Detecting computer network attacks using statistical discriminators and cluster analysis

Raimir Holanda
Professor University of Fortaleza raimir@unifor.br

José Everardo Bessa Maia
Professor University of Fortaleza jmaia@unifor.br

Marcus Fábio Fontenelle do Carmo
Master Degree student at University of Fortaleza.
marcusfabio@edu.unifor.br

Resumo

Ataques representam uma séria ameaça ao ambiente computacional em rede e, portanto, precisam ser prontamente detectados. Novos tipos de ataque, os quais os sistemas de detecção não estão cientes, são os mais difíceis de detectar. Atualmente os métodos disponíveis são principalmente baseados em assinaturas ou algoritmos de aprendizagem e geralmente não são capazes de detectar novos ataques. A abordagem apresentada neste trabalho utiliza-se de um pequeno número de discriminantes estatísticos e análise de agrupamentos para detectar ataques em redes de computadores, obtendo resultados melhores do que resultados previamente obtidos em outros trabalhos. Análise de agrupamento é uma técnica não supervisionada e, portanto, é capaz de detectar novos ataques. Nós realizamos testes empíricos utilizando *traces* reais.

Palavras-chave*: Segurança em redes de computadores. Gerenciamento de dados. Segurança de dados. Detecção de intrusos. Estatística multivariada.*

Abstract

Attacks represent a serious threat to a network environment, and therefore need to be promptly detected. New attack types, of which detection systems may not even be aware, are the most difficult to detect. Currently, the available methods are mainly based on signature or learning algorithms and generally cannot detect these new attacks. The approach presented here uses a small number of statistical discriminators and cluster analysis to detect attacks, obtaining results which are better than the results found in previous papers. Cluster analysis is an unsupervised technique and, therefore, it is able to detect new attacks. We performed an empirical test using real traces.

Keywords**:** *Computer network security. Communication and information security. Data management. Data security. Site security monitoring.*

1 Introduction

Many efforts have been dedicated to research on computer network security. This fact occurs due to the increasing dependence on computer networks by people, companies and governments. Computer network attacks can imply in different levels of threats, from loss of privacy to financial damages. An attack can be considered, therefore, as the use of a network with the purpose of damaging the information stored or carried in it.

The goal of any method of attack detection consists in building a system that automatically monitors the events in a network and detects when the attacks will happen. Once the attack is detected, the system can set off an alarm and corrective measures can be applied. There are many approaches in literature for attack detection, for instance, detections based on signatures, behavior, machine learning, anomalies, and on multivariate statistical properties.

The detection methods based on signatures gather data from the network and detect the attacks using known sequences of data that are in the payload of packets. Such methods are inefficient because of their lack of awareness of new types of attacks, because they present serious limitations related to data privacy that are passing through the network and because signatures are not available for all types of attacks.

A second approach uses a mass of data with previously identified attacks to train learning algorithms about attack behavior. This approach presents the advantage that the algorithm can be re-trained to learn about new types of attacks. However, we have to insert new attack instances into the training file and, after the automatic reorganization of their set of rules, the method would be ready to detect new attacks.

The two approaches presented above have serious limitations because both of them require that the attacks are previously known and, therefore, new types of attacks will not be detected. The same problem appears using machine learning technique. To overcome these limitations, other approaches have been applied.

The anomaly detection method identifies unusual behavior in data, in other words, it detects deviations from behavior that is considered normal. This approach presents a great advantage, namely the possibility to detect known attacks and new ones because new attacks will produce unusual behavior in the network traffic.

Usually, anomaly detection methods require a set of clean data, that is, one without the occurrence of attacks, so that we can be aware of what is normal behavior of the network traffic.

This project is based on multivariate statistical methods to attack detection. The presented approach uses a small number of statistical discriminators and cluster analysis to detect attacks with better results than those found in previous papers. Cluster analysis, which is an unsupervised technique, allows that new attacks be detected. The method presented was validated using real traces.

In section 2 we present the main papers that have been recently published related to attack detection. In section 3, we describe the data used to validate our attack detection proposal. We used real data where the attack flows were previously identified. A description of the methodology used in attack detection is presented in section 4 and we describe in detail how we apply the cluster analysis method to the problem of attack detection. Section 5 presents and discusses the final results and finally in section 6 we show the main conclusions and future research.

2 Related work

Attack detection has received a lot of attention in the last few years and has come to be considered an important research area. Many published papers about identification and attack detection are focused on specific types of attacks such as *DOS attacks* (HUSSAIN et al., 2003), *port scan* (JUNG, 2004) and *worms* (KIM and KARP, 2004), (SCHECHTER et al., 2004).

A widely used approach to detect such attacks has been to consider anomalies such as bulk traffic deviations (BARFORD et al., 2002), (BRUTLAG, 2000), (LAKHINA et al., 2005), (ROUGHAN et al., 2004). In (LAKHINA et al., 2004a) anomalies in backbone networks are analyzed using the amount of bytes passing through a link and in (LAKHINA et al., 2004b) the data are analyzed using the bulk traffic among Origin-Destination (OD) flows. The anomaly detection approach based on bulk traffic has been very successful in identifying changes in traffic behavior, such as attacks known as *bandwidth flooding attacks.* However, there are many anomaly classes that do not produce meaningful changes in bulk traffic. Other approaches have been used based on pattern correlation exploration among different variables from SNMP MIB (THOTTAN and JI, 2003), or based on heuristics to identify specific anomaly types into packet IP flows (KIM et al., 2004).

In (PORTNOY et al., 2001), the authors present an automatic intrusion detection method that shows the possibility of detecting new attacks. However, this method is applied to a small range of attacks. Anomaly based methods have shown high efficiency because of their low operation cost in the network (TAYLOR and ALVES-FOSS, 2000). Using real traces, (TAYLOR and ALVES-FOSS, 2001) present an analysis of unusual traffic events.

More recently a supervised machine learning technique based on a Bayesian neural network were used to train data with categories derived from packet information providing classification without access to the contents of packets (AULD et al., 2007). In (AULD et al., 2007) were obtained about 90% of accuracy in traffic classification.

Most of the methods presented above use metrics based on bulk traffic. We believe, however, that all of them have a limited reach in attack detection because they do not have a complete set of information to define unusual traffic behavior.

On the other hand, we consider that methods capable of individually examining statistical flow properties are more efficient.

3 Traces description

Any work on attack identification requires the use of data. To evaluate the proposed methodology and the selected discriminators were used a set of pre-processed traffic traces. The method of data collection is described in (Moore et al. 2003), having been used the data available in (Moore et al. 2005). These data were collected from a network with 1,000 users connected through a full-duplex Gigabit Ethernet Internet connection and based on a 24-hour period. Ten archives were created, each one related to a period of 1,680 seconds (28 minutes) and available to the scientific community. The traces were used in (Moore e Papagiannaki 2005), (Moore et al. 2005), (Zuev e Moore 2005) e (Auld et al. 2007). At pre-processing for each collected flow was identified an application which the flow was associated. Table (1) shows the applications found into traces and their respective classes.

Table I: Classes and applications

Classes	Aplications Found into Traces
BULK	ftp
DATABASE	postgres, sqlnet oracle, ingres
INTERACTIVE	ssh, klogin, rlogin, telnet
MAIL	imap, pop2/3, smtp
SERVICES	X11, dns, ident, ldap, ntp
WWW	www
P2P	KaZaA, BitTorrent, GnuTella
ATTACK	Internet worm and virus attacks
GAMES	Half-Life
MULTIMEDIA	Windows Media Player, Real Player

Using pre-classified traces makes possible the use of a traffic flow subset for training the classification algorithm. After the conclusion of this step, it is possible to use another subset of traffic flows to validate the efficiency of proposed method.

In this paper we used a flow based approach. Flows are identified as a sequence of packets that present the same set of values in the following fields of TCP/IP header: source IP address, destination IP address, source TCP port, destination TCP port and type of protocol.

Our analysis begins from previously processed data from (MOORE et al., 2005). On pre-processing, each collected flow identifies an application in which is associated. In (MOORE et al., 2005) the traffic was classified into the following categories: *Bulk* (ex: ftp), *Database* (ex: postgres, etc), *Interactive* (ssh, telnet), *Mail* (smtp, etc), *Services* (X11, dns), WWW, P2P (ex: KaZaA, etc), *Games* (Half-Life, etc), *Multimedia* (Windows Media Playes, etc) and *Attack* (virus, worm attacks, etc). During the pre-processing, a set of statistics was generated for each flow related to the flow that in (MOORE et al., 2005) is called discriminators. 249 discriminators were generated including simple statistics about the size and packet delay and TCP protocol information, such as *Syn* and *Ack* packet counters.

The statistical information created was gathered from packet header and a content based analysis identification to identify the application classes. Therefore, our analysis begins from the pre-processed data in which a set of statistics and an application class were created for each flow.

4 Methodology

The methodology consists of two steps: discriminator selection and clustering of attack flows. The discriminator selection consists of a difficult and important step in the traffic classification process.

4.1 Discriminator selection

The task of attack detection is, in fact, a classification task. The discriminator selection step that will be used in classification phase is, probably, the most important one. The classification accuracy is directly related to the discriminators chosen for its elaboration. To use the discriminator variables, it is essential that the sampled elements have been measured into the variables that better distinguish the groups. Otherwise, the classification accuracy will be affected. A very common mistake consists of thinking that the bigger the number of discriminators, the better the solution. The discriminator selection methods based on analysis of variance use, basically, two approaches: univariate analysis of variance or multivariate analysis of variance (ANDERSON, 1958). In this project we applied univariate analysis of variance. From the classified trace, each variable is individually and independently examined and its F-Distribution is calculated. The variables are ordered by F-Distribution values and the discriminators are chosen among the biggest values. On univariate analysis of variance a comparison is done through the analysis of variance of each candidate discriminator variable. Those variables with the most significant F-Distribution values are related to the most important variables for discrimination groups and, therefore, considered discriminators.

The F-Distribution uses a ratio of two estimates, the variance mean of intra-group elements and the mean variance on inter-group elements S_w^2 , defined as follows:

$$\text{Ratio F} = \frac{S_b^2}{S_w^2} \tag{1}$$

where,

$$S_b^2 = n\frac{\sum (\overline{x}_j - \overline{\overline{x}})^2}{(k-1)} \tag{2}$$

and

$$S_w^2 = \frac{1}{k(n-1)}\left[\sum (x_i - \overline{x}_1)^2 + \ldots + \sum (x_i - \overline{x}_k)^2\right] \tag{3}$$

with *k* being the number of groups and *n* the number of group samples.

On F-Distribution, there is a different distribution for each *n* sample size combination and *k* samples. The distribution is contiguous between 0 and +∞. Another fact is that large differences between sampling means and small sampling variances can result in large F-Distribution values.

Each F-Distribution value depends on the number of associated freedom degrees. The numerator and denominator have corresponding freedom degrees. The freedom degrees are based on calculations that are necessary to deduce each population variance estimate. For numerator the freedom degree is (*k - 1*) and for denominator the freedom degree is *k*(*n* - *1*).

The multivariate analysis can be carried out by three methods: *forward*, *backward* and *stepwise*. The *forward* method carries out an analysis of variance for each *p*-variable, that are discriminator candidates, separately. Amongst significant variables, the most significant of all is inserted into the model, in other words, the variable that best identifies the groups. Suppose that a variable is inserted into the model in the first algorithm step, so the *forward* procedure searches for a new significant variable that identifies the groups. The *backward* method begins considering all discriminator candidate variables as part of a unique model. From there, the significance of each variable is tested and the variables that worst define the groups are deleted. If a variable has been removed, the *backward* procedure continues searching for a second variable to remove. The *stepwise* method is a combination of *forward* and *backward* procedures.

4.2 Cluster analysis technique

Cluster analysis belongs to a set of techniques for multivariate statistical analysis. Multivariate statistical analysis is appropriate to any set of data in which multiple measures are carried out, probably with correlations between these measures. Multivariate techniques, in general, analyze the correlation structure between different variables and, in some cases, present more complete results than if variables were analyzed separately (JOHNSON, 1998). Cluster analysis, therefore, can be used to find groups in the data being analyzed (KAUFMAN and ROUSSEEUW, 1990). Cluster analysis is a set of different algorithms and methods to group objects of similar types and their categories. Many researchers from different areas have problems in organizing data under analysis into representative structures. In other words, cluster analysis is an exploration tool that separates components into different groups in such a way that members from the same group are as similar as possible and members from different groups are as different as possible (JAIN, 1991).

Statistically, this results in as small an intra-group variance as possible and as large an inter-group variance as possible. Each cluster describes, in terms of collected data, the class in which their members belong.

Therefore, cluster analysis is a discovery tool. This analysis can show data association, or even when these associations are not evident, they are useful once they had been discovered. Obtained results with cluster analysis can contribute to define a more formal classification plan.

Cluster analyzes have been described in literature through many techniques. However, all techniques basically belong to two classes: hierarchical and non-hierarchical. Non-hierarchical approach begins with a random set of clusters and cluster members are moved until intra-group variance is as small as possible. The hierarchical approach can be implemented in two ways: divided and agglomerative. Using agglomerative approach, given *n* components, the method begins with *n* clusters (each cluster with one component). After that, clusters are joined until a chosen number of clusters have been obtained. Hierarchical divided approach begins with a single cluster (with *n* components) and then, the clusters are divided successively until a certain number of clusters are obtained.

Many distance concepts have been used to create clusters. The best known are: Euclidean distance, weighed distance, Minkowski distance and Jaccard's concordance coefficient. In our work we used the Euclidian distance:

$$dist(x,y) = \sqrt{\sum (x_i - y_i)^2}$$

where x_i and y_i are the coordinates for x and y points.

We used cluster analysis to divide traffic flows into two groups: attack and non-attack, using hierarchical divided approach and Euclidian distance.

5 Results and discussion

In this project, for discriminator selection, we used univariate analysis of variance. This project differs from (ZUEV and MOORE, 2005) in many aspects. First, we are trying to identify a single traffic type and in (ZUEV and MOORE, 2005) the authors obtained a wide classification in ten different categories. Second, we used a simpler method of discriminator selection. In (ZUEV and MOORE, 2005), the authors used the Naïve Bayes method. Our method consists of an independent selection based on F-Distribution. From classified trace each variable is individually and independently examined and its importance is analyzed from F-Distribution values. And, lastly, we use a reduced number of variables in comparison with (ZUEV and MOORE, 2005).

Discriminator selection was based on two criteria: previous knowledge of usual attack behavior and those variables that present large F-Distribution values. Table (2) presents the twelve discriminator candidate variables based on large F-Distribution values.

In Tab. (2) some variables show redundant information, therefore, we selected five variables that better explain the behavior of known attacks. These variables are: Maximum segment size *client to server* (D1), Minimum window advertisement *client to server* (D2), Minimum number of total bytes in IP packet *client to server* (D3), Mean of control bytes in Packet *client to server* (D4), Variance of control bytes in packet *client to server* (D5).

We define the term *trust* as follow:

$$Trust = \frac{\text{nº of flows correctly classified into attack clusters}}{\text{total of flows into attack clusters}}$$

Table (3) shows, individually and together, the trust for attack classification using discriminator variables D1, D2, D3, D4 and D5. Field D1-5 means that the five discriminators variables were joined and analyzed. The ten traces described in section three were used and we applied the five chosen discriminator variables as described above.

Table II: Candidate discriminator variables

Variable Number	Candidate Variable
1	Port server
2	Minimum number of total bytes in IP packet *client to server*
3	Maximum window advertisement *client to server*
4	Mean of control bytes in Packet *client to server*
5	Average segment size *server to client*
6	Maximum window advertisement *server to client*
7	IP data bytes median *client to server*
8	Actual data packets *client to server*
9	Minimum window advertisement *server to client*
10	Data bytes in the wire variance *server to client*
11	Variance of control bytes in packet *client to server*
12	Maximum segment size *client to server*

Table III: Trust by trace and by discriminators

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
D1	94.79%	10.00%	50.00%	99.63%	85.93%	94.21%	100.00%	87.06%	98.99%	98.21%
D2	100.00%	64.29%	93.75%	100.00%	99.17%	96.95%	100.00%	100.00%	96.49%	90.07%
D3	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	80.38%	95.55%	60.43%
D4	8..80%	100.00%	58.33%	100.00%	92.04%	95.28%	83.33%	80.25%	95.28%	98.99%
D5	92.08%	100.00%	70.00%	100.00%	84.62%	93.18%	87.04%	82.12%	95.53%	98.73%
D1-5	85.51%	80.00%	76.19%	100.00%	97.50%	96.85%	100.00%	80.89%	95.30%	100.00%

Figures 1 and 2 were built based on data from Tab. (2) and (3). Figure 1 shows the classification power of the five chosen discriminators and the mean variability obtained from traces using mean classification trust. This variability is shown by maximum and minimum values of each discriminator. The last bar shows the joint processing of the five discriminators.

We can observe in the figures that there is large trace variability. The detailed trace analyzes reveal that when small attack flows are present into trace the classification accuracy diminishes. This is expected evidence because of the reduced bulk of information into collected data.

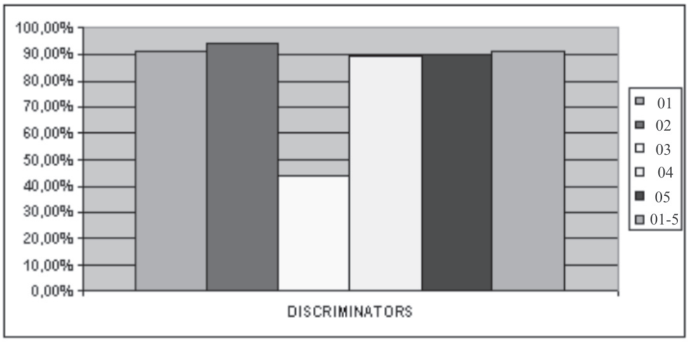

Figure 1: Mean classification trust by discriminators (alone and together).

A different and more intuitive way to visualize and analyze the data is using the Kiviat graph, as shown in Fig. 2. In a Kiviat graph the equidistant radial axis represents the dimensions considered for analysis and each axis represents a discriminator. In each axis the minimum, mean and maximum values are shown and the points of each value are linked.

After the points have been linked we have a visual representation of each discriminator classification power. In the figures the central line represents the mean values and the inside and outside lines represent the minimum and maximum values, respectively. A Kiviat graph advantage is that each discriminator weight can be visually identified.

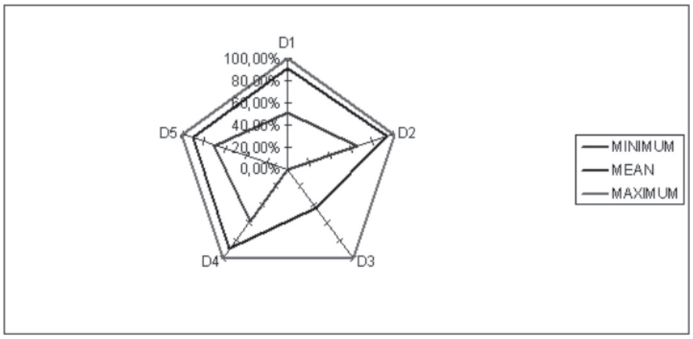

Figure 2: Kiviat graph for mean trust in classification .

Clusters were generated using hierarchical techniques and Euclidian distance. Table (4) shows the results for trust, compared with the results obtained in (ZUEV and MOORE, 2005). In this table we can find the following abbreviations: NB for *Naïve Bayes*, FCBF for *Fast Correlation-based Filter* and Kernel for *Kernel Density Estimation*. The last line, *Cluster*(5) shows the results of our work. It is important to point out that in the five selected discriminators used by this work's method, three of them do not match with the discriminators used in (ZUEV and MOORE, 2005). This fact and the goal to select a single type of application explain the better results achieved.

Table IV: Mean accuracy and method trust

Method	Trust (%)
NB	1.10
NB + Kernel	8.52
FCB + NB	10.38
FCBF + NB + Kernel	13.46
Cluster (5)	91.22

In (Zuev and Moore 2005) the authors used the Naïve Bayes technique to collected data (see section 3) to classify the Internet traffic into ten different classes of applications (see Tab. (1)). In our work we apply to the same set of data used in (Zuev and Moore 2005) the F distribution to select the variables that better identify an attack traffic (discriminators). After the selection of discriminators, we used cluster analysis technique to grouping the traffic flow into attack and non-attack.

It is important to observe that among the five discriminators selected by the method proposed in our work three of them do not match with the discriminators used in (Zuev and Moore 2005). This fact added to the goal of identify a single type of application explain the good results obtained.

As we can see in Tab. (4), the best result obtained by (ZUEV and MOORE, 2005) was 13.46% of trust for attack detection. On the other hand, the discriminator selection and cluster technique applied in this work resulted in 91.22% of trust for attack detection. In other words, the trust on attack detection is almost six times greater than previous values and its percentage is perfectly able to be applied in a work environment.

6 Conclusion

Attack detection is a traffic classification task in which the current success percentage is very low.

This project presented an attack detection methodology based on discriminator selection and a subsequent flow classification.

The obtained results show that the methodology used is better than the main reference used to develop our work. The best result obtained in (ZUEV and MOORE, 2005) was 13.46% of trust for attack identification. In comparison, we obtained in our work 91.22% of trust for attack identification.

This research is not finished yet. We are planning to apply the presented methodology to own traces collected from two ISPs. Also we are planning to apply this methodology to identify other traffic classes, specifically, P2P traffic classification. Knowing the classification limitation based on statistical discriminators, we are also planning to trace semantic analysis with the goal of classifying it.

References

ANDERSON, T. W. *An introduction to multivariate statistical analysis*. New York: 3rd ed. John Wiley*,* 2003. 752 p.

AULD T. et al. Bayesian neural networks for internet traffic classification. *IEEE Transactions on Neural Networks*, Boston, v. 18, n. 1, p. 223-239, 2007.

BARFORD, P. et al. A signal analysis of network traffic anomalies. In: INTERNET MEASUREMENT WORKSHOP, 2., 2002, Marseille. *Proceedings*… Marseille, 2002. p. 71-82. 1 CD-ROM.

BRUTLAG, J. Aberrant behavior detection in timeseries for network monitoring. In: SYSTEMS ADMINISTRATION CONFERENCE-USENIX LISA*,*14., 2000. New Orleans. *Proceedings*… New Orleans, 2000. p. 159-164. 1 CD-ROM.

HUSSAIN, A. et al. A framework for classifying denial of service attacks. In: ACM SIGCOMM*,*3., 2003, Karlsruhe. *Proceedings*… Karlsruhe, 2003. p. 99-110. 1 CD-ROM.

JAIN, R. *The art of computer systems performance analysis*. New York: John Wiley Sons, 1991. 720 p.

JOHNSON, D. *Applied multivariate methods for data analysis*. Belmont: Brooks/Cole, 1998. 567 p.

JUNG, J. et al. Fast portscan detection using sequential hypothesis testing. In: IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 2004, Oakland. *Proceedings*… Oakland. p. 211-225. 1 CD-ROM.

KAUFMAN, L.; ROUSSEEUW, P. *Finding groups in data*: an introduction to cluster analysis. New York: Wiley and Sons, 1990. 335 p.

KIM, H. A.; KARP, B. Autograph: toward automated, distributed worm signature detection. In: USENIX SECURITY SYMPOSIUM, 13., 2004, San Diego, CA. *Proceedings*… San Diego, CA, 2004. p. 210-226. 1 CD-ROM.

KIM, M. S. et al. A flow-based method for abnormal network traffic detection. In: IEEE/IFIP NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, 2004, Seoul. *Proceedings*… Seoul, 2004. p. 599-612. 1 CD-ROM.

LAKHINA, A. et al. *Characterization of network-wide anomalies in traffic flows*. Boston: Boston University, 2004a. Technical Report BUCS-2004-020. Disponível em: <http://citeseer.ist.psu.edu/707784>. Acesso em: 3 abr. 2007.

LAKHINA, A. et al. Diagnosing network-wide traffic anomalies. In: ACM SIGCOMM,4., 2004, Portland. *Proceedings*… Portland, 2004b. 1 CD-ROM

LAKHINA, A. et al. Mining anomalies using traffic feature distributions. In: ACM SIGCOMM,5., 2005. Philadelphia. *Proceedings*... Philadelphia: ACM, 2005. p. 217-228. 1 CD-ROM.

MOORE A. et al. Architecture of a network monitor. In: PASSIVE & ACTIVE MEASUREMENT WORKSHOP (PAM), 4., 2003 La Jolla, CA. *Proceedings*... La Jolla, CA: LNCS, 2003. p. 77-86. 1 CD-ROM.

MOORE, A. et al. *Discriminators for use in flow-based classification*. London: Queen Mary University of London, Department of Computer Science, 2005. 16 p. Technical Report, RR-05.13.

MOORE, A.; PAPAGIANNAKI, K. Toward the accurate identification of network applications. In: PASSIVE AND ACTIVE MEASUREMENT WORKSHOP (PAM), 6., 2005, Boston. *Proceedings*... Boston: LNCS, 2005. p. 41-54. 1 CD-ROM.

PORTNOY, L. et al. Intrusion detection with unlabeled data using clustering. In: ACM WORKSHOP ON DATA MINING APPLIED TO SECURITY (DMSA), 2001. Philadelphia, PA. *Proceedings*... Philadelphia, PA, 2001. 1 CD-ROM.

ROUGHAN, M. et al. Combining routing and traffic data for detection of IP forwarding anomalies. In: ACM SIGCOMM NeTs WORKSHOP. Portland, OR, 2004. *Proceedings*... Portland, OR: ACM, 2004. Poster Section.

SCHECHTER, S. et al. Fast detection of scanning worm infections. In: INTERNATIONAL SYMPOSIUM ON RECENT ADVANCES IN INTRUSION DETECTION (RAID), 7., 2004, Sophia Antipolois. *Proceedings*... Sophia Antipolois: LNCS, 2004. 1 CD-ROM.

TAYLOR, C.; ALVES-FOSS, J. *Low cost network intrusion detection*. Moscow: University of Idaho, 2000. 15 p.

TAYLOR, C.; ALVES-FOSS, J. NATE: network analysis of anomalous traffic events. In: New Security Paradigms

Workshop, 10., 2001, Cloudcroft. 2001. *Proceedings*... Cloudcroft: LNCS, 2001. p. 89-96. 1 CD-ROM.

THOTTAN, M.; JI., C. Anomaly detection in IP networks. *Signal Processing in Networking*, Boston, v. 51. n. 8 p. 2191-2204, 2003. Special issue.

ZUEV, D.; MOORE, A. Internet traffic classification using bayesian analysis techniques. In: CONFERENCE ON MEASUREMENT AND MODELING OF COMPUTER SYSTEMS, Banff, 2005. *Proceedings*... Banff: ACM, 2005. p. 50-60. 1 CD-ROM.

ABOUT THE AUTHORS

Raimir Holanda

Doctor in Computer Science (Technical University of Catalonia - Spain, 2005), Professor of the University of Fortaleza – Computer Science Departament (MIA). Fortaleza - Ce, Brazil. E-mail: raimir@unifor.br

José Everardo Bessa Maia

Master in Eletrical Engeneering (University of Campinas - Brazil, 1985), Professor of the University of Fortaleza; Professor of State University of Ceará - Computer Science Departament, Fortaleza – CE, Brazil.
E-mail: jmaia@unifor.br

Marcus Fábio Fontenelle do Carmo

Master Degree student at University of Fortaleza (MIA), Bachelor in Computer Science (UNIFOR, 2000); Post-graduate in Telecommunication Systems (UNIFOR, 2003); Microsoft Certified Systems Engineer (MCSE) since 1999, Fortaleza-CE, Brazil.
E-mail:marcusfabio@edu.unifor.br