Cooperative Architecture Applied for Distributed Intrusion Forecasting Systems (DIFS)

Elvis Pontes
Technological Research Institute of São Paulo (IPT), São Paulo, Brazil
elvis@pontes.inf.br

Adilson E. Guelfi
Laboratory of Integrable Systems – Polytechnic School at University of São Paulo (LSI - EPUSP), São Paulo, Brazil
guelfi@lsi.usp.br

ABSTRACT: *Nowadays, integrity, availability and reliability from information systems have been threatened by intrusions and Unwanted Internet Traffic (UIT), Intrusion Detection Systems (IDS) are largely employed to cope with UIT, but IDS lack in security as they are mainly based on postmortem approaches: detection and/or blocking happen only after UIT has inflicted serious damage. Intending to improve intrusion detection, in our earlier work we proposed an approach to cope with UIT in a proactive manner, using forecasting techniques combined with Return on Security Investment (ROSI). In this paper we examine the applicability of a cooperative architecture regarding forecasts of UIT on a more complex set-up, with hosts associated with sites geographically divided. The aim of this paper is to show a cooperative architecture of IDS with prediction approaches, covering the gaps of the current forecasting techniques concerning UIT: sensors employment, the use of just one prediction technique and forecasts' sharing. A proof of concept of such architecture is presented, which allows concluding about the improvement in forecasts for IDS to deal with UIT.*

Keywords: Intrusion detection, Intrusion forecasting, Internet traffic, Intrusion prediction techniques

Received: 1 September 2009, Revised 17 October 2009, Accepted 28 October 2009

1. Introduction

Nowadays, Unwanted Internet Traffic (UIT) is threatening information systems along the Internet, compromising availability, integrity and reliability. To protect such systems, several intrusion detection techniques have been developed in the recent years. The Intrusion Detection Systems (IDS) may be based on identification, detection, reporting and prevention (blocking) of threats, attacks and (UIT) [1], but they lack in security as they are postmortem approaches: UIT is identified and/or blocked only after the UIT inflicts serious damage to the computer systems [2]. Notwithstanding, according to [2-16] predictions about UIT may be obtained using programming techniques and hidden Markov chain in distributed IDS (DIDS). Predictions, regarding UIT in IDS, may also be obtained by the use of hybrid forecasting methods (moving average and Fibonacci sequence), as employed by [2-3]. In this study, we classify the IDS generations as follows: the first generation of IDS concerns identification and detection of UIT, the second one is based on prevention and blocking, and the third one (IDS 3G) refers to prediction and forecasting [33].

Although some forecasting techniques have already been applied on IDS 3G in the last few years, three major gaps lie on those approaches: 1) Sensors employment: not many studies about forecasting in IDS adopt sensors. When sensors are

used [2], [9], [13], [15] it is in a limited manner and/or geographically located. According to [29-31], forecasts can be improved using several sources of data. The employment of a large number of sensors, widely spread, allows gathering more relevant information about variables which are going to be analyzed; 2) Usage of just one forecasting technique: as predictions involve uncertain situations, as no single prediction method is 100% certain about the future, and according to [29], to obtain a more accurate result about predictions, it is suggested to use diverse forecasting techniques; 3) Forecasts' sharing: in accordance with [29-31] to share and to combine forecasts among forecasters (that may be geographically divided) in a cooperative manner may result in a more accurate prediction.

In the same way of other sciences, forecasts could be helpful for information technology. In information security field, a future trend with an increasing number of UIT, shown by forecasting analysis, may influence the decisions concerning the security devices adoption before the incidents happen and according to the needs [3-4], [33-34].

The expression "unwanted traffic" was first introduced in the eighties and it has always been related to malicious activity as worms, virus, intrusions etc [20]. Reference [21] defines unwanted Internet traffic (UIT) as unproductive and useless traffic, with malicious (worms, scans, spam) and benign (wrong setting in the routers) events. Reference [33] completes this definition: UIT may result from the noise in the telecommunication network. UIT may also be junk traffic, background traffic and anomalous traffic.

The Request for Comments (RFC) 4948 [22] details the UIT types, the main causes, existent solutions and the actions to be taken in short and long term. The RFC 4948 also refers that some topics regarding UIT would be managed by the IAB, Internet Engineering Task Force (IETF) and Internet Research Task Force (IRTF). Reference [25] published a study in the United States about the losses concerning UIT (non requested traffic, useless, unknown traffic and, a lot of times, illegitimate traffic): UIT caused about $264.6 million of losses in 275.284 organizations. This is up from $239.1 million in total reported losses in 2007. According to [26], in 2008, for the first time, American Internet Service Providers (ISP) also described a far more diversified security landscape, including significant concerns over diverse kinds of UIT: domain name system DNS) spoofing, border gateway hijacking and spam.

The main purpose of this paper is to detail the employment of EWMA and Fibonacci forecasting technique to cover three major gaps of current prediction methods concerning UIT: sensors employment, the use of just one prediction technique and forecasts' sharing. EWMA and Fibonacci forecasting techniques were applied in the IDS 3G architecture [5], which may be composed by four levels: independent security devices of hosts, correlated security devices of hosts, network level and backbone level.

This paper is organized as follows: state of art about forecasting in IDS is in next section. Section 3 presents the description of the IDS 3G – Distributed Intrusion Prediction System. The proof of concept is presented in section 4. Section 5 summarizes conclusions and suggestions for new studies.

2. State of Art

The forecasting approaches in IDS lie mainly in stochastic methods [3-4], [7-19]. With no attention about predictions, [5] applied diverse probabilistic techniques (decision tree, Hotelling's T^2 test, chi-square multivariate, Markov chain and Exponential Weighted Moving Average (EWMA)) on audit data as a way to analyze three properties of the UIT: frequency, duration, and ordering. Reference [5] has come to the following findings: 1) the sequence of events is necessary for IDS, as a single audit event at a given time is not enough; 2) ordering / transaction [19] provide additional advantage to the frequency property, but it is computationally intensive. Frequency property by itself provides good intrusion detection [5], [19]. Even though simulations of the attacks in the [25] datasets (DoS, remote to local, user to root and probing) were done, neither correlation among other types of UIT (spam, virus, worms), nor DIDS were studied in [5]. The employed techniques in this study are commonly used for forecasts.

Moving averages (simple, weighted, exponential, or central) with time series data are regularly used to smooth out fluctuations and highlight trends [28]. EWMA may be applied for autocorrelated (events that carry out a series of related commands in order to complete a given task) and uncorrelated UIT data for detecting intrusions that manifest themselves through significant changes in the intensity of events occurring [6]. Both (EWMA for autocorrelated and uncorrelated) has presented good efficiency for detecting UIT. EWMA was first introduced by [27]. EWMA applies weighting factors which decrease exponentially,

giving much more importance to recent observations while still not discarding older observations entirely. The equation is [28]:

$$EWMA_t = \alpha Y_t + (1-\alpha) EWMA \quad \text{for } t=1, 2, \ldots, n \qquad (1)$$

Where: *EWMA* is the mean of historical data; Y_t is the observation at time *t*; *n* is the number of observations to be monitored including EWMA; $0 < á < 1$ is a constant that determines the depth of memory of the EWMA.

The parameter á determines the rate of weight of older data into the calculation of the EWMA statistic. So, a large value of á gives more weight to recent data and less weight to older data; a small value of á gives more weight to older data.

Reference [14] gives an overview of adopting EWMA with adaptive thresholds, based on normal profile of network traffic. The employment of thresholds with EWMA may summarize the analysis of huge amount of data in network traffic [17-18]. Diverse combined moving averages with Fibonacci sequence forecasting approach were also used by [3-4] to spot trends of UIT in [25-26] datasets.

Markov chain is a stochastic process also used in IDS. In Markov chain future states depend only on the present state, and are independent of past states. Reference [8] studied the behavior of the system (system calls and privileged process), inferring the probability of Markov chain in the observed temporal UIT data. Similarly, [7] employed Markov chains, as well as profiling about normal activities, for dynamic load-balancing algorithm. So, it proposed a real-time prediction method regarding UIT in IDS. Lower false alarm rate and false negative rate were obtained during the application of the method. Although, according to [5] the employment of first-order of Markov model may not produce good intrusion detection, and it advocates about the use of high-order Markov model for UIT.

Hidden Markov Model (HMM) is also used in DIDS, or Distributed Intrusion Prediction and Prevention System (DIPPS) to UIT [2]. Each HMM contains a finite number of unobservable (or hidden) states. Transitions among the states are governed by a set of probabilities. More details about HMM may be found in [2]. The adoption of DIDS during the forecasting of UIT may result in a more comprehensive and accurate prediction, as it makes use of spread sensors in the computer network [3-4]. Though, the result of [3-4] could be better if it used more than five forecasting techniques and a larger amount of sensors [29-31]. Predictions about UIT in IDS may be achieved using Hidden semi-Markov Model (HsMM), too [16] In HsMM, the probability of a change in the hidden state depends on the amount of time that has elapsed since entry into the current state. Data mining techniques with neural networks were used by [10-12], as a way to provide predictions about UIT in IDS. Even though any of the studies used neural networks, the approaches were different: 1) [10] analyzed the normal profile of [25-26] datasets to determine de normal behavior and projecting it in the future. Back propagation neural network and neuro-genetic ensemble network were used to build the predictions. Conclusively, this methodology may be employed in real-time for IDS to make predictions about UIT; 2) As well as the previous study, [11] needed to observe the user behavior (profile). But, instead of back propagation, quick propagation algorithm was used, as it is faster by an order of magnitude or more. Quick propagation algorithm also appears to scale up much better than standard back propagation as the size and complexity of the learning task grows.

In accordance with [11], some restrictions of the use of neural networks and profiling are: 1) Hard to predict how long the user will use a specific resource in the future, but it can predict if the user will use this specific resource or not; 2) Profiling new user's behavior. Notwithstanding, in accordance with [11], statistical models like simple exponential, Bayesian, regression, among others, don't suit well to predictions about UIT, as they are linear methods and UIT is a non-linear problem. Despite the opinion of [11], Bayesian Inference is employed for predicting increase or decrease of various types of attacks, based on past-observed event counts [12]. Therein, forecasts hit ratio for days and hours were analyzed in two manners: attack cycle and fluctuation range of event counts. As a conclusion, attacks may be predicted by the use of Bayesian Inference [12]. Prediction architecture for UIT in DIDS with 2 layers was designed by [9], in which the first layer is responsible for detection (by the use of Bayesian Networks), while the second one is entrusted with forecasting procedures. In this study, the forecasting approach is merely based on probabilistic conditions (not mentioned which ones) about current UIT, UIT's historic series and the possibility of the UIT inflict other hosts in the DIDS. The innovation in [9] lies in the agents (sensors) which compute data among the hosts and report forecasts to the system administrator, analogous to the DIPPS of [2].

3. IDS 3G – Intrusion Forecasting System

The proposed architecture is based on main concepts about forecasts: 1) Sensors widely spread [29-31]; 2) Cooperative forecasts [29-31]; 3) Usage of more than five techniques to make forecasts [29].

As no forecasting technique is perfect in concept to obtain the most accurate results, the employment of more than five forecasting techniques may improve forecasts; indicating a more realistic trend [4]. In other words, in this proposed IDS architecture, IFS makes use of five forecasting techniques: simple moving averages (SMA), exponential weighted moving averages (EWMA), combined SMA, combined EWMA and Fibonacci sequence. IFS contains four levels: 1) hosts' independent security devices, 2) hosts' integrated security devices, 3) network level and 4) backbone level. All levels have some communication and integration degree among each other. In other words, the forecasts obtained from the level 1 are shared, combined and integrated to the forecasts of the other levels. Integration and combining provide either to local hosts, or to the administrator of the LAN, or to the backbone provider, a more accurate trend about possible tendencies concerning UIT. Figure1 shows the forecasting architecture. Similarly to forecasting methodologies used in other fields, in which sensors are adopted (meteorology, for instance, use sensors to capture variables like temperature, humidity [31], while seismology employs sensors to capture electromagnetic emissions from the rocks [30]), IFS for UIT also spread sensors widely to make predictions. Sensors in IFS compute variables about the different kinds of UIT (spam, virus, intrusion, abnormal network traffic) in all of the four levels of the IFS (hosts' independent security devices, hosts' integrated security devices, network level and backbone level). It is important to notice that different classification of UIT occurs from one IFS level to another. It is also important to notice that the shared data by IFS levels is just historical series of UIT (how many spam host H received, e.g.). In this model, the incident itself is not shared or reported, as a way to preserve the confidential properties of hosts, users and organizations.

IFS Level 1 (Host Level: Independent Security Devices) concerns the trend analysis about incidents, alerts and diagnosis reported independently by the hosts' security devices (antivirus, antispyware, host-based IDPS [1] and other anomaly detector systems). For each security device, individual forecasts may be provided, e.g. the trend about spam for next hour or the day of tomorrow. The next step of the IFS level 1 is to help the hosts' security devices to determine whether or not they should adopt countermeasures to stop UIT. According to [33-34], it is not recommended to employ an extremely restrictive posture, as the cost of such posture is more expensive than the benefit it could bring. Even though the individual analysis of security devices (incidents, alerts and diagnosis) may be useful, IFS level 1 may be significantly improved if combined with level 2, 3 and 4. When the integration and combining among the IFS levels are done, a more realistic trend is obtained, which can be any: forecasts about the host, forecasts about all hosts devices in an integrated way, and finally forecasts about the entire network.

IFS Level 2 (Host Level: Integrated Security Devices) involves the integration and correlation of forecasts about the hosts' security devices. At this level, the analysis lays on two databases: 1) All the historical data generated from each one of the hosts' security devices are processed individually by the IFS first level, then stored in a database; 2) The network flow may also be recorded for further forecasting analysis. The next step for the IFS level 2 is to query and to analyze the trends (forecasts) of such databases. After analyzing it, IFS level 2 returns a feedback to IFS level 1. Feedback contains trends of the UIT (concerning incidents, alerts and diagnosis) about both: all the security devices and the network flow. Likewise a conductor in an orchestra (with different musicians and instruments), IFS level 2 may give directions, providing harmony along trends for the different security devices (antivirus, firewall, etc), against malicious activity. It is important to notice that the databases of IFS level 1 work as sensors for IFS level 2. IFS level 2 may also record the provided feedback in databases.

IFS level 4 (Backbone Level) is the major level. It considers the structure of the backbone providers (an ISP, for instance). In the same way IFS level 3 and level 2, different security devices are linked to the backbone level. The steps for IFS level 4 to work are: 1) Backbone security devices record UIT in database; 2) IFS level 4 queries the databases provided by the lower and current level; 3) IFS level 4 analyzes the provided databases to define the trends; 4) IFS level 4 provides feedback of the trend analysis to the current level; 5) IFS level 4 may also give feedback for the lower levels. This step is usually hard to be done, as most of the backbone providers do not publicly reveal how frequently their infrastructure is impacted. Similarly to lower levels, IFS level 4 uses the same concept of sensors: lower databases and the entire lower IFS levels are sensors for IFS level 4. An important note is: the IFS level 4 may be shared among various backbone providers. To share the forecasts of IFS level 4 means to provide the most realistic and integrated trend about UIT, as it may spread sensors along the network.

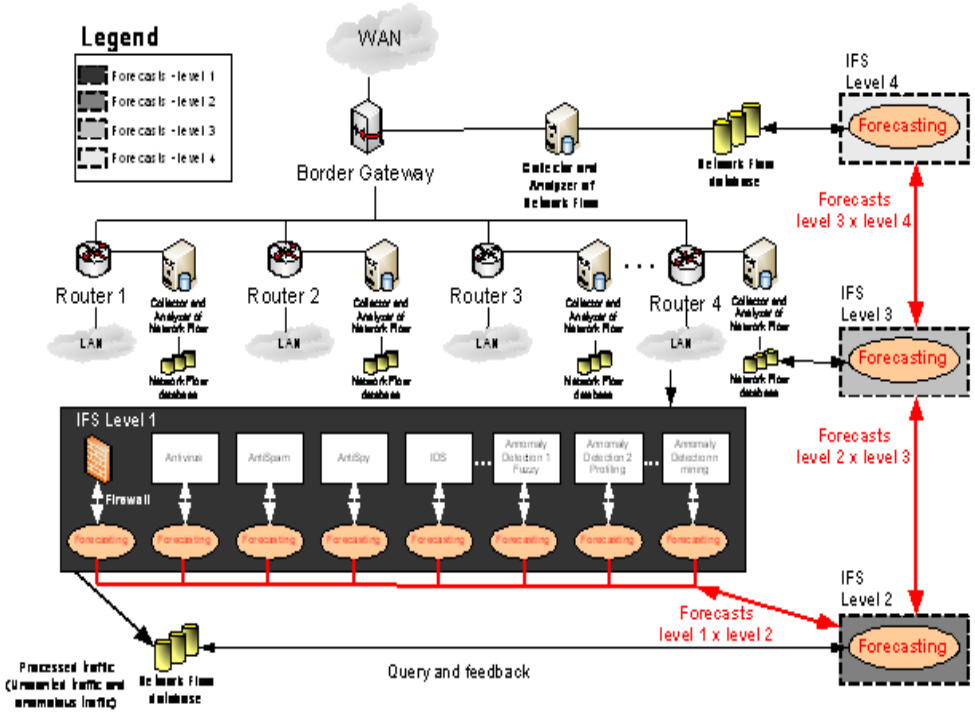

Figure 1. Intrusion Forecasting System (IFS)

4. Proof of Concept

For the proof of concept setup, levels 1, 2 and 3 of the IFS were implemented in three sites geographically divided (A, A' and A''). The following hardware and services were used:

- 1 Pentium core 2 quad 2.0 GHz, 8GB RAM;
- 2 Pentium core 2 duo 1.8 GHz, 4GB RAM;
- 10 virtual machines (Ubuntu 8.04) 512MB RAM;
- 4 virtual machines (WindowsXP) 512MB RAM;
- Windows Vista (host for the virtual machines); VMware Player 2.51; Snort; Netfilter/Iptables; MySQL; OpenVPN.

As a way to provide security to the shared forecasts among the sites geographically divided (fusion), the OpenVPN is used, granting tunneling functionality. Likewise [2], in this prototype the simulation of UIT was divided in just in four types: 1) Denial of service (DoS): Ping of Death and SYN Flood are examples of this kind of UIT; 2) Remote to local (R2L): Buffer over flow and SQL injection are examples of this kind of UIT; 3) User to root (U2R): Buffer over flow and SQL injection are also examples of this kind of UIT; 4) Probe (Scanning): Nmap is an example of software for scanning. During four weeks, we simulate usual network traffic and UIT among hosts in each site. Normal network traffic and UIT were also simulated between sites. H-IDS [1] was installed in each one of the hosts. N-IDS [1] was installed at the gateway. Figure 2 illustrates the sites, hosts with normal activities and infected hosts. Infected hosts inflict UIT to the hosts of each site and to sites, as pointed by arrows.

In this prototype, the propagation of UIT was in the following sequence: from site A to site A', from site A and A' to site A'', from site A'' to site A. Table 1 shows the results to forecast UIT, where correct and wrong forecasts consider just the predicted elapsed time before UIT hit the victim. For this prototype, IFS was developed in JAVA, by the authors. The open source IDS Snort is the tool used to analyze the network traffic. All classified UIT is lately recorded in a MySQL database. IFS

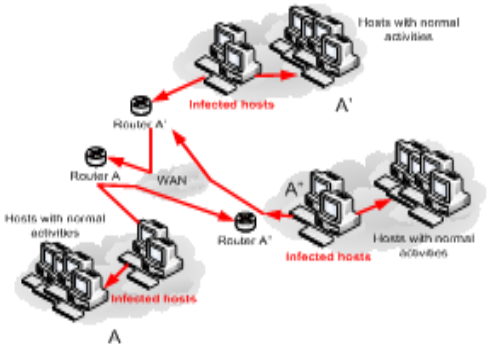

Figure 2. Intrusion Forecasting System (IFS) Prototype

collects the data from the MySQL database, analyzes the information and then, when a particular threshold of UIT is exceeded, a signal (warning) is sent to the IFS collaborators. Details about the adopted forecasting techniques are not reported in this paper due space limitations, but the reader may consult [3-4] for more details about the employed forecasting techniques.

5. Conclusion

Table 1 depicts the results of forecasting UIT in the prototype. The UIT hit 4.320 thresholds from site A to site A' and, gradually, it increased with propagation of the UIT among the three sites. The total amount of the UIT thresholds among the three sites was about 16.416. In Table 1, correct forecasts are the number of times that it was possible to foresee the increasing and/or decreasing UIT's phases, without any delay.

	A → A'	**A → A' → A"**	**A" → A**
Overall UIT thresholds	4.320	8.208	16.416
Correct forecast	2.623	4.984	9.967
Forecast with delay	1.483	2.818	5.635
Times not predict	214	407	813

Table 1. Results of Forecasting the UIT Propagation

The correct predictions' rates were about 60,71%. Forecast with delay are the number of the times the increasing and decreasing thresholds were identified lately. In this prototype, forecasts' rates with delay were about 34,74%. During the prototype tests, sometimes it was not possible to identify thresholds for of UIT decreasing or increasing. The rate for the times we could not predict was about 4,95%. Although Fibonacci sequence approach is computationally intensive, IFS employment was able to predict the UIT increasing and decreasing, as thresholds were signaled among hosts and sites. Conclusively this study has attempted to deal with UIT in sites geographically divided. It was done an experiment with a prototype, employing diverse sensors and forecasting techniques, in a cooperative manner. In this prototype it was possible to track UIT in advance; hence such methodology may be employed as an early warning system.

Even though only 4,95% of the thresholds for UIT's increasing and decreasing were not detectable, the value of the outcome is still questionable, as this early warning system still has 34,74% of warnings being lately reported. As a way to improve the forecast's result, among the suggestions for future works there are the aggregation of the fractal approaches (according to [32]), and the use of other kinds of forecasting techniques (as Markov chains and neural networks) to follow [29]'s advices. The IDS 3G has not yet undergone extensive training enough to be used in commercial applications.

7. References

[1] NIST SP 800-94 (2007). Guide to Intrusion Detection and Prevention Systems (IDPS)", (2007).

[2] Haslum, K., Abraham, A ., Knapskog, S (2008). Fuzzy Online Risk Assessment for Distributed Intrusion Prediction and Prevention Systems, *IEEE ICCMS*, p. 216-223.

[3] Pontes, E., Guelfi, A. E., Alonso, E. (2008). Análise de Tendências Futuras para Eventos de Segurança da Informação em Sistemas de Detecção de Intrusão, *In*: Proc. VIII SBSEG, SBC. p. 253-260.

4] Pontes, E., Guelfi, A. E (2008). Forecasting for Return on Security Information Investment: New Approach on Trends in Intrusion Detection and Unwanted Internet Traffic, *In:* Proc. IEEE. VII I2TS. p 203-210.

[5] Ye, N., Li, X., Chen, Q., Emran, S. M., Xu, M. (2001). Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data, IEEE Transactions on Systems, Man and Cybernetics, 2001, p 266-274.

[6] Ye, N., Vilbert, S., Chen, Q. (2003). Computer Intrusion Detection Through EWMA for Autocorrelated and Uncorrelated Data, *IEEE Transactions on Reliability*. p 75-82.

[7] Lai-Chenq, C.(2007). A High-efficiency Intrusion Prediction Technology Based on Markov Chain, IEEE CISW.

[8] Yin, Q., Shen, L., Zhang, R., Li, X (2004). A New Intrusion Detection Method Based on Behavioral Model, IEEE WCICA, p. 4370-4374.

[9] Jemilli, F., Zaghdoud, M., Ahmed, M. B (2006). DIDFAST.BN :Distibuted Intrusion Detection and Forecasting Multiagent system Using Bayesian Network, IEEE ICTTA. p 3040-3044.

[10] Sindhu, S.S., Geetha, S.S., Sivanath, S.S., Kannan, A. (2006). A Neuro-genetic Ensemble Short Term Forecasting Framework for Anomaly Intrusion prediction, *In:* Proc. IEEE ADCOM, p 187-190.

[11] Ramasubramanian, P., Kannan, A.,"Quickprop Neural Network Ensemble Forecasting Framework for Database Intrusion Prediction System, *In*: Proc Springer 7th ICAISC, 2004, p. 9-18.

[12] Alampalayam, P., Kumar, A. (2004). Predictive Security Model Using Data Mining, *In*: Proc IEEE Globcom.

[13] Kim, Chung, Y I., Lee, C., Im, E. G., Won, D. (2006). Design of On-Line Intrusion Forecast System with a Weather Forecasting Model, Springer ICCSA.

[14] Cisar, D., Cisar, S. M. (2007). EWMA Statistic in Adaptive Threshold Algorithm", IEEE INES, p. 51-54.

[15]Leu, F., Yang, W., Chang,W. (2005). IFTS: Intrusion Forecast and Traceback based on Union Defense Environment", IEEE ICPADS.

[16] Zhengdao, Z., Zhumiao, P., Zhiping, Z. (2008). The Study of Intrusion Prediction Based on HSMM", IEEE Asia-Pacific Services Computing Conference, 2008, pp 1358-1363.

[17] Viinikka, J., Debar, H. ,Mé, L., Séguier, R. (2006). Time Series Modeling for IDS Alert Management, ACM ASIAN ACM Symposium on Information, Computer and Communications Security.

[18] Ishida, C., Arakawa, Y., Sasase, I. (2005). Forecast Techniques for Predicting Increase or Decrease of Attacks Using Bayesian Inference, IEEE PACRIM. p 450-453.

[19]Wong, W., Guan, X., Zhang, X. Yang, L (2006). Profiling Program Behavior for Anomaly I Based on the Transition and Frequency Property of Computer Audit Data, ELSEVIER Computer & Security.

[20] Feitosa, E. L., Souto, E. J., Sadok, D.(2008). Tráfego Internet não Desejado: Conceitos, Caracterização e Soluções". in Proc. VIII SBSeg, SBC. p. 91-137.

[21] Soto, P. (2005). Identifying and Modeling Unwanted Traffic on the Internet, Masters Dissertation, Dept. of Electrical Engineering and Computer Science, MIT.

[22] Andersson, L., Davies, E., Zhang, L.S(2007). Report from the IAB workshop on Unwanted Traffic March 9-10, 2006", RFC 4948, IETF. 2006.

[23] Internet Crime Complaint Center (2008). 2008 Internet Crime Report. Bureau of Justice Assistance and National White Collar Crime Center, www.ic3.org.

[24] McPherson, D., Labovitz, C. (2008). Worldwide Infrastructure Sec. Report, www.fbiic.gov/public/2008/

[25] DARPA, 1998. http://www.ll.mit.edu/mission/

[26] KDD Cup 1999, http://kdd.ics.uci.edu/databases/

[27] Roberts, S. W. (1959). Control chart tests based on geometric moving average. Technometrics.

[28] NIST/SEMATECH e-Handbook of Statistical Methods, 2008. [Online]. Available: www.itl.nist.gov/.

[29] Armstrong, J. S.(2002). Principles of Forecasting: A Handbook for Researchers and Practitioners. Springer, USA.

[30]Bleier,T., Freund, F. (2005). Impending earthquakes have been sending us warning signals—and people are starting to listen. IEEE Spectrum,

[31] Lajara, R., Alberola, J. , Pelegri, J., Sogorb, T., Llario, J. V (2007). Ultra Low Power Wireless Weather Station, IEEE SENSOR COMM. p. 469-474.

[32]Mandelbrot, B., Hudson, R. L (2006). The Behavior of Markets: A Fractal view of risk, ruin and reward, John Willey.

[33]Pontes, E., Guelfi, A. (2009). IFS – Intrusion forecasting system based on collaborative architecture. *In*: IEEE ICDIM, Michigan, USA.

[34]Pontes, E., Guelfi, A. E (2009). Third generation for intrusion detection: applying forecasts and ROSI to cope with unwanted traffic. *In:* IEEE ICITST London.