of anomalies, which includes besides their detection, the localization of their origin aiming to facilitate the determination of the cause and consequently of the solution of problems.

There are some works related to the class of anomalies named flash crowd, to which a case study will be presented in section 5, such as [1] and [7], that try to characterize it and present its effects on the networks. Jung *et. al.* [5] have studied the flash crowd anomalies and the Denial of Service attacks presenting the similarities and differences between them and the impact caused on the services provided by websites.

3 Servers Studied

Aiming for concrete results about the proposals in this work, a real environment was used to test the system. The network servers from the State University of Londrina used in the tests were:

- S_1: is the firewall from the State University of Londrina network and it gathers a traffic of approximately 3000 computers to the Internet;

- S_2: is the main Web server from the State University of Londrina;
- S_3: is the proxy server from the State University of Londrina and it interconnects its 3000 computers to the Internet;

The following SNMP objects present in MIB-II [9] were monitored in our studies: ifInOctets (determines the number of bytes received by certain interface of the device monitored), ipInReceives (determines the number of IP packets received by the device) and tcpInSegs (determines the number of TCP segments received by the device).

4 BLGBA Model and DSNS

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.

The BLGBA (Baseline for Automated Backbone Management) model proposed by Proença *et. al.* [11][12], is responsible for the DSNS (Digital Signature of Network Segment) generation, which can be useful for different function inherent to the network management, including anomaly detection.

This model performs a statistical analysis of the history of data collected in the SNMP objects, taking into account the exact moment of the collection. The period of this history can range from 4 to 12 weeks and the generation of DSNS is performed for each second of the day, every day of the week. As a result, we have the *bl-7* type DSNS, which has an individual behavior profile for each day of the week. This approach is much closer from the ideal since it is possible to identify different behaviors on the network movement for each day of the week. More detail about the BLGBA model and DSNS can be found at [11][12].

Aiming to illustrate the use of the DSNS generated by the BLGBA model, figure 4.1 contains the weekdays of a whole week monitoring server S_1 with its DSNS. The blue line in the graphics represents the movement levels expected from the estimative found at the DSNS. The green indications show that real traffic is below the DSNS and the red ones mean it overcame the DSNS, which can represent an anomalous event or not.

5 Anomaly Detection

Different answers have already been presented to the issue on which situation characterize an anomaly and must be reported to the network administrator. Thottan *et. al.* [16] used to treat as anomaly only the events that resulted in interruption of the service. Lakhina *et. al.* [7] highlighted the need to detect events that can degrade the quality of the service even when it is not interrupted. Roughan *et. al.* [14] has also related the existence of some events that despite not resulting in extreme

consequences to the network needed verification. This work searches to detect the significant behavior deviations and correlate them, alerting the administrator about situations that can generate from degradation to interruption of services.

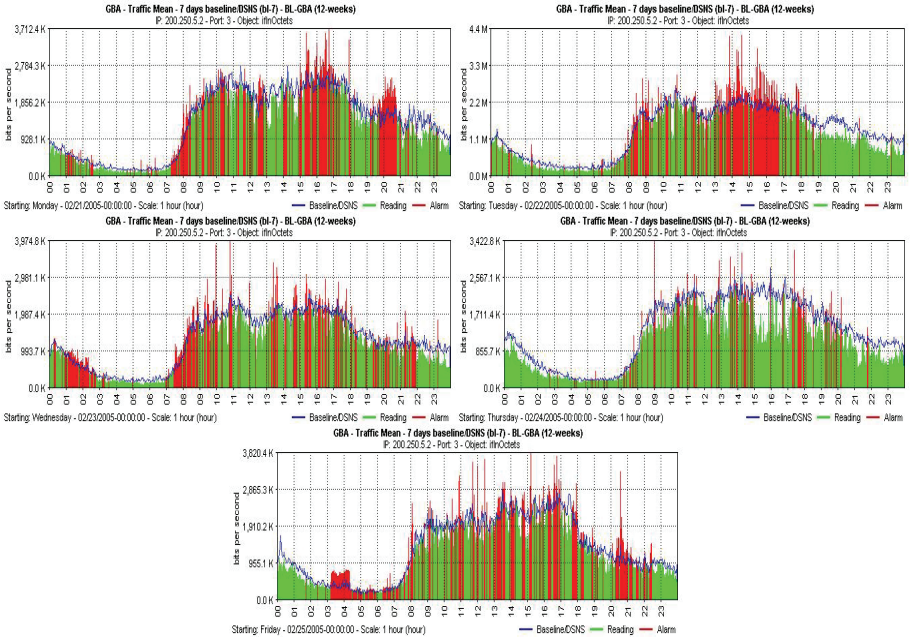

Fig. 4.1 Real traffic and DSNS at S_1, ifInOctets

Considering that, our first objective at this step of the work will be to identify among all the data obtained through certain SNMP object, which are deviating from the normal behavior established by the DSNS. The key point to our approach is the correlation of the deviations detected in different SNMP objects, which will point out whether an anomaly is happening or not.

Figure 5.1 presents the reference model of the *Anomaly detection system*. It is possible to notice that the GBA tool (Automated Backbone Management) [12] is responsible for the collection of samples and generation of the DSNS. The *Alarm system* performs the comparison between the real traffic and the DSNS, reporting through alarms the deviations detected. The *Correlation system* is in charge of assembling all these alarms and verifying the occurrence of anomalies.

The alarms are generated when the three facts bellow happen together:

- Fact 1: the real sample analyzed overcomes the limit established by the DSNS.
- Fact 2: the current sample analyzed overcomes the previous sample related to the occurrence of fact 1 in the hysteresis interval *t*.
- Fact 3: the number of occurrences of fact 2 overcomes the value of $\boldsymbol{\delta}$.

The requirement of the occurrence of these three factors to characterize a significant behavior deviation aims to avoid the generation of false positives. With the intention of increasing the mechanism reliability, another variable was inserted in

the context: the mean of the residual resulting from the comparison between the real sample and the DSNS in the interval *t*. Figure 5.2 presents the automaton that represents the functioning of the algorithm to identify the three facts mentioned above.

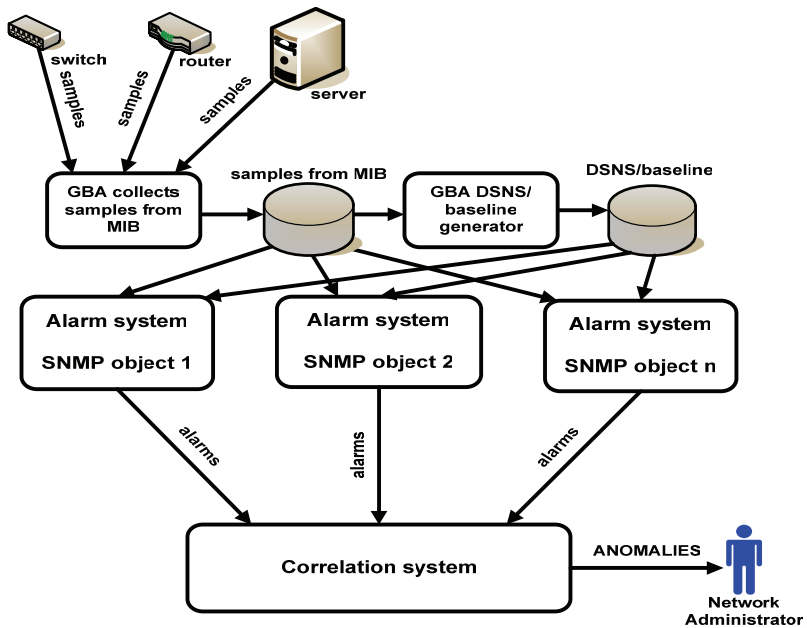

Fig. 5.1 Reference model of the *Anomaly detection system*

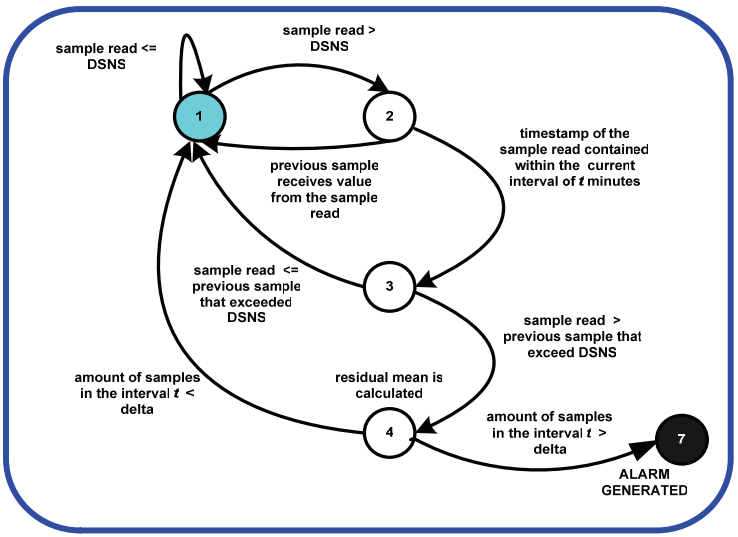

Fig. 5.2 Automaton of the alarms generation system

The time interval *t* can range from 300 to 900 seconds (corresponding to t_{min} and t_{max}, respectively in formula (3) that will be presented lately). The value of δ is within

the range 130 and 390. These conventions were defined after performing many tests in different situations. The value of these parameters varies according to the residual mean calculated within the interval *t*, in such a way that the smallest the residual mean is, the greater the analysis interval will be and the more rigid the parameters for alarm generation will be. The objective is to force the *Alarm system* to analyze the less incisive deviations for a greater period of time to attest that they should actually be notified.

The residual are normalized according to formula (1) where *sample(i)* and *DSNS(i)* represent the values of the real sample and the value of the DSNS respectively, related to the instant *i* when fact 2 happens.

$$residual(i) = \frac{sample(i)}{DSNS(i)} - 1 \quad (1)$$

The residual mean is calculated for each of the *n* occurrences of fact 2 while *n* is smaller than $\boldsymbol{\delta}$. The formula that determines the mean is as follows:

$$mean = \frac{\sum_{i=1}^{n} residual(i)}{n} \quad (2)$$

Formula (3) determines the value of the interval *t*, using the residual mean calculated:

$$t = t_{\max} - \left[\left(\frac{mean}{mean_{\max}} \right) * \left(t_{\max} - t_{\min} \right) \right] \quad (3)$$

Formula (3) is only used when the mean value is smaller than 5 ($mean_{\max}$). Otherwise, *t* and $\boldsymbol{\delta}$ will assume the minimum values possible, which are 300 and 130 respectively. The variation of $\boldsymbol{\delta}$ is based on the variation of *t*.

The value of $mean_{\max}$ was found when analyzing the daily mean of the residual distribution for six months in all the servers studied. An example of a result of this analysis is presented in figure 5.3. It is possible to observe that the residual values presenting a higher frequency belong to the 0 to 5 range. This fact was observed in all the servers analysed.

Figure 5.4 will present a real case of behavior deviation detection accomplished by the *Alarm system*. The event happened during the day in February 25th 2005 for the ifInOctets object of S_1. At the upper area of the figure, it can be observed the graphic that shows the behavior of the whole day, highlighting the deviation occurred. At the bottom area, the deviation is presented in a highlighted way, where it is possible to observe its course and the alarms generated after the system verifies the intensity of the sudden change detected.

Figure 5.5 presents the daily alarms mean generated for the servers S_2, objects ifInOctets, ipInReceives and tcpInSegs and S_3, objects ipInReceives and tcpInSegs in the second semester of 2004.

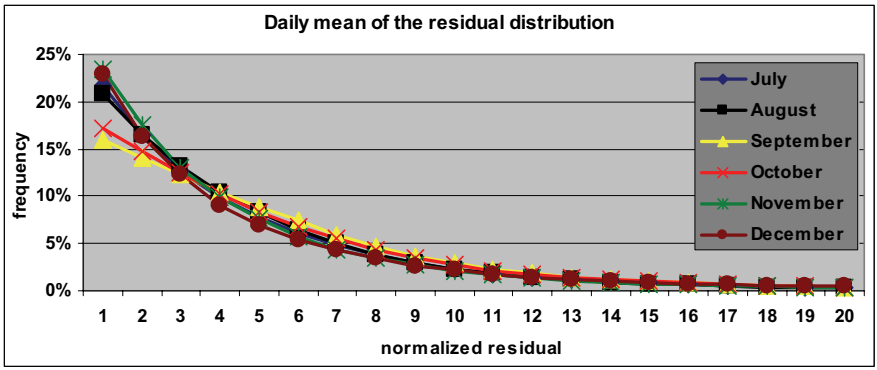

Fig. 5.3 Distribution of residual for S_1, ifInOctets

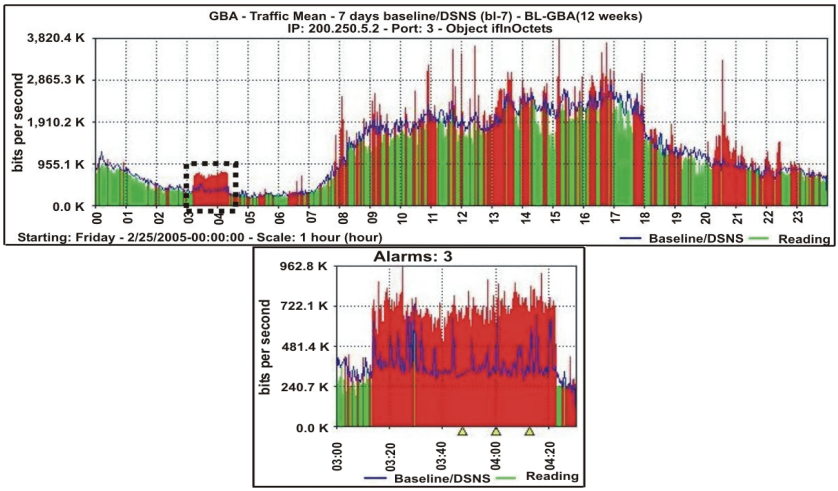

Fig. 5.4 Deviation detected and consequent alarms generated

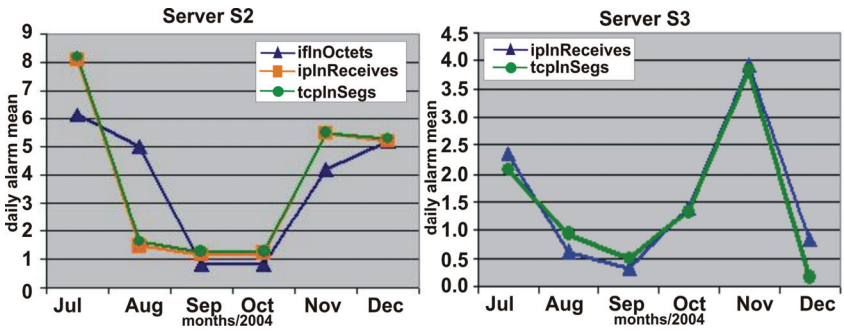

Fig. 5.5 Daily alarm means for S_2 and S_3

These graphics show that the daily alarm means in different objects are similar for all the months. At S_2, the means of ipInReceives and tcpInSegs are so similar that their curves in the graphic overlap each other. These results indicate that the alarms are generated in different objects for the same situations leading to the conclusion that there is a correlation on the behavior of theses objects face to the anomalies. It was possible to notice at the three servers that most of the anomalies are reflected in the movements of at least two of the objects analyzed. This phenomenon occurred mostly in servers S_2 and S_3, whose clients established TCP connections due to the nature of the services used, and where there is a strong correlation between the objects ipInReceives and tcpInSegs. Particularly for S_2 server, the object ifInOctets has also presented correlation to the objects ipInReceives and tcpInSegs. S_1 also has many correlated events, but it is possible to realize that anomalies arise in different ways for each object. They are usually more easily perceptible at the ifInOctets object and appear in a more discrete way at ipInReceives.

Based on these conclusions a simple and effective correlation rule was formulated. The anomaly is detected when alarms are generated in more than one SNMP object at the same time interval *t*. This rule is also based on the fact that it is very unlikely that a false alarm arises simultaneously in more than one SNMP object.

A case study will be present to illustrate the functioning of the *Anomaly detection system*. This case study will describe the scenario corresponding to an anomaly named flash crowd, which has occurred at server S_2.

Flash crowd type events are characterized by the arise of an unusual demand for a specific service resulting into an increase of the server workload, restricting the ability of the links involved, leading to a considerable increase in the packets loss and causing a network congestion. One of the most famous cases of this anomaly happened during the terrorist attacks on September 11th 2001 in the United States, when at many news portals, such as www.cnn.com, the number of accesses increased in a very fast way leading to the unavailability of many services. This class of anomalies presents some characteristics similar to those of the Denial of Service attacks. The first difference resides on the nature of the accesses, which are legitimate at the flash crowd whereas malicious at the Denial of Service attacks.

In our case, the anomaly happened due to the announcement of the results of the admission examination from the State University of Londrina at their website, overloading their main Web server (S_2). The anomaly has started just before 2 o'clock in the afternoon, when the results were announced, and it ended around 2:25 pm. It is possible to observe at figure 5.6 that the first alarms were generated by the *Alarm system*, for tcpInSegs around 2:05 pm and for ipInReceives very soon after that. The *Correlation system* received the two alarms generated for the different objects and verified that they belonged to the same hysteresis interval. Thus, the *Correlation system* caused the *Anomaly detection system* to indicate the occurrence of the anomaly about 5 minutes after it has started and notify the network administrator. Both objects have reacted to the anomaly in a very similar way, as already verified in other situations, and this fact confirms the great correlation existent between them.

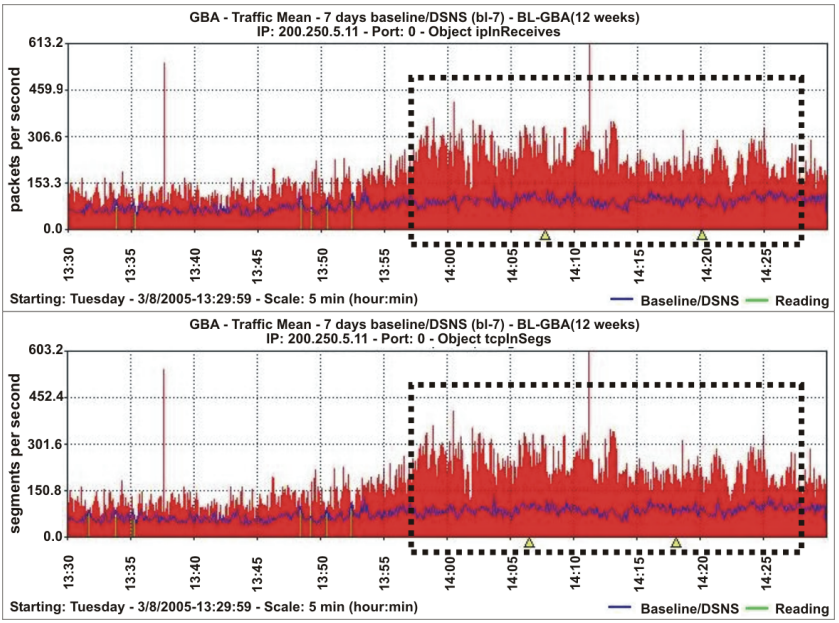

Fig. 5.6 Flash crowd type anomaly ocurred in server S_2

6 Conclusions

This work has enabled us to once again confirm that, as well as in [11] and [12], the DSNS generated by the BLGBA model present good results when characterizing the traffic using the SNMP objects belonging to three different groups of the MIB-II (interface, IP and TCP) for all the servers studied in this paper. The effectiveness approach was essential for the success of the *Anomaly detection system*, since the traffic characterization is the first fundamental step to detect anomalies.

Besides helping on the reduction of false positives, the use of the residual mean to detect anomalies has provided the system with another good characteristic. The frequency and the number of alarms generated for one deviation were intimately connected to the residual mean enabling the determination of how discrepant the event was from the simple analysis of these properties of the alarms.

The correlation of behavior of the SNMP objects face to anomalies was observed. At those servers with TCP connections, S_2 and S_3, the movement of data referent to the ipInReceives and tcpInSegs objects is highly correlated. At S_1, the two object monitored (ifInOctets and ipInReceives) have reacted to the anomalies in most of the case even if in different ways.

Future works include increasing the variety of SNMP objects monitored for each one of the MIB-II groups approached at this work, always searching for the behavior correlation among them in order to reduce even more the false positives. The other

step is related to the localization of the origin of theses anomalies, providing a more complete diagnosis to facilitate the determination of the cause and solution of the problem.

References

[1] P. Barford, J. Kline, D. Plonka, A. Ron ***A Signal Analysis of Network Traffic Anomalies***. Proceedings of the ACM SIGCOMM Internet Measurement Workshop (IMW'02), p. 71-82, nov. 2002

[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 may 2001.

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

[4] 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.

[5] J. Jung, B. Krishnamurthy, M. Rabinovich. ***Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDN's and Web Sites***. Proceedings of the eleventh international conference on World Wide Web. p. 293-304, may 2002

[6] B. Krishnamurthy, S. Subhabrata, Z. Zhang, Y. Chen ***Sketch-based Change Detection***: ***Methods, Evaluation and Applications***. Proceedings of the 3rd ACM SIGCOMM Internet Measurement Conference (IMC'03), p. 234-247, oct. 2003.

[7] A. Lakhina, M. Crovella, C. Diot ***Characterization of Network-Wide Traffic Anomalies in Traffic Flows***. Proceedings of the 4th ACM SIGCOMM conference on Internet Measurement Conference (IMC'04), p. 201-206, oct. 2004

[8] A. 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

[9] K. McCloghrie, M. Rose ***Management Information Base for Network Management of TCP/IP-based internet: MIB-II***. RFC 1213, mar 1991.

[10] C. C. Michael ***Finding the Vocabulary of Program Behavior Data for Anomaly Detection*** Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03), p. 2-12, 2003

[11] M. L. Proença Jr., C. Coppelmans, M. Bottoli, A. Alberti, 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. L. Proença Jr., C. Coppelmans, M. Bottoli, L. S. Mendes ***Baseline to Help With Network Management***, ICETE 2004 – International Conference on E-business and Telecommunication Networks, Setubal – Portugal – 24-28 aug. 2004. Proceedings of ICETE, INSTICC Press, ISBN 972-8865-15-5.

[13] X. Qin, W. Lee, L. Lewis, J.B.D. Cabrera ***Integrating Intrusion Detection and Network Management*** Network Operations and Management Symposium, 2002., p. 329-344, april 2002

[14] 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.

[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] N. Wu, J. Zhang ***Factor Analysis Based Anomaly Detection*** Proceedings of the 2003 IEEE, Workshop on Information Assurance, p. 108-115, jun. 2003.