5

Earthquake Prediction: Analogy with Forecasting Models for Cyber Attacks in Internet and Computer Systems

Elvis Pontes, Anderson A. A. Silva, Adilson E. Guelfi and Sérgio T. Kofuji
Laboratory of Integrated Systems, Polytechnic School of the University of São Paulo
Brazil

1. Introduction

Currently, security of the cyber space (computer networks and the Internet) is mostly based on detection and/or blocking of attacks by the use of Intrusion Detection and Prevention System (IDPS), according to (National Institute of Standards and Technology [NIST SP800-94], 2010). However IDPS lacks in security as it is based on *postmortem* approaches - threats and attacks are identified and/or blocked only after they can inflict serious damage to the computer systems either while attacks are happening, or when attacks have already imposed losses to the systems (Haslum et al, 2008).
On the subject of earthquakes, one can notice the same kind of limitation: once an earthquake has already begun, devices can provide warnings with just few seconds before major shaking arrives at a given location (Bleier & Freund, 2005), (Su & Zhu, 2009). In the cyber space context, intending to cover the deficiency of late warnings, predicting techniques have already been approached in a small number of studies for cyber attacks in the last few years (Pontes & Zucchi, 2010), (Haslum et al, 2008), (Lai-Chenq, 2007), (Yin et al 2004).

1.1 Motivation

Although studies based on 1) historical earthquake records and 2) monitoring the earth's surface had contributed to map affected regions, short-term earthquake predictions are not efficient yet (Bleier & Freund, 2005).
Some researchers are studying and correlating signals gathered in the ionosphere that can precede earthquakes, like odd radio noise and lights in the sky.
According to (Bleier & Freund, 2005) "both the lights and the radio waves appear to be electromagnetic disturbances that happen when crystalline rocks are deformed--or even broken--by the slow grinding of the earth that occurs just before the dramatic slip that is an earthquake".
Some occurrences of earthquakes show signals and disturbances like following reported ones:

- Loma Prieta, San Francisco,1989: two weeks before a 7.1-magnitude earthquake, strong signals (20 times that of normal background noise at the 0.01 Hz frequency) of magnetic

disturbance were detected. Three times before the quake the signals jumped to 60 times normal size at the 0.01 Hz frequency;
- Spitak, Armenia, 1988: signals occurred shortly before a 6.9-magnitude quake;
- Guam, Pacific Ocean, 1993: signals were observed before a 8.0-magnitude quake;
- Parkfield, California, 2003: nine hours before a 6.0-magnitude quake, spikes of activity, four to five times normal size (0.2 to 0.9 Hz frequency) were detected;
- Taiwan, 1999: sensors registered unusually large disturbance in a normally quiet signal before the 7.7-magnitude earthquake. Researchers calculated the current required to generate those magnetic-field disturbance: between 1 million and 100 million amperes.

Those examples show that the occurrence of electromagnetic signals does not justify a public warning, but it is an important source of data for forecasters and are also useful for directing the course of research on earthquake prediction such as changes in the conductivity of the air over the quake zone caused by current welling up from the ground, that contribute to the formation of the so-called earthquake lights in the Mojave Desert (Fig. 1).

Fig. 1. Earthquake lights (Bleier & Freund, 2005)

There are some theories about these signals generation, but details are not conclusive yet. Notwithstanding, electromagnetic effects of the signals can be detected in a number of ways (see Fig. 2 next page).

Ground-based sensors, monitor changes in the low-frequency magnetic field and measure changes in the conductivity level of the air. Satellites monitor noise level at extremely low frequency and monitor the infrared light which is probably emitted when rocks are deformed or even broken. Some example:
- after the 1989 Armenia earthquake, electromagnetic Extremely Lower Frequency (ELF) disturbances were observed by a Soviet Cosmos satellite by a month;
- an U.S. satellite detected ELF bursts before and after a 6.5-magnitude earthquake in 2003 at California;
- In 2004 France has launched a satellite for Detection of Electro-Magnetic Emissions Transmitted from Earthquake Regions (DEMETER) that unfortunately presented malfunctioning.

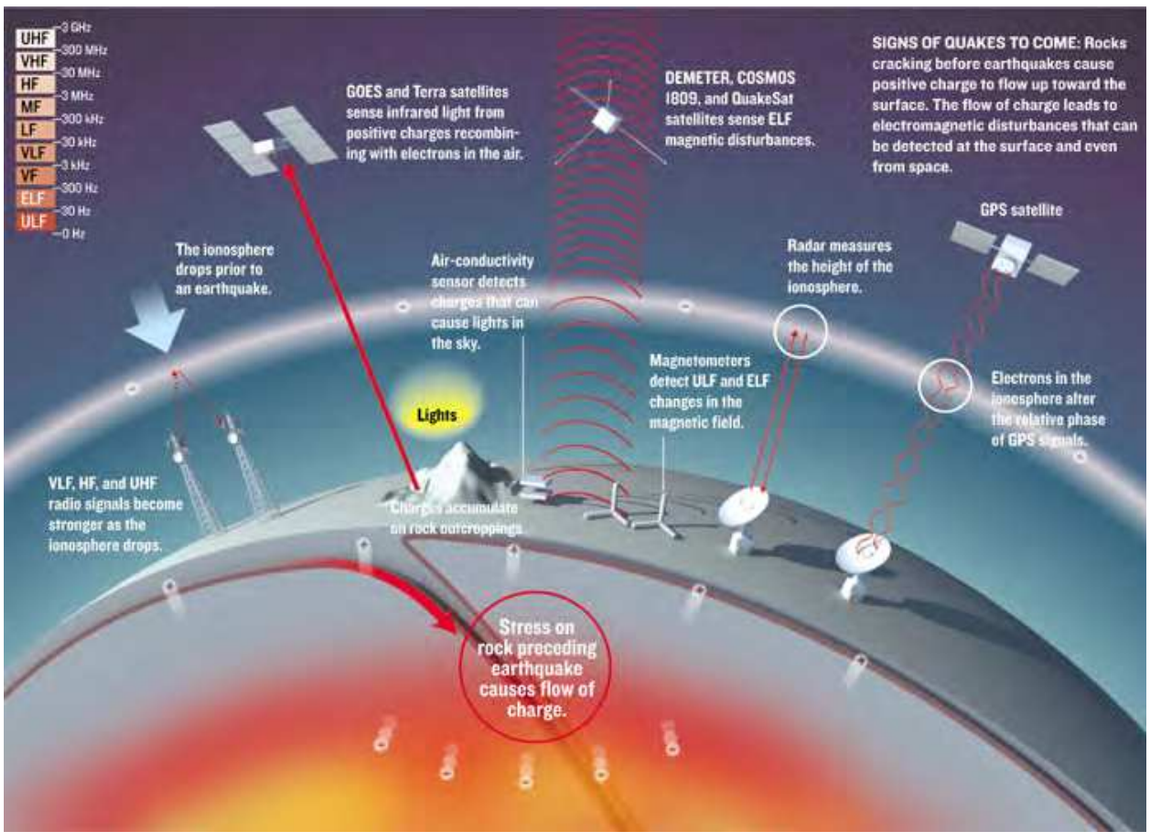


Fig. 2. Electromagnetic signals detection (Bleier & Freund, 2005)

According to (Bleier & Freund, 2005), "infrared radiation detected by satellites may also prove to be a warning sign of earthquakes to come". In China satellite-based instruments had registered the occurrence of several infrared signature instances with a jump of 4 to 5 oC before some earthquakes during the past two decades Sensors in NASA's Terra Earth Observing System satellite registered what NASA called a thermal anomaly on 21 January 2001 in Gujarat, India, just five days before a 7.7-magnitude quake there; the anomaly was gone a few days after the quake (Fig. 3). Accordingly with (Bleier & Freund, 2005), in both cases researches believe these sensosrs have detected an infrared luminescence generated by the recombination of electrons and holes, not a real temperature increase.

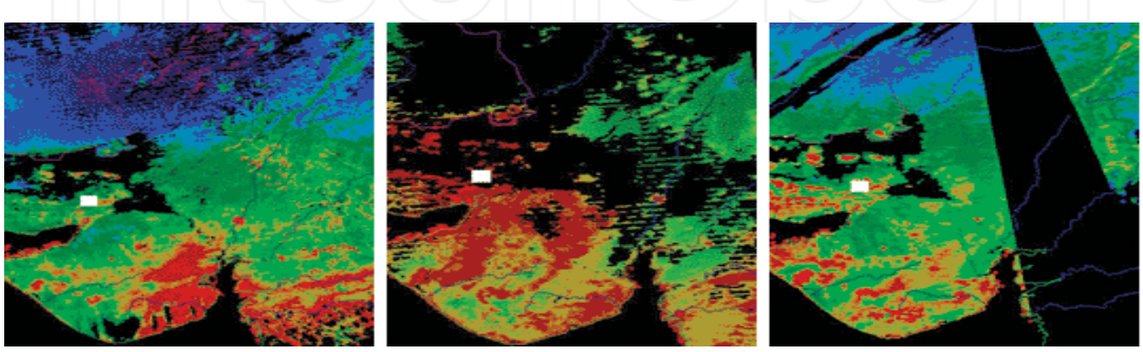


Fig. 3. Infrared radiation detected by satellites n (Bleier & Freund, 2005)

The connection between large earthquakes and electromagnetic phenomena in the ground and in the ionosphere is becoming increasingly solid. Researchers in many countries, including China, France, Greece, Italy, Japan, Taiwan, and the United States, are now contributing to the data by monitoring known earthquake zones.
Some correlations between historical data can be traced as well: monitoring 144 earthquakes (1997-1999), Taiwanese researches noticed significant changes in the electron content of the ionosphere some days before the quakes higher than 6-magnitude.
Therefore, the integration of: (1) several types of sensors (ground and space-based), (2) a network to bring together those signals, (3) a good distribution of the sensors (several sensors in a large area), (4) several types of detection (Ultral Low Frequency (ULF), ELF and magnetic-field changes, ionospheric changes, infrared luminescence, and air-conductivity changes--along with traditional mechanical and GPS monitoring of movements of the earth's crust and (5) the correlation of all data gathered, could make forecast more reliable.

1.2 Analogy with forecasting in cyber security

Cyber attacks can be classified as a set of actions with the purpose of compromising the integrity, confidentiality or availability of computer systems. Cyber attacks can be caused by users or malicious software, which try either to obtain access, to use systems in an unauthorized way, or to enumerate privileges (NIST SP800-94, 2010).
(Internet Crime Complaint Center [IC3], 2010) published a study in the United States about losses in 2009 concerning cyber-attacks: frauds in cyber space caused about $559.7 million of losses in 336,655 organizations. This was a 111,5% increase for the losses and a 22.3% increase for the complaints, as compared to 2008 when 275,284 complaints were received, reporting $264.6 million in total losses. According to (McPherson & Labovitz, 2010), in 2009 the largest reported volumetric Distributed Denial of Service (DDoS) attack exceeded 49 Gbps sustained towards a single target in Europe.
Beyond sheer attack size, (McPherson & Labovitz, 2010) indicated that cyber-attacks become more sophisticated, with attackers expressly aiming to exhaust resources other than bandwidth, such as firewalls, load-balancers, back-end database infrastructure and associated transaction capacity, cached data serving algorithms, etc. This increasing sophistication is a trend that has been captured in previous editions of the survey of (McPherson & Labovitz, 2010) as well. Regarding DDoS attacks, it is expected these attacks to become more common against independent media and human rights sites in 2011, as the recent highly publicized DDoS attacks on Wikileaks, and "Operation Payback" attacks by "Anonymous" on sites perceived to oppose Wikileaks (Zuckerman et al, 2010).
According to (Pontes et al, 2008), (Pontes & Guelfi, 2009a), (Pontes & Guelfi, 2009b), (Pontes & Zucchi, 2010), an early warning system showing a future trend outlook with an increasing number of cyber-attacks, exposed by forecasting analysis, may influence decisions on the security devices adoption (e.g. rules in IDPS combined with rules in firewalls) before incidents happen, according to the needs. Although, three major gaps lie in the studies about forecasting of cyber attacks: a) the use of few sensors and/or sensors employed locally; b) the use of just one forecasting technique; and c) lack of information sharing among sensors to be used for correlation (Pontes & Guelfi, 2009a). Correlation of information between IDPS and forecasters means looking for similar characteristics that may be related (Pontes & Guelfi, 2009a) (Abad et al, 2003). Throughout correlation it is possible to eliminate redundant and false data, to discover attack patterns and understand attack strategies (Zhay et al, 2006).

Nevertheless, forecasts and alert correlation may be challenging as they depend on the reliability of the source of the security alerts (Silva & Guelfi, 2010). Therefore, the precision level of the detection tools is an important issue for validating correlations. Multi-correlation or integration of alerts with information from different sources, e.g. tools for monitoring or operating system logs, can allow a new classification for alerts, improving accuracy of the results (Abad et al, 2003), (Zhay et al, 2006). References (Abad et al, 2003), (Zhay et al, 2006), (Zhay et al, 2004) employed multi-correlation; however neither a detailed analysis concerning influence of isolated alerts in the FP rates, nor forecasting techniques were not applied for predicting future attacks (forecasting).

Forecasting analysis in the information security area can be similar to forecasting methodologies used in any other fields: meteorology, for instance, use sensors to capture data about temperature, humidity, etc (Lajara et al, 2007), (Lorenz, 2005); seismology employs sensors to capture electromagnetic emissions from the rocks (Bleier & Freund, 2005); for economics, specifically stock market, data is collected from diverse companies (annual profit, potential customers, assets, etc) to draw trends about shares of companies (Prechter & Frost, 2002), (Mandelbrot & Hudson, 2006). For any field formal models can be applied to predict events over the collected data. But, before applying formal models, data regarding different kind of variables should be correlated (Armstrong, 2002). According to (Armstrong, 2002), to obtain a more accurate and realistic result about predictions it is suggested: (1) to use diverse forecasting techniques; (2) to analyze information regarding diverse variables and acquired data, from sensors for instance; (3) to employ diverse kind of employed forecasting models.

Concerning cyber attacks, (Lai-Chenq, 2007), (Yin et al 2004) employed forecasting models, however they used just one formal method for predicting events and they did not make use of any kind of correlation process. In this chapter, security events for cyber security are actions, processes that have an effect on the system, disregarding the kind of the effect – in other words, actions that could result in positive or negative effects on the system. In other hand, security alerts are types of security events, indicating anomalous activities or cyber attacks (Silva & Guelfi, 2010). In our earlier works we proposed the Distributed Intrusion Forecasting System (DIFS) (Pontes & Guelfi, 2009), (Pontes & Zucchi, 2010), which covered the following gaps of today's forecasting techniques in IDPS: a) the use of few sensors and/or sensors employed locally for capturing data; b) the use of just one forecasting technique; and c) lack of information sharing among sensors to be used for correlation. Notwithstanding, we faced huge amount of alerts which could have negative influence over forecasting results.

1.3 Proposal

The goal of this chapter is to propose a Distributed Intrusion Forecasting System (DIFS) with a two stage system which allows: (1) in the first stage it is possible to make a correlation of security alerts using an Event Analysis System (EAS); and (2) to apply forecasting techniques on the data (historical series) generated by the previous stage (EAS). The DIFS works with prediction models and sensors acting in different network levels (host, border and backbone), which enables the use of different forecasting techniques (e.g. Fibonacci sequence and moving averages), the cooperation among points of analysis and the correlation of predictions. Additionally to the main goal, the aim of this chapter is proposing an analogous approach for earthquake prediction. As results it is intended to increase reliability of incidents predictions (e.g. earthquake incidents, cyber attacks), to prevent

incidents in a proactive manner and to improve risk management employed for security of the homeland cyber space. A proof of concept of such architecture (DIFS) is presented, which allows concluding about the improvement of forecasts in the cyber space; furthermore, tests applied over two datasets - (Defense Advanced Research Projects Agency [DARPA], 1998) and (Knowledge Discovery and Data Mining Tools Competition [KDD], 1999) - with an IDPS have shown that the employed techniques define incidents trends.
This chapter is organized as follows: state of art concerning forecasting and event correlation in IDPS are in section 2. Section 3 introduces the proposal of this chapter: the DIFS and the two stage system for correlation regarding cyber attacks. Section 4 presents details about the tests and environment to validate the proposal. Results are analyzed in section 5 and section 6 summarizes conclusions and suggestions for new studies.

2. State of art – Cyber attacks, event correlation and forecasting

In this section we approach event correlation for detecting cyber-attacks, the forecasting methods used to predict cyber-attacks and Distributed Architecture for Intrusion Forecasting System (DIFS (Pontes & Guelfi, 2009), (Pontes & Zucchi, 2010).

2.1 Unwanted internet traffic and cyber attacks

The expression "unwanted traffic" was first introduced in the eighties and it has always been related to malicious activity as worms, virus, intrusions etc (Feitosa et al, 2008). Reference (Feitosa et al, 2008) defines unwanted Internet traffic (UIT) as unproductive and useless traffic, with malicious (worms, scans, spam) and benign (wrong setting in the routers) events. Reference (Soto, 2005) completes this definition: UIT may result from the noise in the telecommunication network. (Andersson et al, 2007) classified UIT as the malicious or useless one, with the objective to compromise vulnerable hosts, to spread malicious code, spam, DoS and DDoS. UIT may also be junk traffic, background traffic and anomalous traffic.
Symposiums and workshops have been done about the issue of UIT, like the one promoted by Internet Architecture Board (IAB), on March 2006 (Andersson et al, 2007) and April 2008: the intention was to share information among people from different fields and organizations, fostering an interchange of experiences, views, and ideas between the various research communities. As a result, the Request for Comments (RFC) 4948 details the UIT types, the main causes, existent solutions and the actions to be taken in short and long term. It was decided, in this workshop, that some other research topics about UIT would be managed by the IAB, Internet Engineering Task Force (IETF) and Internet Research Task Force (IRTF).
According to (Feitosa et al, 2008), several of the losses caused by UIT are due to the inefficiency of today's techniques and security devices (anti-spam, antivirus, Intrusion Detection and Prevention Systems (IDPS) (NIST, 2010), firewalls), whether for detecting and preventing the intrusion, or to treat the UIT. Furthermore, the high rates of false positives, false negatives and the lack of a forecasting approach for the Internet traffic are some of the reasons of the UIT increasing. Internet attacks continue apace, with UIT, such as phishing, spam, and distributed denial of service attacks increasing steadily. However, it is important to classify whether it is unwanted or not: Voip (Skype), peer-to-peer (P2P), instant messengers (MSN, Google talk, ICQ), online social networks. Different classification may be employed from one company to another, from user to user, from country to country. China,

for instance, does not allow calls from Skype to telephones. Another example: routers for backbone providers and for small companies - the UIT is differently classified in both cases (Feitosa et al, 2008).

2.2 Approaches for correlation of security events

Correlation techniques for security events can be classified into three categories: (1) rule-based, (2) based on anomaly and (3) based on causes and consequences (Prerequisites and Consequences (PC)) (Abad et al, 2003). The rule-based method requires some prior knowledge about the attack, so the target machine has to pass through a preparation phase called training. The goal of this phase is to make the target machine able to precisely detect the vulnerabilities in which the target machine was trained for (Abad et al, 2003), (Mizoguchi, 2000). Gaps of rule-based method are: (1) it is computer intensive; (2) it results in lots of data; (3) the method works only for known vulnerabilities.

The method based on anomaly analyzes network data flow, using correlation with statistical methods, using accumulation of gathered information and using observations of the occurred deviations throughout processes of network data flow; in a manner to allow detecting new attacks. For instance, (Manikopoulos & Papavassiliou, 2002) demonstrates a system for detecting anomalies which is characterized by monitoring several parameters simultaneously. Reference (Valdes & Skinner, 2001) presents a probabilistic correlation proposed for IDPS, based on data fusion and multi-sensors. However, the method which uses anomaly cannot detect anomalous activity hidden in a normal process, if it is performed at very low levels. Besides, as this method analyzes normal processes reporting only wrong deviations, hence the method is not suitable for finding causes of attacks (Ning et al, 2001).

The PC method lies on connections between causes (conditions for an attack to be true) and consequences (results of the exploitation of a cause), in order to correlate alerts based on the gathered information. This method is suitable for discovering strategies of attacks. Both causes and consequences are composed of information concerning attributes of alerts (specific features belonging to each alert) and are correlated. Arrangement of attributes is called tuple. According to Fig. 4, for the connections to be valid, a preparatory alert must have in its consequences at least one tuple, which repeats in the causes of the resulting alert. In other words, the preparatory alert contributes to the construction of the resulting alert, and therefore it can be correlated. For this connection, illustrated by Fig. 4, the timestamp of the preparatory alert has to come before the resulting alert (Silva & Guelfi, 2010), (Pontes & Guelfi, 2010), (Ning et al, 2001).

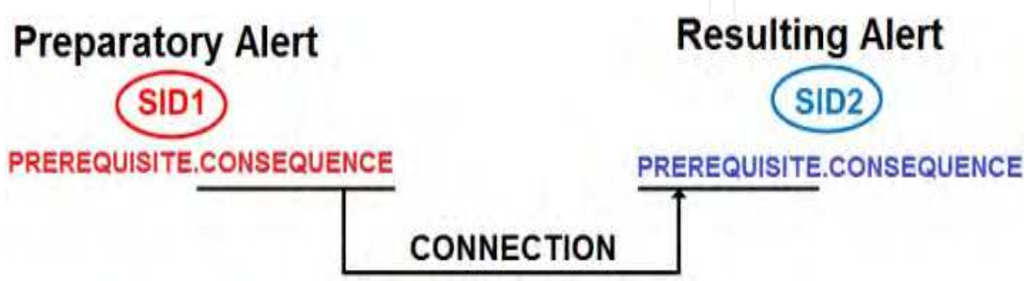


Fig. 4. Connections Between Alerts - Consequence of Preparatory Alert (SID1) is Connected to Prerequisites of Resulting Alert (SID2).

In order to reduce complexity, correlation can be shown in graphs where alerts are represented by nodes and connections are depicted by arrows (representing correlations between alerts).

Yet, some gaps in the PC method may be mentioned, such as the difficulty in obtaining causes and consequences of alerts (Pietraszek & Tanner, 2005), the impossibility to analyze isolated alerts (alerts that are not correlated) and the fact that missed attacks are hard to correlate. An alternative to minimize the problem is to apply complementary correlation techniques (Morin & Debar, 2003), using sensors to work in cooperation, in order to supervise the environment for minimizing missed detections. There are two techniques to map IDPS' alerts and logs obtained from other sources: descending analysis and ascending analysis (Abad et al, 2003), (Silva, 2010).

Descending analysis is based on the investigation of occurred attacks, verifying (correlating) whether other logs (e.g. logs from O.S.) have or do not have vestiges of the attacks' incident. For occurred attack, other traced logs (e.g. Operational System's logs) can be analyzed based on timestamp. This type of analysis is useful to trace evidences about strategies of events, in order to map attacks to its source.

The ascending technique is used to discover attacks by the analysis of several logs. Once an anomaly is detected in one of these logs, other logs are checked based on timestamp. Although ascending technique is computer intensive, this technique allows detecting new attacks.

In an earlier work we proposed the EAS (Silva & Guelfi, 2010), (Silva, 2010), intending to improve results of security events correlation and intrusion detection. EAS is able to make multi-correlation for events from Operational Systems (OSs) and from IDPS (log analysis), consequently, EAS is also capable for verifying the influence of isolated alerts in the cyber-security context.

The EAS architecture has 4 modules, as shown by Fig.5: (a) converter: the aim of this module is to handle the input data into the system (IDPS signatures, alerts and logs from the OS); (b) updating: it controls data which is going to be used by the system; (c) correlating: it does mappings for the correlation processes, FP identification, and the identification of isolated alerts; (d) calculator: it analyzes and compares FP, based on the results from the correlating module.

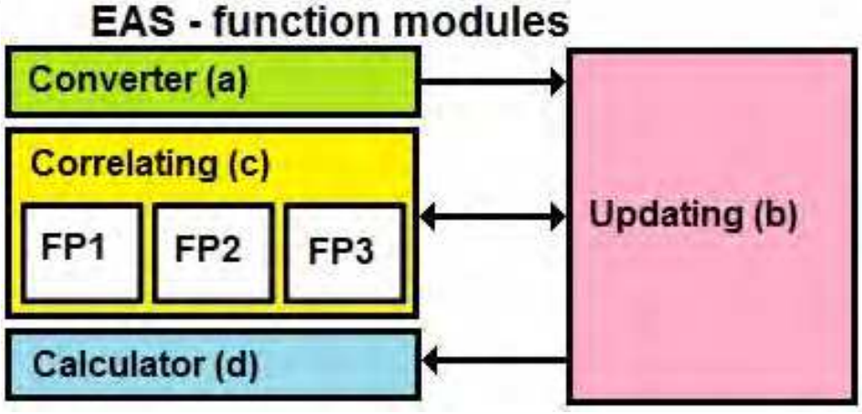


Fig. 5. EAS's Architecture (Silva, 2010), (Silva & Guelfi, 2010)

According to (Silva, 2010), (Silva & Guelfi, 2010), with the employment of the EAS it was possible to improve the today's results of correlation regarding security events, considering the following issues: (1) traceability for causes and consequences within the PC-correlation method (with multi-correlation criteria, correlation analysis (ascending/descending) and identification of FP alerts through tables and graphs); and (2) the process of results validation regarding the correlation. In (Silva, 2010), (Silva & Guelfi, 2010), results of correlating phase were evaluated in three steps (FP1, FP2 and FP3) using tables and graphs. The stepwise analysis allowed comparison of the results. EAS achieved an increase of 112.09% in the identification of FP alerts after the multi-correlation. Another important result of EAS was the evidence of preparatory connections between individual alerts that are in fact part of larger and more elaborated attacks. In other words, EAS can show that individual alerts can be grouped in a single attack, since they are part of the same attack strategy (Silva, 2010), (Silva & Guelfi, 2010).

2.3 Related forecasting methodologies for earthquakes

Statistical based forecast methodologies are used to understand and predict earthquake signals (Kagan, & Jackson, 2000). It is important to discuss these other researches to notice the variety of forecasting applications. Two forecast researches are summarized below.

2.3.1 Earthquake forecasting and its verification

Holliday et. al (2005) has based their forecast research on the association of occurrence of small earthquakes with probably future large ones. In fact, the method does not predict earthquakes, but spots regions (Hotspots regions) where they are most likely to occur in the future (about ten years).

Basically the research objective is to reduce risk areas analyzing the historical seismicity for anomalous behaviour.

The approach is based on a pattern informatics (PI) method which quantifies temporal variations in seismicity and is as follows Holliday et al, (2005):

1. The region of interest is divided into N_B square boxes with linear dimension Δx. Boxes are identified by a subscript i and are centered at x_i. For each box, there is a time series $N_i(t)$, which is the number of earthquakes per unit time at time t larger than the lower cut-off magnitude Mc. The time series in box i is defined between a base time t_b and the present time t.
2. All earthquakes in the region of interest with magnitudes greater than a lower cutoff magnitude M_c are included. The lower cutoff magnitude M_c is specified in order to ensure completeness of the data through time, from an initial time t_0 to a final time t_2.
3. Three time intervals are considered:

a. A reference time interval from t_b to t_1.
b. A second time interval from t_b to t_2, $t_2 > t_1$. The change interval over which seismic activity changes are determined is then $t_2 - t_1$. The time t_b is chosen to lie between t0 and t1. Typically we take t_0 = 1932, t_1 = 1990, and t_2 = 2000. The objective is to quantify anomalous seismic activity in the change interval t_2 to t_1 relative to the reference interval t_b to t_1.
c. The forecast time interval t_2 to t_3, for which the forecast is valid. The change and forecast intervals are taken and forecast intervals to have the same length. For the above example, t_3 = 2010.

4. The seismic intensity in box *i*, $I_i(t_b, t)$, between two times $t_b < t$, can then be defined as the average number of earthquakes with magnitudes greater than M_c that occur in the box per unit time during the specified time interval t_b *to* t. Therefore, using discrete notation, we can write:

$$I_i(t_b, t) = \frac{1}{t - t_b} \sum_{t'=t_b}^{t} N_i(t'), \tag{1}$$

Where the sum is performed over increments of the time series, say days.

5. In order to compare the intensities from different time intervals, it is required that they have the same statistical properties. Therfore, the seismic intensities are normalized by subtracting the mean seismic activity of all boxes and dividing by the standard deviation of the seismic activity in all boxes. The statistically normalized seismic intensity of box *i* during the time interval t_b to t is then defined by

$$\hat{I}_i(t_b, t) = \frac{I_i(t_b, t) - < I_i(t_b, t) >}{\sigma(t_b, t)}, \tag{2}$$

Where $< I_i(t_b, t) >$ is the mean intensity averaged over all the boxes and $\sigma(t_b, t)$ is the standard deviation of intensity over all the boxes.

6. The measure of anomalous seismicity in box *i* is the difference between the two normalized seismic intensities:

$$\Delta I_i(t_b, t_1, t_2) = \hat{I}_i(t_b, t_2) - \hat{I}_i(t_b, t_1). \tag{3}$$

7. To reduce the relative importance of random fluctuations (noise) in seismic activity, the average change in intensity is computed, $\underline{\Delta I_i(t_0, t_1, t_2)}$ over all possible pairs of normalized intensity maps having the same change interval:

$$\underline{\Delta I_i(t_0, t_1, t_2)} = \frac{1}{t_1 - t_0} \sum_{t_b=t_0}^{t_1} \Delta I_i(t_b, t_1, t_2), \tag{4}$$

Where the sum is performed over increments of the time series, which here are days.

8. The probability is defined as a future earthquake in box *i*, $P_i(t_0, t_1, t_2,)$, as the square of the average intensity change:

$$P_i(t_0, t_1, t_2,) = \underline{\Delta I_i(t_b, t_1, t_2)}^2. \tag{5}$$

9. To identify anomalous regions, it is desirable to compute the change in the probability $P_i(t_0, t_1, t_2,)$ relative to the background so that we subtract the mean probability over all boxes. This change in the probability is denoted by

$$\Delta P_i(t_0, t_1, t_2) = P_i(t_0, t_1, t_2) - < P_i(t_0, t_1, t_2) >, \tag{6}$$

Where $< P\ (t\ ,\ t\ ,\ t\ ) >$ is the background probability hotspots are defined to be the regions where $\Delta P_i(t_0, t_1, t_2)$ is positive. In these regions, $P_i(t_0, t_1, t_2)$ is larger than the average value for all boxes (the background level). Note that since the intensities are squared in defining probabilities the hotspots may be due to either increases of seismic activity during the

change time interval (activation) or due to decreases (quiescence). The following hypothesis is taken into account: earthquakes with magnitudes larger than $M_c + 2$ will occur preferentially in hotspots during the forecast time interval t_2 *to* t_3.
To evaluate the model a Relative Operating Characteristic (ROC) diagram, which can be viewed as binary forecast either to occur or not to occur, was used and presented significant results with a relative high proportion of hotspots representing locations of probably future large earthquakes.
Although good results, the model Holliday, J.R., et. al, (2005) could be used as an input in a larger forecast system like DIFSA which would provide the communication and correlation of data with others different models.

2.3.2 Probabilistic forecasting of earthquakes

(Kagan, & Jackson, 2000) has developed a research with both short and long-term forecast approach and testing both with a likelihood function to 5.8-magnitude (or larger) quakes. Although the long-term approach (see Table 1), is not completely developed and is suitable to estimation of occurrence of earthquakes, it is derived from statistical, physical and intuitive arguments while the short-term forecast seismicity model is based on a specific stochastic model and updated daily (see Table 1).
The research assumes that the rate density (probability per unit area and time) is proportional to a smoothed version of past seismicity and depends approximately on a negative power of the epicentral distance and linearly on magnitude of the past earthquakes.
The model (Kagan, & Jackson, 2000) does not use retrospective evaluation of seismic data. The parameters of long-term are evaluated on the basis of success in the forecasting of seismic activity also indicating possible earthquakes perturbations. A maximum likelihood procedure to infer optimal values are applied on short-term approach which can be incorporated into real-time seismic networks to provide seismic hazard estimate.
About the scientific results (Kagan, & Jackson, 2000) concluded that the research depicted a statistical relationship between successive earthquakes in a quantitative way that facilitate hypothesis testing. About the practical results the quantitative predictive assessment can be adopted into mitigation strategies.

Latitude	Longitude	Long-term forecast						Short-term forecast	
		Probability $m \geq 5.8$ eq/day*km^2	Focal mechanism T-axis Pl	T-axis Az	P-axis Pl	P-axis Az	Rotation angle degree	Probability $m \geq 5.8$ eq/day*km^2 time-dependent	Probability ratio time-dependent/ independent
119.5	19.5	3.18E-09	31	208	10	304	64.8	1.79E-14	5.62E-06
120.0	19.5	5.23E-09	17	213	32	314	68.8	1.41E-10	2.71E-02
120.5	19.5	4.28E-08	7	93	75	335	21.4	2.12E-07	5.0
121.0	19.5	3.02E-08	69	135	21	302	28.2	2.84E-07	9.4
121.5	19.5	1.82E-08	77	106	13	296	40.9	6.14E-08	3.4
122.0	19.5	7.81E-09	60	32	3	297	48.4	1.13E-10	1.45E-02
122.5	19.5	4.15E-09	81	228	4	113	51.8	1.00E-12	2.41E-04
123.0	19.5	3.01E-09	78	251	9	110	50.3	7.70E-16	2.56E-07
123.5	19.5	2.43E-09	76	273	13	107	49.5	1.08E-20	4.43E-12

Table 1. Example of long- and short-term forecast, 1999 February 11, north of Philippines.(Kagan, & Jackson, 2000)

The versatility of the methodology based on forecasts is evident in this work, presenting significant results. This scenario shows that quite different methods (e.g, that use and do not use historical data) can be used in conjunction with an approach that uses DIFSA.

2.4 Forecasting for cyber attacks

The forecasting approaches in IDPS lie mainly on stochastic methods (Ramasubramanian & Kannan, 2004), (Alampalayam & Kumar, 2004), (Chung et al, 2006). With no attention about predictions, references (Ye et al, 2001), (Ye et al, 2003), (Wong et al, 2006) 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 (Ye et al, 2001), (Ye et al, 2003) has come to the following findings: 1) The sequence of events is necessary for IDPS, as a single audit event at a given time is not sufficient; 2) Ordering (transaction (Wong et al, 2006)) provides additional advantage to the frequency property, but it is computationally intensive. According to (Ye et al, 2001), (Ye et al, 2003), (Wong et al, 2006), the frequency property by itself provides good intrusion detection. References (Ye et al, 2001), (Ye et al, 2003), (Wong et al, 2006) did not approach correlation for IDPS.

Moving averages (simple, weighted, EWMA, or central) with time series data are regularly used to smooth out fluctuations and highlight trends (NIST, 2009). EWMA may be applied for auto correlated and uncorrelated data for detecting cyber-attacks which manifest themselves through significant changes in the intensity of events occurring (Ye et al, 2001). Both (EWMA for auto correlated and uncorrelated) has presented good efficiency for detecting attacks. EWMA applies weighting factors which decrease, giving much more importance to recent observations while still not discarding older observations entirely. The statistic that is calculated is (NIST, 2009):

$$EWMA_t = \alpha Y_t + (1 - \alpha) EWMA_{t-1} \quad \text{for t=1, 2, …, n.} \tag{7}$$

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

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

Reference (Cisar and Cisar, 2007) gives an overview of adopting EWMA with adaptive thresholds, based on normal profile of network traffic. The analysis of thresholds with EWMA may summarize huge amount of data in network traffic (Zhay et al, 2006), (Pontes & Zucchi, 2010). Diverse moving averages, combined with Fibonacci sequence forecasting approach, were also used by (Zuckerman et al, 2010) to spot trends of cyber attacks in the (DARPA, 1998) datasets.

A simple moving average (SMA) is the non weighted mean of the previous n data. For example, a 10-hours SMA of intrusive event X (DoS, e.g.) is the mean of the previous 10 hours' event X. If those events are: $e_M, e_{M-1}, \ldots, e_{M-9}$. Then the formula is (NIST, 2009), (Roberts, 1959):

$$SMA = \frac{e_M + e_{M-1} + \cdots + e_{M-9}}{10} \tag{8}$$

When calculating successive values, a new value comes into the sum and an old value drops out, meaning a full summation each time is unnecessary,

$$SMA_{current\ hour} = SMA_{last\ hour} - \frac{e_M - n}{n} + \frac{e_M}{n} \quad (9)$$

Nevertheless, the forecasting approaches which use moving averages to cope with cyber attacks in IDPS are limited to analyze cyber attacks individually, e.g. in just one IDPS. Therefore, there is no collaboration among the forecasters. Besides: the concept of sensors is not adopted in (Pontes et al, 2008), (Pontes & Guelfi, 2009a), (Pontes & Guelfi, 2009b), (Pontes & Zucchi, 2010), (Ishida et al, 2005), (Viinikka et al, 2006), (Ye et al, 2003).

3. The distributed intrusion forecasting system with the two stage system (Pontes et al, 2011)

Intrusion Forecasting Systems (IFS) can work proactively in cyber security contexts, as early warning systems, in order to indicate or identify UIT (incidents, threats, attacks) in advance. IFS can also represent an improvement of IDPS, which is based on postmortem approaches (UIT is identified and/or blocked only after they can inflict serious damage to the computer systems). IFS predicts UIT by the use of different forecasting techniques (for instance, moving average, Fibonacci sequence etc) applied either for local or distributed environment. Additionally, for distributed environments, e.g. DIFS, the use of cooperative sensors can improve accuracy about predictions of incidents.

Fig. 6 depicts the proposal of this chapter, i.e. the DIFS and the forecasting levels. Similarly to forecasting methodologies used in other fields (e.g. Meteorology), DIFS also spreads agents and/or sensors widely to make predictions about the different kinds of UIT (spam, virus, intrusion, abnormal network traffic). There are four levels of the IFS: level 1 - independent security devices of hosts; level 2 - integrated security devices of hosts; level 3 - the network level; and level 4 - the backbone level. All levels have some communication degree among each other. In other words, the forecasts obtained from level 1 are shared and correlated to the forecasts of the other levels. Lower levels work as sensors to higher levels; consequently feedback about the UIT trends may be exchanged from one level to another.

Level 1 concerns the trend analysis about incidents, alerts and diagnosis reported independently by the hosts' security devices (antivirus, antispyware, host-based IDPS 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, or the trend about virus infection etc. 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

Level 2 involves correlation of forecasts about the hosts' security devices. At this level, the analysis lays on two databases: a) 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; b) 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. It is important to notice that the databases of IFS level 1 work as sensors for IFS level 2.

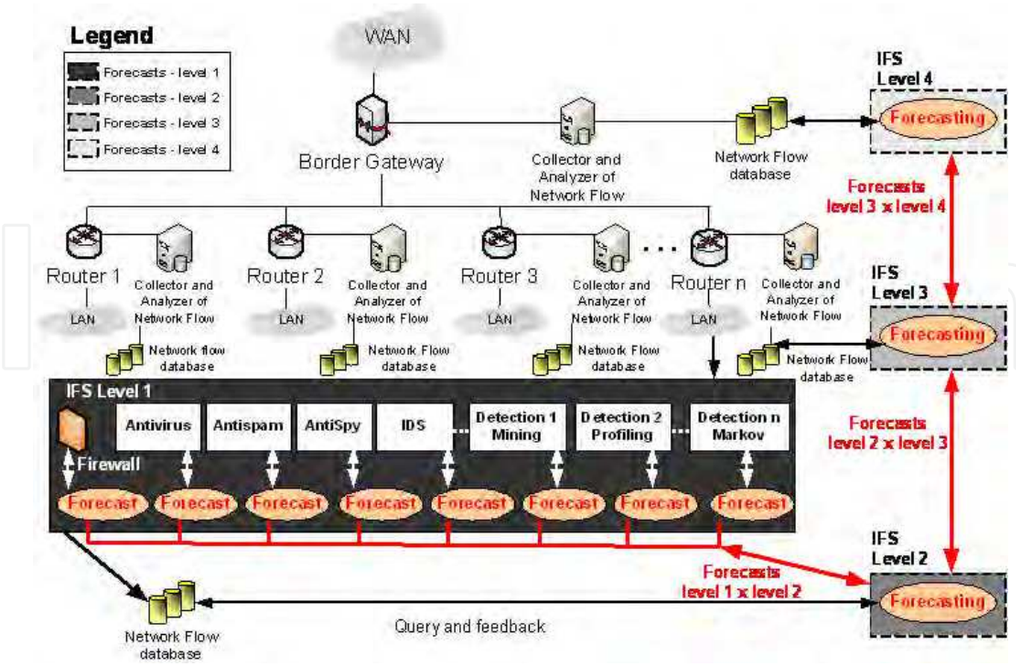


Fig. 6. DIFS Architecture - adapted from (Pontes & Guelfi, 2009)

The implementation of IFS level 3 happens at the gateway of the LAN. IFS level 3 is analogous to IFS level 2, as it queries databases generated by IFS levels 1 and 2. Likewise IFS level 1, some security devices may be installed at the gateway (as firewall, regular IDPS, etc) and they may also be analyzed. The steps for analysis at this level are: a) Network security devices record UIT in databases; IFS level 3 queries the databases provided by the lower levels and current level; b) IFS level 3 analyzes the provided databases to define trends; c) IFS level 3 provides feedback of the trend analysis to the security devices; d) IFS level 3 may also give feedback for the lower levels. It is important to notice that IFS level 1 and level 2 databases work as sensors for IFS level 3. The sensor elements may be more numerous at IFS level 3.

IFS level 4 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: a) Backbone security devices record UIT in database; b) IFS level 4 queries the databases provided by the lower and current level; c) IFS level 4 analyzes the provided databases to define the trends; d) IFS level 4 provides feedback of the trend analysis to the current level; e) IFS level 4 may also give feedback for the lower levels. 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 and correlated among various backbone providers. To correlate forecasts of IFS level 4 means to provide the most realistic and integrated trend about UIT, as it may spread sensors along the network (Lajara et al, 2007).

It is important to notice that for the IFS we implemented a two stage system (Pontes et al, 2011), intending to improve the forecasting results by the use of correlation. Fig. 7 presents the sequence of activities done by the system:

1. The first task is the multi-correlation, running the EAS, to filter FP and tracing sophisticated. During this step, OS's logs, IDPS's logs, network traffic and other logs are analyzed by the EAS. According to Fig. 4, diverse logs and network traffic represent the Entry 1 for the two stage system.

2. The second task is done by the IFS, applying forecasting techniques over the EAS' generated data (historical series, without a considerable amount of FP). Several forecasting techniques may be adopted in this stage (e.g. EWMA, Fibonacci sequence, Markov chains). As illustrated by Fig. 7, EAS' generated data is the Entry 2 for the two stage system. Sep 2 of the two stage system considers just data from Entry 2.

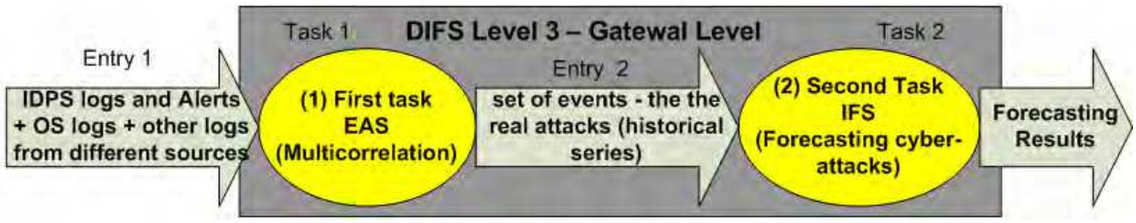


Fig. 7. Sequence of Steps: (1) EAS Filtering – (2) IFS (Pontes et al, 2011)

4. Proof of concept

In this section we are going to describe two of the prototypes we have prepared and analysed. In the first one (Pontes et al, 2009), for the proof of concept, levels 1, 2 and 3 of the DIFS were implemented in three sites geographically divided (A, A' and A''). The following hardware and services were used: a) 1 Pentium core 2 quad 2.0 GHz, 8GB RAM; b) 2 Pentium core 2 duo 1.8 GHz, 4GB RAM; c) 10 virtual machines (Ubuntu 8.04) 512MB RAM; d) 4 virtual machines (WindowsXP) 512MB RAM; e) Windows Vista (host for the virtual machines); VMware Player 2.51; Snort; Netfilter/Iptables; MySQL; OpenVPN.

Likewise (Haslum et al, 2008), 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): SQL injection is an example of this kind of UIT, where typical vulnerabilities that are exploited is buffer overflow and pure environment sanitation; 3) User to root (U2R): SQL injection is also example of this kind of UIT; 4) Probe (Scanning): Nmap, IPswep, Satan are examples of software for scanning. During eight weeks, we simulate usual network traffic and UIT among hosts in each site. Normal network traffic and UIT were also simulated among sites. H-IDPS (NIST SP800-94, 2007) was installed in each one of the hosts. N-IDPS (NIST SP800-94, 2007) was installed at the gateway. Fig. 8 illustrates the sites, hosts with normal activities and infected hosts. Infected hosts inflict UIT to the hosts of each site and to hosts from other 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, A' and A" to site A. For this prototype, IFS was developed in JAVA and it runs in the three levels of DIFS. The IDPS Snort was used to analyze the network traffic. All classified UIT is lately recorded in a MySQL database. IFS collects data from the database, analyzes them and next, when a particular threshold of UIT is exceeded, a warning is sent to the IFS collaborators.

For the second prototype (Pontes et al, 2009), the two stage system was implemented and employed in a wired LAN, specifically in a computer working as gateway for the Internet (level 3 of the DIFS). Elements of level 1 (logs from the OS) were used in the. Although level 3 of the DIFS was approached, level 1, 2 and 4 were disregarded in the second prototype. The reason for implementing only level 3 is the representativeness of the gateway level: (a) the simulated cyber-attacks and the real network traffic have just one path to reach the Internet: throughout

the gateway; (b) at the gateway level it was possible to assure timestamp conditions for correlation processes, as the IDPS is set at the same machine, the EAS and the gateway.

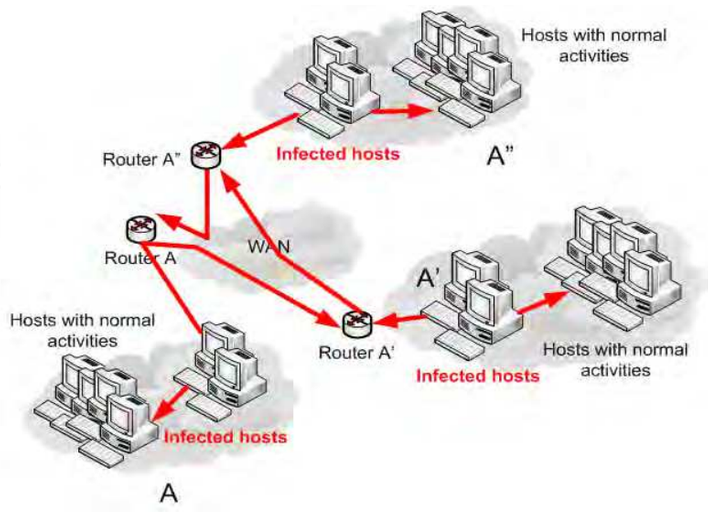


Fig. 8. DIFS Prototype – adapted from (Pontes & Guelfi, 2009)

Fig 9 illustrates the LAN for the tests, which is based on the diversity: diverse machines, settings, protocols and services are executed; further more there are several OS and free access to the Internet. Virtualized OSs (Linux Fedora), using VMWare, the host operational systems with Windows 7 and Windows XP are used in the prototype.

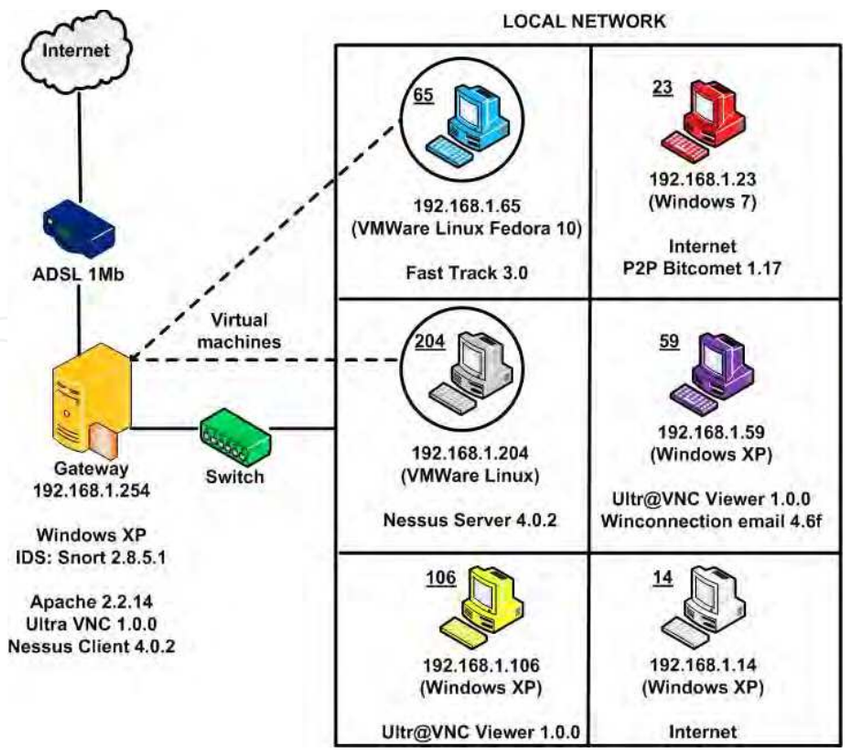


Fig. 9. Environment for Tests of the TSS – Computers, OSs and Services (Pontes et al, 2011)

The computer working as gateway (DIFS level 3) was able to register all alerts of the Network IDPS and logs from its own OS. Table 2 details services used in the two stage system, as the source machines for each service and the reached destiny for each service. In the environment for the tests, multi-correlation was done between alerts from an IDPS with the OS' logs.

Services	Source machine	Destiny
Internet browser	14 and 23	Internet
Remote access (VNC)	59 and 106	Gateway
Peer-to-peer (Bitcomet)	59	Internet
E-mail server (Winconnection)	59	Internet
Complete attack test (Fast-Track)	65	Gateway
Complete attack test (Nessus)	204	Gateway

Table 2. Services in the Prototype (Pontes et Al, 2011)

Table 3 presents applications which were used in the prototype. EAS was developed by the authors, in Visual FoxPro. Finally, Table 3 shows the elapsed time for the prototype. Both simulation of normal network traffic and simulation of cyber-attacks were referred in the prototype. Normal network traffic was brought up as well. Unlike (Pontes et al, 2008), (Pontes & Guelfi, 2009a), (Pontes & Guelfi, 2009b), (Pontes & Zucchi, 2010) Cyber-attacks concern the following types: (1) AWStats - allows remote attackers to execute arbitrary commands via shell; (2) SNMP: remote attackers can cause a DoS or gain privileges via SNMPv1 trap handling (SNMP AGENTX/TCP REQUEST is an example of this kind of attack); (3) P2P: multiple TCP/IP and ICMP implementations allow remote attackers to cause a DoS (reset TCP connections) via spoofed ICMP error messages.

Features	Applications	Time (m)	Details
EAS	Visual FoxPro		
IDPS	Snort	19	13113 signatures
logs Detection	Procmon	19	752851 logs
Graphs	Graphviz		

Table 3. Experiment Applications (Pontes et Al, 2011)

The following hardware were used for our prototype: gateway - Intel Core 2 Duo 2.66 GHz, 3 GB RAM – Windows XP Professional; number 65 – VMWare Workstation 6.0.2 768 MB RAM – Fedora 10 (Fast Track); number 204 - VMWare Workstation 6.0.2 512 MB RAM – Fedora 10 (Nessus Server 4.0.2); number 14 – Intel Core 2 Duo 2.5 GHz, 4 GB RAM – Windows XP Professional (browser's Internet access); number 23 – Intel Pentium 4 3.2 GHz, 4 GB RAM – Microsoft Windows 7 (browser's Internet accesss, Bitcomet 1.17); number 59 – Intel Pentium 4 3.06 GHz, 1 GB RAM – Windows XP Professional (Winconnection E-mail Server 4.6f, Ultr@VNC Viewer 1.0); number 106 – Intel Pentium 4 2,4 GHz, 2 GB –Windows XP Prof. (Ultr@VNC Server 1.0).

It is important to notice that the cyber-attacks considered in this prototype are, in matter of fact, a set of events (alerts and logs) classified as a single and more elaborated attack. In our earlier works (Pontes et al, 2008), (Pontes & Guelfi, 2009a), (Pontes & Guelfi, 2009b), (Pontes & Zucchi, 2010), forecasting techniques considered just individual events in the cyber-security context. Consequently in this paper forecasting techniques are differently

employed, considering the DIFS architecture, as the prototype deals with more refined sets of attacks. Details regarding the EAS and the IFS tasks are not reported in this chapter due space limitations, but the reader may consult (Silva & Guelfi, 2010), (Silva, 2010) and (Pontes et al, 2008), (Pontes & Guelfi, 2009a), (Pontes & Guelfi, 2009b), (Pontes & Zucchi, 2010) for more information relating to EAS and IFS, respectively.

5. Results

Table 4 depicts the results of forecasting UIT in the first 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 4, correct forecasts are the number of times that it was possible to foresee the increasing and/or decreasing UIT's phases, without any delay. 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%.

	A →A′	**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	406	814

Table 4. Results of Forecasting the UIT Propagation Using EWMA and Fibonacci Sequence (Pontes et al, 2009)

Table 5 depicts the results of forecasting UIT with only one forecasting technique (Fibonacci sequence) to the same experiments. The correct predictions' rates were among 5,21% and 7,55%. Forecasts with delay were among 3,92% and 4,68%.

	A →A′	**A →A′ →A″**	**A →A′ →A″ →A**
Overall UIT thresholds	4.320	8.208	16.416
Correct forecast	326	534	855
Forecast with delay	195	384	643
Times not predict	3.799	7.290	14.918

Table 5. Results of Forecasting the UIT Propagation Using Only Fibonacci Sequence (Pontes et al, 2009)

In the second prototype, for the first step (EAS), results are achieved by analyzing consecutive graphs and tables from each phase. Quantity of alerts and correlations are independently accounted, according to the registered route (source and destination). In case the alerts and correlation regards the gateway, whether for source or destination), they are registered as Gateway; the alerts and correlation which disregard the gateway are registered as Non-Gateway. Table 6 summarizes the prototype and some results. Correlation shows a range of attack strategies. In each strategy a number of different alerts are connected sequentially as they were a single attack. A peer-to-peer (P2P) attack performed on machine 23 was chosen for the analysis of forecasting (Fig. 10, Fig. 11, Fig. 12 and Fig. 13).

	Values		Total
Detected alerts	2554 Gateway	1588 Non-gateway	4142
Alert types			137
Isolated alerts	29 (all in FP1)	21 FP / 8 TP	72,41% FP
Correlated alerts	14 FP1 = 21.08%	55 FP3 = 44.72%	
% FP	21.08 (FP1)	44.72% (FP3)	54.22%
% TP	45.78%	10.52% of all TP alerts were isolated	

Table 6. Prototype Results (Pontes et al, 2009)

Fig. 10 depicts the amount of FP which was detected, considering a preliminary correlation without FP filters. Notice there are 17 alerts (nodes) with 69 correlations among them (connections between alerts represented by arrows). Fig. 10 denotes the first scenario for comparisons: the DIFS level 3 work\ing without EAS.

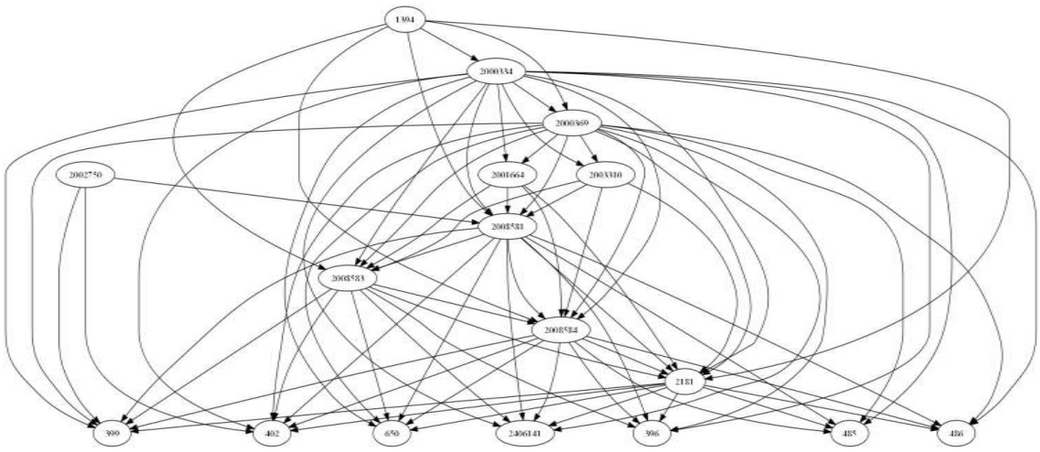


Fig. 10. P2P Graph Attack (TP + FP alerts) (Pontes et al, 2009)

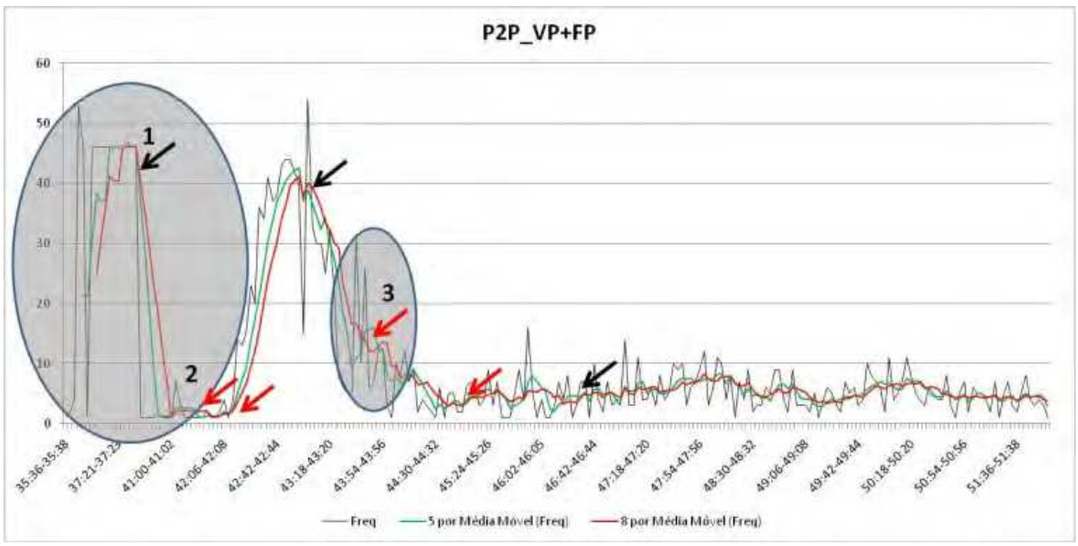


Fig. 11. True Positives + False Positves for P2P Attack (Pontes et al, 2009)

Fig. 11 illustrates the forecasting for cyber-attacks before the use the EAS, specifically for P2P events. Thus Fig. 11 takes into account the same scenario of Fig. 10. The ellipse spots the high volume of FP at the beginning of the experience with the prototype, consequently it is possible to notice three false thresholds for the forecasting, as shown by points (1), (2) and (3). Forecasting was done by the use of diverse EWMA.

Fig. 12 represents the graph after applying EAS filtering. Notice there are just 8 alerts (nodes) with 22 correlations among them (connections between alerts represented by arrows). Fig. 12 denotes the second scenario for comparisons: the DIFS level 3 (gateway level) working with the EAS filtering. As a result by the use of EAS, it was possible to track FP, filtering them, in order to improve forecasts, as the false thresholds for the predictions were eliminated as well.

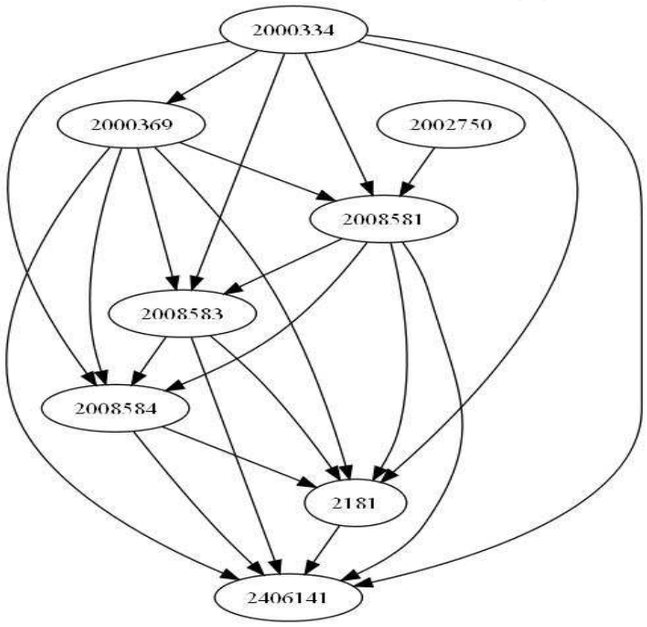


Fig. 12. P2P Graph Attack (only TP alerts) (Pontes et al, 2009)

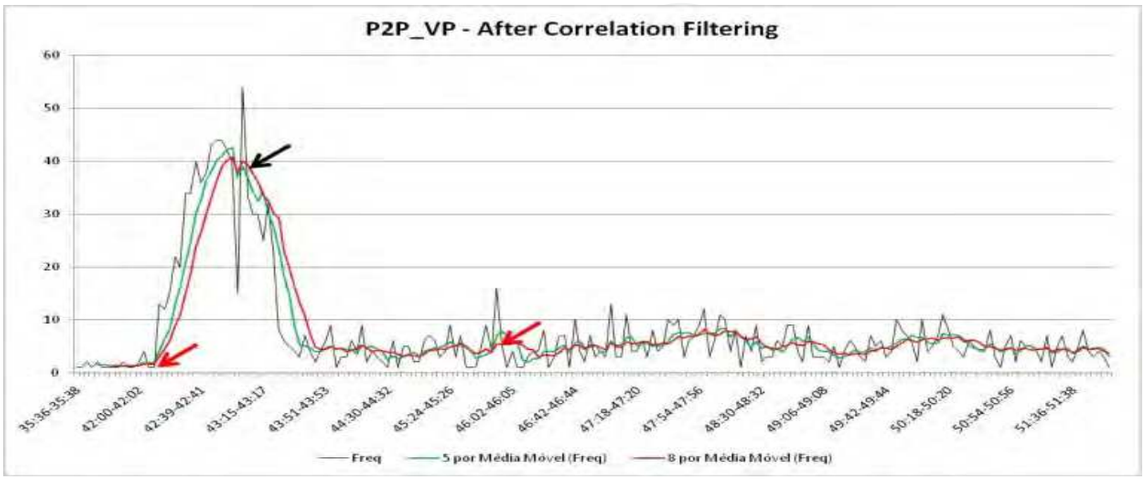


Fig. 13. True Positives for the P2P Attack – After the Correlation Filtering (Pontes et al, 2009)

Fig. 13, in the next page, depicts the application of forecasting techniques (diverse EWMA), i.e. the IFS, after the employment of EAS filtering. In Fig. 13 it is possible to verify two thresholds pointing out the increasing of events (as indicated by the red arrows, and one threshold point out the decreasing of events (as shown by black arrow). Notice there is no significant occurrence of alerts at the beginning of the experiment and two false thresholds regarding forecasts were eliminated. It is also important to observe that the second ellipse with the FP were eliminated after the EAS filtering, hence, another false threshold was wipe out as consequence. More details regarding results can be found in (Pontes et al 2011).

6. Conclusion

As a conclusion, this chapter has introduced the Distributed Intrusion Forecasting System (DIFS) (Pontes et al, 2009), approaching cyber attacks and UIT in the cyber space context. The DIFS also presented the two stage system with the EAS implemented for making the multi-correlation (step 1) (Pontes et al, 2009), afterwards the application of the forecasting techniques over the generated data by the EAS (step 2). The forecasting model presented in this chapter could be analogously employed for earthquake prediction, due the following aspects: a) DIFS, with the Two Stage System and the EAS, was able to track in advance the increasing and decreasing rates of cyber attacks and UIT; hence such methodology may be employed as an early warning system; b) DIFS considers just frequency and temporal characteristics (timestamp) of events (UIT and cyber attacks), thus this approach can be similarly used in other areas.

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. The use of two forecasting techniques represented better results if compared to the use of only one prediction technique. The reason for the accuracy using two forecasting techniques, according to (Pretcher and Frost, 2002), is due to the fact Fibonacci sequence depends on EWMA for marking the first wave. Thus, it was possible to observe just some of the trends drew by the Fibonacci sequence. Another characteristic for predictions with Fibonacci sequence is forecasts in the long term (2, 3 days): EWMAs don't have this feature, so, predictions using only EWMA lack in long term predictions. Employing both of the techniques aggregates the positive of either techniques, making the forecast more accurate.

For the EAS, it was suggested a standard to define causes and consequences within the PC-correlation method combined with multi-correlation criteria, correlation analysis (ascending/descending) and identification of FP alerts through tables and graphs. It was done an experiment with a prototype, in a LAN, with diverse machines and OS, which used a gateway to get access to the Internet. The obtained results from the tests in our prototype indicate that level 3 of DIFS was improved, as some FPs were treated and predictions concerning cyber-attacks were more accurate. It is possible to come to this conclusion by verifying that, despite high FP rates of FP1 (21.08%) and FP3 (44.72%) – see Table III -; during the whole experiment, no TP alert was correlated exclusively as result of an FP alert.

As a suggestion for improving the work, it is suggested to automate analysis' processes that require user interpretation (table correlation and mapping) for using the EAS in real time.

The accuracy of the results can be improved whether the multi-correlation is extended to entire LAN. Regarding the forecast's result, among the suggestions for future works there are the aggregation of the fractal approaches (according to (Mandelbrot & Hudson, 2006)), and the use of other kinds of forecasting techniques (as Markov chains and neural networks) to follow (Armstrong, 2002)'s advices. It is also suggested to extend the employment of the EAS for the

four levels of DIFS, so levels 1, 2 and 4 may be approached in future works. The EAS/DIFS has not yet undergone extensive training enough to be used in commercial applications.

7. References

A. A. A. Silva, "A security event analisys system to identify false positive alerts and evaluate isolated alerts creating multi-correlation criteria". IPT; São Paulo, SP, Brasil, 2010, 107 f. Masters Dissertation in Computer Engeneering.

Abad, Cristina et al. "Log correlation for intrusion detection a proof of concept".. p. 10. In the 19th IEEE ACSAC 2003. University of Illinois as Urbana-Champaign; 2003, ISBN 0-7695-2041-3, pp. 8-12.

Andersson, L.; Davies, E.; Zhang, L.; 2007 "Report from the IAB workshop on Unwanted Traffic March 9-10, 2006", RFC 4948, IETF. 2006

Alampalayam, P.; Kumar, A. "predictive security model using data mining", in proc IEEE Globcom, 2004.

Armstrong, J. S.. Principles of Forecasting: A Handbook for Researchers and Practitioners, (2002). Springer (Ed), ISBN 0792379306, USA, 2002

Bleier, T.; Freund, F. (2005). Earthquake [earthquake warning systems], In IEEE Spectrum. Vol 42, Issue 12, (05 December 2005) , pp. 22, ISSN 0018-9235.

Chung, Y.; Kim, I.; Lee, C.; Im, E. G.; Won, D. "Design of on-line intrusion forecast system with a weather forecasting model", In the Springer ICCSA 2006.

Cisar, P.; Cisar, S. M. "EWMA Statistic in Adaptive Threshold Algorithm", In the IEEE INES, 2007, pp 51-54.

Feitosa, E. L.; Souto, E. J.; Sadok, D. "Tráfego Internet não Desejado: Conceitos, Caracterização e Soluções". in Proc. VIII SBSeg, SBC. 2008 pp. 91-137.

Gula, Ron. Correlating IDS Alerts with Vulnerability Information. Chief Technology Officer – Tenable Network Security; Columbia, MD, EUA, 2007. p. 10.

Haslum, K.; Abraham, A.; Knapskog, S., (2008). Fuzzy Online Risk Assessment for Distributed Intrusion Prediction and Prevention Systems, Proceedings of IEEE UKSIM 2008 10th International Conference on Computer Modeling and Simulation, pp. 216-223, ISBN 0-7695-3114-8, Cambridge, UK, April 1-3, 2008

Holliday, James R.; Nanjo, Kazuyoshi Z.; Tiampo, Kristy F.; Rundle, John B.; Turcotte, Donald L.; (2005). Earthquake forecasting and its verification, Nonlinear Processes in Geophysics,.

IC3 - Internet Crime Complaint Center, "2009 Internet Crime Report" Bureau of Justice Assistance and National White Collar Crime Center, 2010, [Online]. Available: www.ic3.gov, 2010.

Ishida, C.; Arakawa, Y.; Sasase, I. "Forecast Techniques for Predicting Increase or Decrease of Attacks Using Bayesian Inference", In the IEEE PACRIM, 2005, pp 450-453.

Jemilli, F., Zaghdoud, M.; Ahmed, M. B. "DIDFAST.BN :Distibuted intrusion detection and forecasting multiagent system using bayesian network", In the IEEE ICTTA, 2006, pp 3040-3044.

King, Samuel; Chen, Peter; Mao, Z. Morley; Lucchetti, Dominic G. "Enriching intrusion alerts through multi-most causality". In the 12th NDSS 2005, University of Michigan, USA, 2005. p. 13.

Lai-Chenq, C. "A high-efficiency intrusion prediction technology based on markov chain", In the IEEE CISW, 2007.

Lajara, R., Alberola, J., Pelegri, J., Sogorb, (2007) Ultra Low Power Wireless Weather Station, Proceedings of IEEE SENSOR COMM International Conference on Sensor

Technologies and Applications, pp. 469-474, ISBN 978-0-7695-2988-2, Valencia, Spain, October 14-20, 2007

Leu, F.; Yang, W.; Chang, W. "IFTS : Intrusion Forecast and Traceback based on Union Defense Environment", In the IEEE ICPADS, 2005.

Lorenz, E. N. "Designing chaotic models", Journal of the Atmospheric Sciences: Vol. 62, No. 5, ISSN 1520-0469, 2005, pp. 1574–1587.

Mandelbrot, B.; Hudson, R. L. "The behavior of markets: a fractal view of risk, ruin and reward", John Willey, 2006.

Manikopoulos, Constantine; Papavassiliou; Symeon, Network Intrusion and Fault Detection: A Statistical Anomaly Approach. In IEEE Communications Magazine 40, 2002, pp. 76-82 New Jersey Institute of Technology, NJ, EUA, 2002. p. 7.

McPherson, D.; Labovitz, C. "5th Worldwide Infrastructure Sec. Report", 2010, [Online]. Available: http://seclists.org/funsec/2010/q1/295 /, 2010.

Mizoguchi, Fumio, Anomaly Detection using Visualization and Machine Learning. In the IEEE 9th International WET ICE, 2000, pp. 76-82. Science University of Tokyo – Information Media Center; Noda, Japan, 2000. p. 6.

Morin, Benjamin; Debar, Hervé. Correlation of Intrusion Symptoms: An Application of Chronicles. France Télécom R&D; In the 6th International Conference on RAID, 2003, PP. 94-112. Springer-Verlag - Berlin Heidelberg , 2003, G. Vigna, E. Jonsson, and C. Kruegel (Eds.).

Ning, Peng; Cui, Yun. "An intrusion alert correlator based on prerequisites of intrusions". Technical Report TR-2002-01 North Carolina State University; Raleigh, NC, USA, 2002. p. 16.

Ning, Peng; Cui, Yun; Reeves S., Douglas; Analyzing Intensive Intrusion Alerts via Correlation. North Carolina State University; In the 5th International Symposium on RAID, 2002, p. 21. Raleigh, NC, EUA, .

NIST – National Institute of Standards and Technology, (2007). Guide to Intrusion Detection and Prevention Systems (IDPS), In: NIST SP 800-94, December, 2010, Available from: <http://csrc.nist.gov/publications/>

NIST/SEMATECH, e-Handbook of Statistical Methods, 2009, www.itl.nist.gov/.

Pietraszek, Tadeusz; Tanner, Axel. Data mining and Machine Learning – Towards Reducing False Positives in Intrusion Detection. IBM Zuurich Research Laboratory, Ruschlikon, Suécia, 2005. Information Security Technical Report, Vol. 10, ed. 3, pp 169-183.

Pontes, E.; Guelfi, A. E., "Third generation for intrusion detection: applying forecasts and ROSI to cope with unwanted traffic". In Proceedings of 4th IEEE ICITST 09, London, UK, November 2009, ISBN 978-1-4244-5647-5, pp. 1-6.

Pontes, E.; Guelfi, A. E.; Alonso, E. "Forecasting for return on security information investment: new approach on trends in intrusion detection and unwanted traffic". In IEEE Journal Latin America Transactions, 2009, Vol 7, ISSN 1548-0992, pp 438-445.

Pontes, E.; Guelfi, A., (2009). IFS – Intrusion forecasting system based on collaborative architecture, Proceedings of the IEEE ICDIM 2009 4th International Conference on Digital Information Management, pp. 1-4, ISBN 978-1-4244-4253-9, Ann Arbor, Michigan, USA, Nov 1-4, 2009

Pontes, E.; Zucchi, W. L. "Fibonacci sequence and EWMA for intrusion forecasting system". In 5th ICDIM 2010, Lakehead University, Thunder Bat, Canada, July 2010, ISBN 978-1-4244-7571-1, pp. 1-6.

Pontes, E.; Guelfi, A. E., Silva, A. A. A., Kofuji, S. T. "Applying Multi-Correlation for Improving Forecasting in Cyber Security". In 6th ICDIM 2011, Melbourne University, Thunder Bat, Canada, July 2010, ISBN 978-1-4244-7571-1, pp. 1-6.

Prechter, R. R. Jr; Frost, A. J "Elliott Wave Principles", John Wiley, 2002.

Ramasubramanian, P.; Kannan, A. "Quickprop neural network ensemble forecasting framework for database intrusion prediction system", In the Springer 7th ICAISC, 2004, pp 9-18.

Reeves S., Douglas; Ning, Peng; Cui, Yun. "Constructing attack scenarios through correlation of intrusion alerts". In the 9th ACM CCCS, North Carolina State University; CCS'02, Washington, DC, USA., 2002. p. 10.

Roberts, S. W. "Control Chart Tests Based On Geometric Moving Average", Technometrics, pages 239-251,1959.

Silva, A. A. A.; "A security event analisys system to identify false positive alerts and evaluate isolated alerts creating multi-correlation criteria". IPT; São Paulo, SP, Brasil, 2010, 107 f. Masters Dissertation, Computer Engineering Department.

Silva, A. A. A.; Guelfi, A. E. "Sistema para identificação de alertas falso positivos por meio de análise de correlacionamentos e alertas isolados", In the 9th IEEE I2TS 2010, Rio de Janeiro, Brazil, 2010.

Sindhu, S.S.S.; Geetha, S.; Sivanath, S.S.; Kannan, A. "A neuro-genetic ensemble short term forecasting framework for anomaly intrusion prediction", In the IEEE ADCOM, 2006, pp 187-190.

Su, You-Po; Zhu, Qing-Jie (2009). Application of ANN to Prediction of Earthquake Influence, Proceedings of IEEE ICIC '09 Second International Conference on Information and Computing Science, pp. 234 – 237, ISBN 978-0-7695-3634-7, Manchester, UK, May 21-22, 2009

Valdes, Alfonso; Skinner, Keith; Probabilistic Alert Correlation. SRI International; In the 2001 International Workshop on the RAID, 2001, pp. 54-68. Springer-Verlag Berlin Heidelberg , 2001, W. Lee, L. Me, and A. Wespi (Eds).

Viinikka, J.; Debar, H.; Mé, L.; Séguier, R. "Time Series Modeling for IDS Alert Management", A In the CM ASIAN ACM Symposium on Information, Computer and Communications Security, 2006.

Wong, W.; Guan, X., Zhang, X.; Yang, L. "Profiling program behavior for anomaly intrusion detection based on the transition and frequency property of computer audit data", In the ELSEVIER Computer & Security, 2006.

Ye, N.; Li, X.; Chen, Q.; Emran, S. M.; Xu, M. "Probabilistic techniques for IDS based on computer audit data", In the IEEE Transactions on Systems, Man and Cybernetics, pages 266-274, IEEE, 2001.

Ye, N.; Vilbert, S.; Chen, Q. "Computer intrusion detection through EWMA for autocorrelated and uncorrelated data", In the IEEE Transactions on Reliability, pages 75-82, IEEE, 2003.

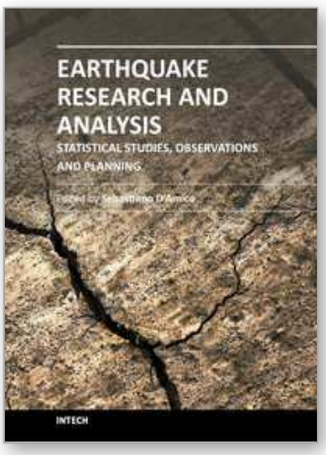
Yin, Q.; Shen, L.; Zhang, R.; Li, X "A new intrusion detection method based on behavioral model", In the IEEE WCICA, 2004, pp 4370-4374.

Zhay, Yan; Ning, Peng; Iyer, Purush; Reeves, Douglas S. "Reasoning about complementary intrusion evidence", In 20th Annual CSAC. North Carolina State University;USA, 2004. pp. 39-48.

Zhay, Yan; Ning, Peng; Xu, Jun "Integrating IDS alert correlation and os-level dependency tracking". Technical Report TR-2005-27 North Carolina State University , 2006, S. Mehrotra et al. (Eds.): ISI 2006, LNCS 3975, pp. 272–284, 2006.

Zhengdao, Z.; Zhumiao, P.; Zhiping, Z. "The Study of Intrusion Prediction Based on HSMM", In the IEEE Asia-Pacific Services Computing Conference, 2008, pp 1358-1363.

Zuckerman, E.; Roberts, H.; McGrady, R.; York, J.; Palfrey, J. "distributed denial of service attacks against independent media and human rights sites", 2010, [Online]. Available: http://www.soros.org, 2010.



Earthquake Research and Analysis - Statistical Studies, Observations and Planning

Edited by Dr Sebastiano D'Amico

ISBN 978-953-51-0134-5
Hard cover, 460 pages
Publisher InTech
Published online 02, March, 2012
Published in print edition March, 2012

The study of earthquakes plays a key role in order to minimize human and material losses when they inevitably occur. Chapters in this book will be devoted to various aspects of earthquake research and analysis. The different sections present in the book span from statistical seismology studies, the latest techniques and advances on earthquake precursors and forecasting, as well as, new methods for early detection, data acquisition and interpretation. The topics are tackled from theoretical advances to practical applications.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen