Traffic Anomaly Detection and Characterization in the Tunisian National University Network

Khadija RAMAH [1], Hichem AYARI [2], Farouk KAMOUN [3]

[2,3] CRISTAL laboratory
École Nationale des Sciences de l'Informatique
University of Manouba
2010 Manouba, Tunisia
[1] Ecole d'Aviation Borj El Amri
[1] khadija.houerbi@cristal.rnu.tn, [2] H.ayari@ensi.rnu.tn, [3] farouk.kamoun@ensi.rnu.tn

Abstract. Traffic anomalies are characterized by unusual and significant changes in a network traffic behavior. They can be malicious or unintentional. Malicious traffic anomalies can be caused by attacks, abusive network usage and worms or virus propagations. However unintentional ones can be caused by failures, flash crowds or router misconfigurations. In this paper, we present an anomaly detection system derived from the anomaly detection schema presented by Mei-Ling Shyu in [12] and based on periodic SNMP data collection. We have evaluated this system against some common attacks and found that some (Smurf, Sync flood) are better detected than others (Scan). Then we have made use of this system in order to detect traffic anomalies in the Tunisian National University Network (TNUN). For this, we have collected network traffic traces from the Management Information Base MIB of the central firewall of the TNUN network. After that, we calculated the inter-anomaly times distribution and the anomaly durations distribution. We showed that anomalies were prevalent in the TNUN network and that most anomalies lasted less than five minutes.

Keywords Anomaly Detection, Principal Component Analysis, Temporal Characteristics

1 Introduction

For the last few years, we have observed a continuous increase of malicious traffic in the Internet in form of distributed denial of service attacks, virus and worms propagation, intrusions, etc. In fact recent studies ([4], [8], [14]) have revealed the important rise in malicious traffic volume in the entire Internet. This rise is in a huge proportion caused by the propagation in the Internet of worms such as CodeRed [5] [13], Nimda [13], the Slammer worm [6], Msblaster and Funlove. Consequently,

defending networks against such malicious traffic is a day by day incessant activity for network operators.

A lot of techniques have been developed in order to detect, identify and prevent propagation of malicious traffic over networks. We differentiate between two classes of intrusion detection techniques: Misuse Detection and Anomaly Detection. The Misuse Detection Systems try to detect intrusions by comparing the current activity of the audited resource to a database of known attack scenarios. Those techniques can not detect unknown attacks. However, the Anomaly Detection Systems (ADS) try to detect intrusions by comparing the current activity of the audited resource to an established "normal activity" represented in form of a profile.

The majority of these techniques need to keep per-connection or per-flow state over a single link or node. Thus, they must be widely deployed in all nodes in order to be effective. Moreover they require a lot of computing resources making their cost unaffordable for many ISPs. In this work, we tried to develop an anomaly detection tool able to detect attacks without keeping a per flow state. This tool doesn't attempt to identify the different types of attacks or their origins. So it can be useful as a first-line anomaly detection tool. In fact, this tool can be used to indicate when a more sophisticated intrusion detection system, based on per-flow data collection, must be started.
In fact, we developed an Anomaly Detection System (ADS) derived from the anomaly detection schema presented by Mei-Ling Shyu in [12] and based on SNMP data. After evaluating this system against some common attacks, we exploit it for the detection of traffic anomalies in the TNUN network. Finally we studied some temporal patterns of network traffic anomalies.
This paper is organized as follow. First, in the second section, we discuss previous related work. In the third section, we describe the anomaly detection technique used by our ADS system. Then we present the evaluation method and discuss evaluation results. In section four we describe the TNUN network. After that, we discuss some temporal characteristics of traffic anomalies in the TNUN network in the fifth section. Finally we conclude with a summary of the themes developed during our study.

2 Related Work:

Anomaly detection techniques always start by the construction of a profile for "normal" network behaviour and then mark deviations from such profile as possible attacks. Many approaches have been proposed since anomaly detection was originally proposed by Denning in [7] and they are mainly statistical ones. Indeed, the definition of a normal profile, in those approaches, relies on the use of known statistical properties of normal traffic or on a training period. Then those approaches employ statistical tests to determine whether the observed traffic deviate significantly from the norm profile. The work of J Brutlag in [2] and the one of R Kompella in [16] are examples of such statistical approaches.

Some other statistical approaches are based on clustering techniques ([3], [11], [12]). For example, in [11], Chhabra presents an algorithm that monitors packets at network components and uses a clustering technique to group active flows into categories based on common values in the fields of the packets. If the total number of packets in a cluster is greater than a specified threshold, then the common fields and the corresponding values for the packets in the cluster form an attack signature.

On the other hand, anomaly characterization is the subject of recent research aiming at understanding anomalies statistical, temporal or spatial behaviour in order to be able to develop better and more powerful ADS in the future. Some anomaly characterization studies were based on identified attack traces ([1], [14]). For example, the study elaborated by Yegneswaran in [14] was based on intrusion logs from firewalls and IDS systems at sites distributed throughout the Internet. However, Pang anomaly characterization in [8] was based on measuring background radiation (traffic sent to unused or unallocated IP addresses). Several other studies were based on anomaly traces generated by previously implemented ADS ([3]). All these studies have showed some interesting characteristics of anomalies.

In fact, in [1] Barford used SNMP data, IP flow data and a journal of known anomalies and network events in order to achieve wavelet analysis of network traffic anomalies. He classified anomalies into three groups: network operation anomalies, flash crowd anomalies and network attack anomalies. He found that flash crowd events were the only long lived anomaly events. He also showed that coarse-grained SNMP data can be used to expose anomalies effectively.

By analysing a set of firewall logs, the authors in [14] found that the Internet suffers from a large quantity and wide variety of intrusion attempts on a daily basis. They also found that the sources of intrusions are uniformly spread across the Autonomous System space. The authors affirmed also that a very small collection of sources are responsible for a significant fraction of intrusion attempts in any given month and their on/off patterns exhibit cycles of correlated behaviour. They also found that worms like codeRed or Nimda persist long time after their original release. Finally, they established that the distribution of source IP addresses of the non-worm intrusions as a function of the number of attempts follows Zipf's law.

In [8], the authors used traffic filtering and honeypots techniques in order to study the characteristics of "background radiation" (traffic sent to unused addresses). They broke down the components of this non-productive traffic by protocol, application and often specific exploits, they analysed temporal patterns and assessed variations across different networks and over time. They found that worms probes and "autorooter" scans (similar to worms, but without self propagation) heavily dominate background radiation.

In [3], the authors found that the anomalies are highly diversified including denial of service attacks, flash crowds, port scanning, downstream traffic engineering, high-rate flows, worm propagation and network outages. They also found that most anomalies

are small in time (duration) and space (Number of Origin-Destination flows implicated in each anomaly).

3 The Anomaly Detection System

In order to detect anomalies we developed an ADS tool based on the work of Shyu in [12]. In fact, in [12], Shyu proposed an unsupervised anomaly detection schema based on Principle Component Analysis (PCA) and assuming that anomalies can be detected as outliers.
PCA is a multivariate method, concerned with explaining the variance-covariance structure of a set of variables through a few new variables which are linear combinations of the original ones. On the other hand, outliers are defined as observations that are different from the majority of the data or are sufficiently unlikely under the assumed probability model of data [12].
Shyu has evaluated her method over the KDD CUP99 data and she has demonstrated that it exhibits better detection rate than other well known outlier based anomaly detection algorithms such as the Local Outlier Factor "LOF" approach, the distance of Canberra based approach, the Nearest Neighbour approach and the K^{th} Nearest Neighbour approach.
KDD CUP99 data is the data set used for the Third International Knowledge Discovery and Data Mining Tools Competition. It is composed of TCP connection records labelled as either normal or as an attack with one attack type.
In our ADS tool we propose to use SNMP data. Although this information gives us an aggregated view of the state of the network traffic, it has the advantage to be simple, consume acceptable amount of resources and so it can be used for real time anomaly detection. So we choose to collect the following "MIB" counters for any given monitored equipment: ifInUcastPkts (number of received unicast packets by an interface), ifInOctets (number of received octets by an interface), ifOutUcastPkts (number of unicast packets send by an interface) and IfOutOctets (number of octets transmitted by an interface).
We have implemented this ADS tool using MATLAB environment. For the collection of SNMP data, we used a commercial network management system WhatsUP [15].
In the Next section we present the Shyu's anomaly detection schema used by our ADS tool.

3.1 Shyu's Anomaly Detection Schema

Shyu's method needs, to perform PCA, a robust estimation of the correlation matrix and the mean of the normal observations. In order to obtain such estimators, from a data set of unsupervised data, Shyu proposes the use of the multivariate trimming technique based on the Mahalanobis distance in order to identify the β% (β is given)

extreme observations that are to be trimmed. The Mahalanobis distance is calculated as in Eq. 1 for each observation x_i .

$$d_i^2 = \left(x_i - \bar{x}\right)' S^{-1} \left(x_i - \bar{x}\right) \quad \textbf{(1)}$$

Where $\bar{x}$ is the arithmetic mean estimator and **S** is the correlation matrix estimator. Subsequently, the robust estimators of arithmetic mean and the correlation matrix are calculated from the remaining observations.

In Shyu's method, PCA analysis is based on the use of both major principle components and minor ones, in order to detect both outliers with respect to one variable and multivariate outliers. For the selection of these principle components, Shyu proposes to select the q major principal components that account for a given amount of energy (for example: 50 % of total data set energy). For the minor ones, she proposes to choose them from principal components which eigenvalues are less than to 0.20.

Given the *q* major and *r* minor components selected from p principal components, an observation x is classified as an attack if it satisfies Eq. 2, otherwise it is classified as normal.

$$\sum_{i=1}^{q} \frac{y_i^2}{\lambda_i} > c_1 \quad \text{or} \quad \sum_{i=p-r+1}^{p} \frac{y_i^2}{\lambda_i} > c_2 \quad \textbf{(2)}$$

Where y_i is the i[th] principal component and λ_i is the corresponding eigenvalue. c_1 and c_2 are outlier thresholds determined according to the classifier specified false alarm rate.

3.1 Evaluation Method:

In order to evaluate our ADS, we need a trace where traffic anomalies are well identified. So we have deployed an experimental network (Figure 1) which consists of two local networks connected by a router. In order to simulate normal traffic, we used a network traffic generator LANTRAFFIC [9] which maintains sixteen TCP and UDP bidirectional connections between a victim and the traffic generator machine. Those connections are completely customizable (data length, time between packets, connection generation distribution, packets length…). We also deployed two machines in order to launch attacks over this experimental network. Finally, we deployed our ADS station which processed the collected SNMP data from the central router. This data was collected by a WhatsUP management system every 20 seconds.

For the ADS system we fixed the amount of energy explained by the chosen major principal components to be at least equal to 50% of total data set energy and the trimming to be 0.5% of all observations in the data set.

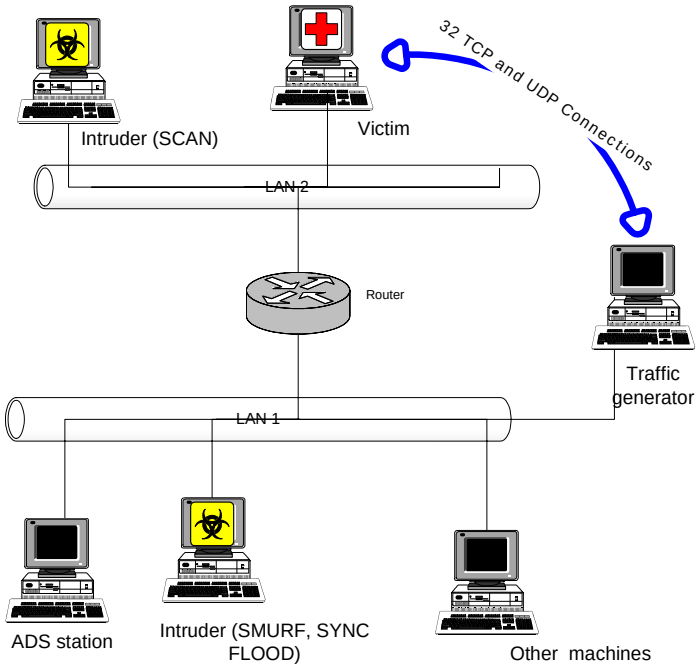

Fig 1: The experimental network for the ADS evaluation.

We evaluate our ADS tool according to the following general and per-attack metrics presented by Lazarevic in [10] (tables 1 and 2).

Table 1 General metrics definition

Real false alarm rate	Number of false alarms divided by the total number of observations
Detection rate	Number of truthful alarms divided by the total number of real anomalous observations
Precision	Number of truthful alarms divided by total number of alarms

Table 2 Per-attack metrics definition

Burst Detection Rate (bdr)	Ratio between total number of intrusive observations that have score value higher than threshold and the total number of real intrusive observations
Response Time (Trep)	Time elapsed from the beginning of the attack until the moment the score value reaches the threshold

3.2 Evaluation Results

Three different types of attacks were launched from the two intruder machines at fixed moments illustrated in figure 2. The chosen attacks are SMURF, SYN-Flood and a network scan attack performed by the NMAP tool. The first two attacks are Deny Of Service (DOS) attacks using flooding techniques. In figure 3, we show the repartition over time of anomalies detected by our ADS.

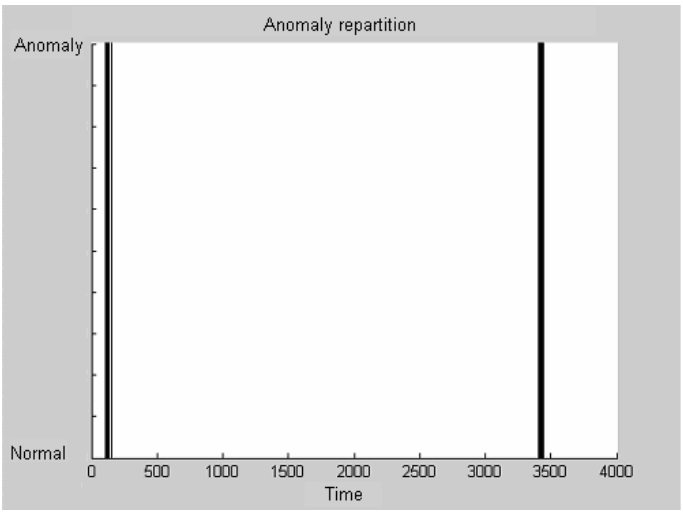

Fig 2: Real anomaly repartition over time

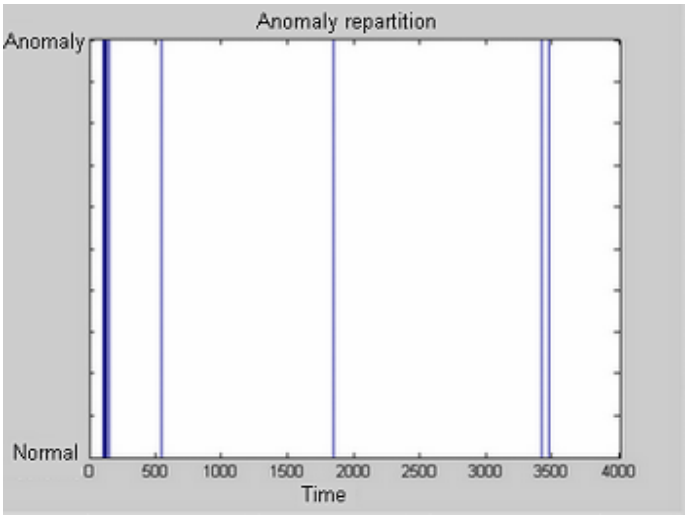

Fig 3: detection results for a 2% fixed false alarm rate

When we increase the fixed false alarm rate, the precision decrease rapidly but the detection rate didn't greatly improve (Table 3). In fact, a fixed false alarm rate of 2% offers acceptable performance.
We remark also, that some attacks are better detected by our system than others (Table 4). In fact, Smurf and SYN-flood attacks are precisely detected (burst detection rate near 100%) and rapidly (response time near 0). Furthermore, we remark that network scan is difficult to detect (burst detection rate very low) and need more time for detection. We think that this low detection rate of network scan anomalies is due to the fact that we have used only one scan process in our experimentation. However in real networks, we assist nowadays to a continuous apparition of new worms and virus that start multiple network scanning threads in each infected machine in order to find backdoors and security holes in other computers. If one vulnerable computer is detected, those worms copy themselves in the victim system which also starts scans in order to attack other computers. So, we think that the impact of those scanning activities will be more apparent in the case of real worm infection than it was in our experiment and we expect to have a better detection rate of our algorithm.

Table 3: Variation of the general performances according to the fixed false alarm rate

Fixed false alarm rate	2%	4%	6%
Observed false alarm rate	1,14%	1,71%	2,54%
Detection rate	47,14%	62,86%	68,57%
Precision	91,67%	56,41%	41,74%

Table 4: Variation of performances by attack type according to the fixed false alarm rate

	Fixed false alarm rate					
	2%		**4%**		**6%**	
	bdr	**Trep**	**bdr**	**Trep**	**bdr**	**Trep**
Smurf	0,93	1	0.97	0	0,97	0
SYN flood	1	0	1	0	1	0
SCAN	0.03	19	0.32	19	0.44	3

The performances of our ADS tool are not as good as those obtained by Shyu in [12]. In fact, she obtained 98.94% for detection rate and 97.89% for precision with a false alarm rate of 0.92%. But, we must notice that Shyu used her method in a supervised manner. In fact, all outlier thresholds were determined from a training data composed of 5000 normal connections.
In our case, we used our ADS tool with no training period, because in real networks it's very difficult to have a training period composed of only normal traffic.

Moreover, our ADS tool is simpler than Shyu's method because it is based only on SNMP data (8 variables in this evaluation test).
Whereas Shyu's method is based on per-flow data (TCP connections composed of 41 variables). In addition, the size of SNMP data used by our ADS tool depends only on the period of collection; whereas the size of the data used by Shyu's method and other ADS systems based on per-flow data depends on traffic volume which makes these systems difficult to adapt for real time anomaly detection in high speed networks.

4 TNUN Network

After evaluation of the ADS tool, we used it in order to detect anomalies in the Tunisian National University Network (TNUN).
The TNUN network is connecting all Tunisian universities to each others and to the Internet. It is composed by a unique central node located at the region of Tunis / El Manar and more than one hundred dispersed universities. In fact, all universities institutions are connected to this central node by mean of direct leased lines or indirect ones (throw the Tunisian national backbone). This central node treats all the network traffic between universities and the Internet and is designed around a central firewall (Fig 4). Thus, the central firewall represents the ideal point of data collection.

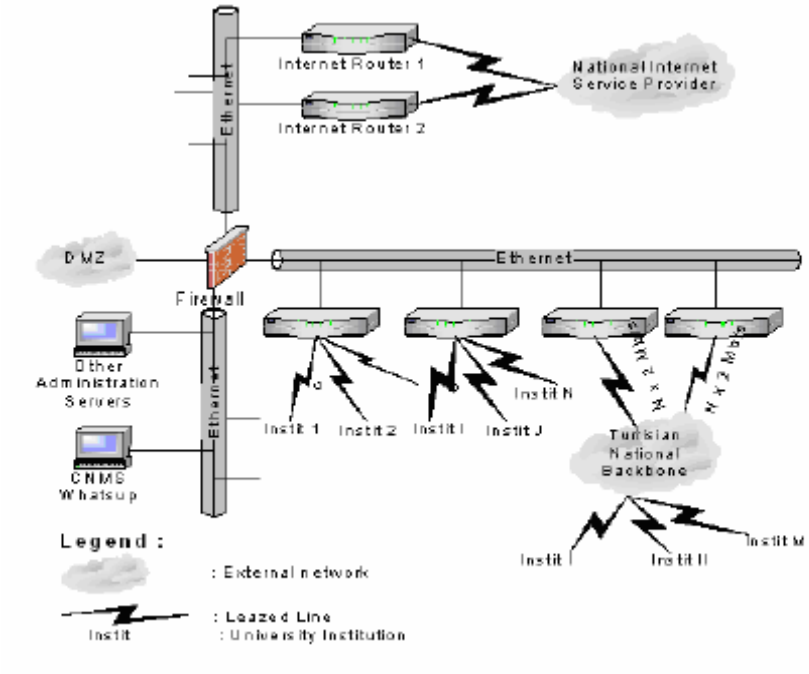

Fig 4: The TNUN Network: CCK/ EL Manar Central Node

So In order to detect anomalies in the TNUN network, we collected periodically, every minute, “MIB” information counters from this central firewall.

5 Characterization of Anomalies in TNUN

In order to study network anomaly characteristics, we define two temporal metrics. The anomaly duration is the lapse of time during which all samples are labeled as anomalous by the ADS system. The inter-anomaly time is the time between the end of an anomaly and the beginning of the next one.
We used the ADS to detect anomalies in TNUN network, for a 45 days period (between 03/04/2004 and 18/05/2004).
We found that anomalies are frequent in the TNUN network. In fact, figure 5 shows that more than 50% of anomalies are separated by less than 60 minutes. We also found that most anomalies are short lived. In fact, figure 6 shows that 90% of anomalies last less than 5 minutes.

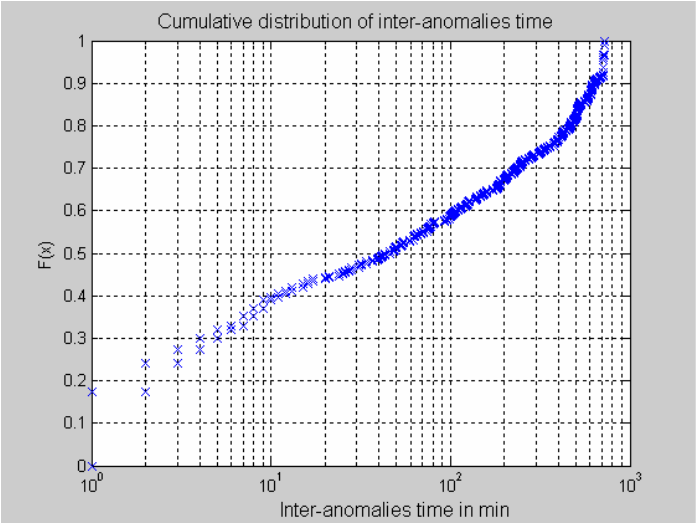

Fig 5: Cumulative Distribution of inter-anomalies time

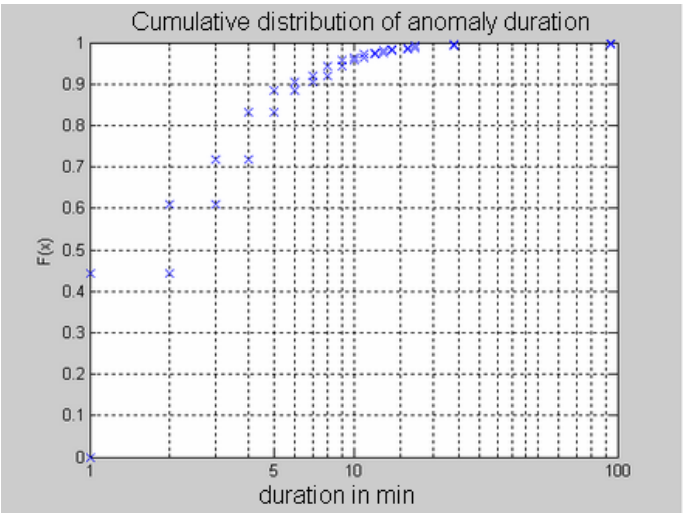

Fig 6: Cumulative Distribution of anomaly duration

These results are consistent with previous studies witch have established that attacks are very frequent in the Internet. For example in [8], Pang affirmed that in the Lawrence Berkeley National Laboratory (LBL), in one arbitrarily-chosen day, about 8 millions connection attempts are scans. This number account for more than double the site's entire quantity of successfully established incoming connections. In [3] Lakhina affirmed that anomalies can last anywhere from milliseconds to hours and that the most prevalent anomalies in his datasets are those that last less than 10 minutes.

6 Conclusion

In this paper, we presented a first level anomaly detection system based on SNMP data. This system can be used for automatic real time detection of traffic anomalies. We have evaluated this system against some well known attacks and found that it is efficient in detecting flooding attacks that disrupt network traffic. These attacks are very difficult to detect with usual intrusion detection systems and to prevent with firewalls because they make use of normal connection attempts.
Next, we showed that in the TNUN network anomalies are prevalent but most of them are short lived. Similar results were previously found in other studies mainly in [3] and [8]. So, we can say that our study offers another proof of the high prevalence of anomalous traffic in Internet.
Finally, we plan to deploy our system over the entire TNUN in order to help network operators in the Tunisian universities early detect on-going attacks. In future work we plan to add to our system modules for attack identification. So network operators can implement filters to mitigate the effect of anomalous traffic on the "good" traffic.

Acknowledgement

This work couldn't be achieved without the active cooperation of the Khawarizmi Calculus Center (CCK). We would like to thank all the CCK personal and particularly his director Madam Henda BEN GHAZALA.

References:

1. P. Barford and D. Plonka, Characteristics of Network Traffic Flow Anomalies, in Proceedings of ACM SIGCOMM Internet Measurement Workshop, San Francisco, CA, November 2001.
2. J.Brutlag, "Aberrant Behaviour Detection in Time Series for Network Monitoring", in Proceeding of the USENIX Fourteenth System Administration Conference LISA XIV, new Orleans, LA, December 2000
3. Anukool Lakhina, Mark Crovella, Christophe Diot, Characterisation of Network-Wide Anomalies in Traffic Flows, IMC'04, Italy, October 2004.
4. D. Moore, G. Voelker, and S. Savage: Inferring Internet Denial of Service activity. In Proceedings of the 2001 USENIX Security Symposium , Washington DC, August 2001.
5. D.Moore, C.Shannon and J.Brown: Code-Red: a Case Study on the Spread and Victims of an Internet Worm. In Internet Measurement Workshop (IMW); 2002.
6. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford and N. Weaver: Inside the Slammer Worm. In Security and Privacy, July/August 2003.
7. D.E. Denning: An Intrusion Detection Model. In IEEE Transaction on Software Engineering, 1987.
8. R. Pang, V. Yegneswaran, P. Barford, V. Paxon, L. Peterson: Characteristics of Internet Background Radiation. In IMC'04, Italy, October 2004.
9. LANTRAFFIC : http://www.zti-telecom.com/
10. A. Lazarevic, L. Eroz, V. Kumar, A. Ozgur and J. Srivastava; A Comparative Study of Anomaly Detection Schemes. In Network Intrusion Detection; Proceeding of Third SIAM International Conference on Data Mining; San Francisco; 2003.
11. P. Chhabra, A. John, and H. Saran. "PISA: Automatic Extraction of Traffic Signatures", In fourth International Conference in Networking, Ontario, Canada, May 2005
12. Mei-Ling Shyu, Shu-Ching Chen, K. Sarinnapakorn, and L. Chang: A Novel Anomaly Detection Scheme Based on Principal Component Classifier. In Proceedings of the IEEE Foundations and New Directions of Data Mining Workshop, in conjunction with the Third IEEE International Conference on Data Mining (ICDM'03), pp. 172-179, Melbourne, Florida, USA, 2003.
13. S. Staniford, V. Paxson and N. Weaver: How to 0wn the Internet in Your Spare Time, In Proc. USENIX Security Symposium 2002.
14. V. Yegneswaran, P. Barford and J. Ullrich; Internet Intrusions: Global Characteristics and Prevalence. In SIGMETRICS'03; USA; June 2003.
15. Ipswitch Whatsup CNMS. www.ipswitch.com
16. R. Kompella, S. Singh, G. Varghese: On Scalable Attack Detection in the Network. Internet Measurement Conference 2004: pp 187-2004.