Security in Cloud Manufacturing: Forecasting and Multi-correlation Techniques for Dealing with Cyber attacks

Elvis Pontes, Anderson A. A. Silva, Adilson E. Guelfi, Sérgio T. Kofuji
Laboratory of Integrated Systems of the Polytechnic School at the University of São Paulo (EPUSP) – São Paulo, Brazil
elvis.pontes@usp.br, anderson@uol.com.br, {guelfi, kofuji}@lsi.usp.br

ABSTRACT: *With the advent of globalization and competitiveness all over the world, manufacturing systems are forced to be revised in order to meet three major qualities –data integration, distributed environment and centralized management. To cover the required qualities for the manufacturing systems, Internet based technologies were developed in the last few years. However, even thought collaboration and distributed access in Internet are regularly approached in those technologies; most of the times manufacturing systems do not consider cyber attacks and the inherent security events of the Internet computer systems. The goal of this paper is to propose a Two Stage System for dealing with cyber attacks, which allows: (1) employment of an Event Analysis System for making multi-correlation of security events detected by an Intrusion Detection System and logs from the computer Operational Systems; and (2) applying forecasting techniques on data generated by the Event Analysis Systems to predict future incoming cyber attacks. The obtained results allow concluding about the enhancement of the accuracy regarding forecasts of cyber attacks. Therefore, by anticipating cyber attacks it is possible to improve the manufacturing systems, given by the failure avoidance (considering data integration, distributed environment and centralized management).*

Keywords: Event multi-correlation, Cloud manufacturing, Cyber attacks, False positives, Intrusion forecasting, Manufacturing systems

Received: 10 June 2011, Revised 29 July 2011, Accepted 31 July 2011

1. Introduction

Companies from the productive sector have always been looking for integration among manufacturing process, information management models and resource sharing (Lan 2009). With globalization and the consequent increasing of competition among companies, technology has became an important ally for business, allowing data integration and distributed environments in a dynamic manner, by the use of a so called Internet Based Manufacturing (Tian et al 2002).

There are diverse models which explore the Internet as a way for integrating productive process, like: Computer Integrated Manufacturing (CIM) (Tian et al. 2002), Agile Manufacturing (AM) (Mehrabi et al 2000), Network Manufacturing (NM) (Chen et al. 2001) and Manufacturing Grid (MGrid) (Tao, Hu, Zhou 2008), among others.

In this context, the Cloud Manufacturing (CMfg) (Zhang et al. 2010; Luo et al. 2011) is a model which combines the use of emergent computer techniques (cloud computing, virtualization and service oriented technologies), with advanced business models for manufacturing regarding the integration of productive processes (Tao et al. 2011), presenting advantages as effective collaboration and making access and the data processing easier (Xu 2011).

In other hand, manufacturing models are becoming closer to the network related technologies, what brings up inherent problems of the computer systems, like cyber attacks and the consequent requirements of security (Pontes et al 2011A).

Cyber attacks can be classified as a set of actions intending to compromise the integrity, confidentiality or availability of computer systems (Feitosa et al 2008). 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 (Scarfone and Mell 2007).

Reference (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.

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 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 (McPherson and Labovitz 2010).

In relation to DDoS, 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).

Nowadays, Intrusion Detection and Prevention Systems (IDPS) are regularly employed for monitoring, detecting and/or blocking cyber attacks (Scarfone and Mell 2007). However, two deficiencies of IDPS can be mentioned: (1) it usually results in a huge amount of data (alerts like False Positives - FP) (Silva and Guelfi 2010); (2) it relies on reactive approaches, as attacks are identified and/or blocked most of the times only after they can inflict serious damage to the computer systems (Pontes and Guelfi 2009).

One way for improving the analysis of data is to correlate information between them, looking for similar characteristics that may be related (Silva and Guelfi 2010; Abad et al. 2003). Throughout correlation it is possible to eliminate redundant and false data, to discover attack patterns and understand attack strategies (Ning and Cui 2002; Zhay et al. 2006; Ning et al. 2002; Zhay et al. 2004; Pontes et al., 2009).

Nevertheless, event correlation may be challenging as it depends on the reliability of the source of security alerts (Silva and Guelfi 2010). Therefore, the level of precision of 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 results accuracy (Abad et al. 2003; Zhay et al. 2006). References (Abad et al. 2003; Zhay et al. 2006; Zhay et al. 2006) employed multi-correlation; however, neither a detailed analysis of the influence of individual alerts in the rates of FP nor forecasting techniques were applied to the prediction of future attacks. According to (Pontes and Guelfi 2009A; Pontes et al., 2009; Pontes and Guelfi 2009B; Pontes and 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.

Forecasting analysis in the information security area can be similar to forecasting methodologies used in 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 and 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 and Frost 2002).

For any field formal models can be applied to predict events over the collected data. Notwithstanding, 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 forecasting in IDPS, (Lai-Cheng 2007; Yin et al. 2004) employed forecasting models, though they used just one formal method for predicting events and they did not make use of any kind of correlation process. In other hand, in our earlier works we proposed the Distributed Intrusion Forecasting System (DIFS) (Pontes and Guelfi 2009; Pontes and 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.

In this paper, 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 and Guelfi 2010).

Therefore, the goal of this paper is to propose a Two Stage System (TSS) which allows: (1) in the first stage it is possible to make multi-correlation of security events using an Event Analysis System (EAS); and (2) to apply forecasting techniques on the data generated by the previous stage (EAS) to predict future incoming cyber attacks.

This paper is organized as follows: state of art concerning Cloud Manufacturing, event correlation and forecasting in IDPS are in section 2. Section 3 presents the proposal of this paper and details about the tests and environment created to validate the TSS. Results are analyzed in section 4 and section 5 summarizes conclusions and suggestions for new studies.

2. Event Correlation and Forecasting in the Cloud Manufacturing

This section regards 1) the concept of Cloud Manufacturing (Armbrus et al. 2009; Xu 2001); 2) event correlation for detecting cyber attacks and incidents related to computer systems (Silva and Guelfi 2010); and 3) forecasting methods used to predict events (cyber attacks) on computer systems (Pontes and Guelfi 2009), (Pontes and Zucchi 2010).

2.1 Cloud Manufacturing

There are diverse concepts in the models of CMfg, but the main ones are cloud computing and smart manufacturing processes, according to Armbrus et al. (2009). Two services are essential in Cloud Computing: applications delivered as a service over the Internet and the datacenters which provide hardware (servers, routers and network infrastructure) and software (applications, security and data) required for user interaction. This kind of software is known as Software as a Service (SaaS) or on-demand software.

In fact, the cloud computing concept is not new, but just recently it has become commercially useful, offering low costs and compatibility between APIs (Application Programming Interface), data encryption, VLANs (Virtual Local Networks), firewalls, geographic scalable storage, backup services (Armbrus et al. 2009).

(Xu 2001) points out that SaaS is just part of the model required for the cloud computing to work. Platform as a Service (a development platform that includes diverse systems and environments) and Infrastructure as a Service (a method of payment in which the customer only pays what he uses) are also part of the application service delivered by a provider through:

- Customer Relationship Management (CRM);
- Web services, service oriented architecture (SOA);
- Quality of Service (QoS), fault tolerance;
- load balancing and virtualization management.

Another important concept is the Smart Manufacturing, a set of features based on software developments that improves the manufacturing processes (reducing time for the tasks to be executed), optimizing activities and supporting the task management. New methods and production procedures support comparisons that can be made between current employed production settings and expected production settings as well, in order for sizing the current state of production plants and, consequently, making earlier detection of anomalous conditions from manufacturing plants (Whitel 2003).

CMfg is based on service-oriented networks that allows centralized management, distribution and sharing of the human resources and manufacturing skills, mainly if they are geographically dispersed. In a CMfg model, assorted resources and abilities can be monitored, connected and managed through the Internet with support for any network technology (e.g. wireless and different protocols) and any manufacturing processes (Zhang et al. 2010; Tao et al. 2011).

CMfg model can focus on the Business Process Management (BPM) applications such as Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) functions (Xu 2011). Nevertheless, the main feature of the CMfg model is the ability to integrate different production models. For example the study conducted by (Zhang et al. 2010) uses a method of integration of resources with more complex tasks, called Composition Resource Service (CRS). The flexibility management of the CMfg model is used to solve dynamic changes that affect CRS.

There are other models to make integration of manufacturing process and network services, like: Agile Manufacturing (AM), Network Manufacturing (NM), Manufacturing Grid (MGrid), Computer Integrated Manufacturing (CIM). However, in cloud computing environments, CMfg is proposed as it has higher efficiency, low consumption of IT resources (as workstations, servers, software and infrastructure for maintaining servers) and it combines production processes and information technology, enabling virtualization, web semantics and integration of information in the entire life cycle of production. Figure 1 illustrates the architecture of CMfg system (Luo et al. 2011; Tian et al. 2002).

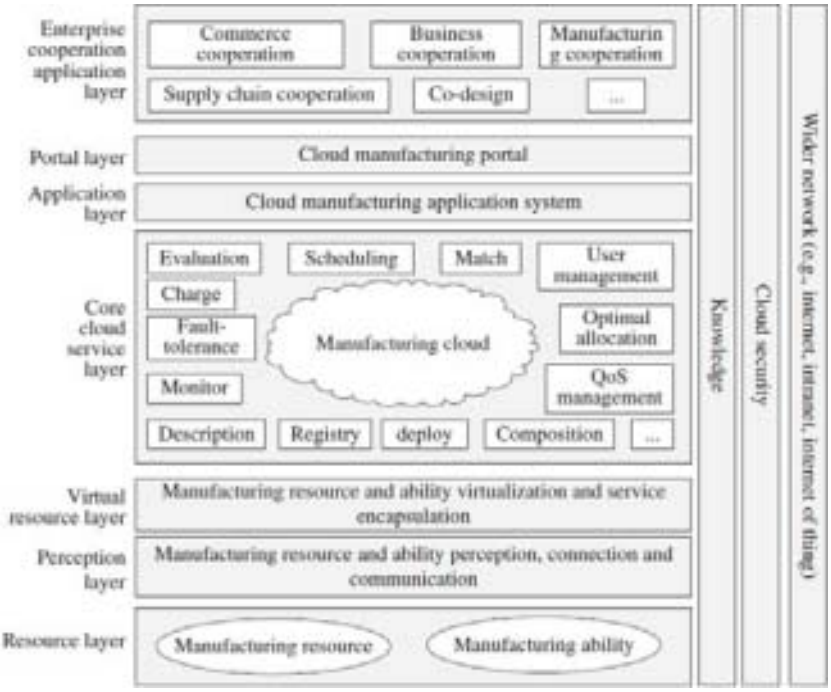

Figure 1. Architecture of CMfg model (Tao et al. 2011)

The architecture of CMfg system illustrated on Figure 1 has some layers (Tao et al. 2011):

- Resource layer: ensures that resources and abilities required by manufacturing processes can be accessed by users as services;

- Perception layer: ensures sizing of resources and abilities can be connected to network for data generation;

- Resource Virtualization layer: is related to virtualizing manufacturing resources and abilities, transforming them into cloud services;

- Cloud Service layer: concerns two different kinds of services - Manufacturing Cloud Service (MCS), which is the result of transforming resources and abilities in accessible service by users; CMfg Core Services which are the main services supporting management and access by operators, providers and consumers in description, registry, publication, evaluation, match and search operations;

- Application layer: involves development of applications based on specific requirements making integration between manufacturing process and MCfg platform (e. g. computer applications customized to manufacturing process and ERP);

- Portal layer: provides interfaces to allow interaction between men and machines in access and invoke MCSs in CMfg;

- Enterprise Cooperation Application layer: accomplishes different types of cooperation application, including in: commerce, business, design and manufacturing in both of services (MCS and CMfg Core Services) included in Cloud Service Layer;

- Knowledge layer: provides essential knowledge for the other layers;

- Cloud Security layer: concerns providing different kinds of security processes and methodologies for the CMfg platform;

- Wider Internet layer: concerns providing the base environment to every resources,services, users and operations connected in the CMfg platform.

Although, the inherent problems found in computer systems are present in the CMfg model, as the CMfg model is implemented networks based technologies. (Xu 2011) emphasizes the worries about intellectual properties managed by external entities on remote servers in the cloud, as well as the sharing of data regarding customers, consumers, employees and business know-how.

The research developed by (Lan 2009) brings out issues like alerts about security management mechanisms that are required to specify different levels of accessibility permissions for different users, the requirement of data encryption transaction methodologies and possible damages caused by virus, trojans and unauthorized access.

Luo et al. (2011) proposes a division of the CMfg model in three view models: function view model, network view model and running view model.

The network view model is divided in four parts (Luo et al. 2011), as depicted by Figure 2:

- resources network: it connects all kinds of manufacturing resources, such as software (data and programs) and hardware (machines, computers and logistic processes);

- sensor network: centralizes, executes and integrates information from various sensors (bar code readers, data collectors, Global Positioning System (GPS) and Radio Frequency Identification (RFID));

- communication networks: different networks and protocols that operate in the cloud manufacturing;

- application network: devices that can provide services and interact with the cloud manufacturing.

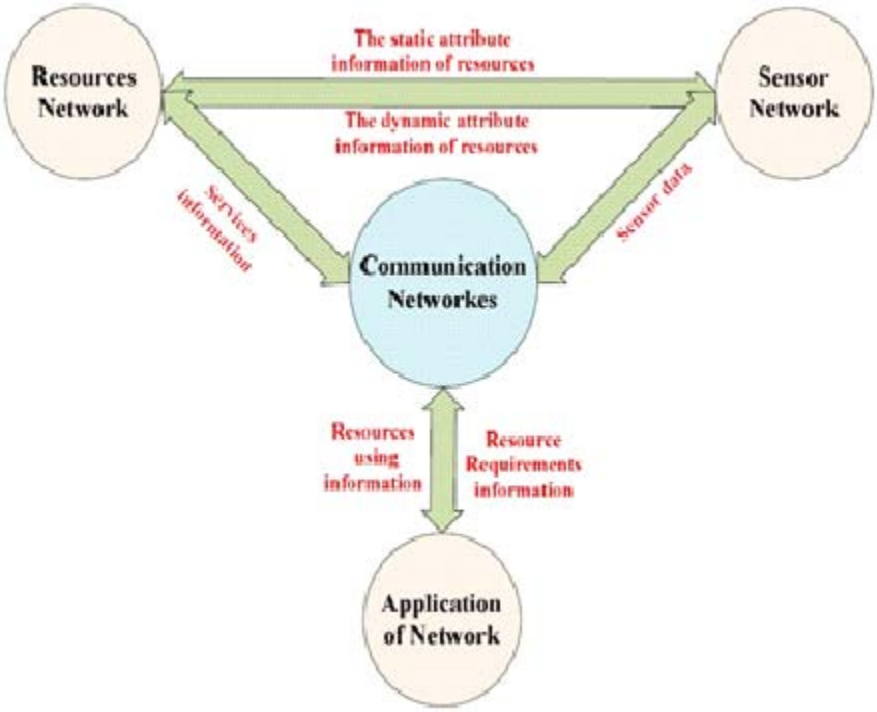

Figure 2. Cloud manufacturing network view mode (Luo et al. 2011)

The network-view model allows risks from cloud computing systems to be isolated and minimized. However, even though some security aspects are considered by (Tao et al. 2011; Kuo et al 2011), CMfg does not neither approach correlation nor forecasting for security events and cyber attacks.

2.2 Correlation Approaches for Security Events (Silva and Guelfi 2010)

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 preciseness 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 by 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 and Papavassiliou 2002) demonstrates a system for detecting anomalies which is characterized by monitoring several parameters simultaneously. Reference (Valdes and 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. 2002).

The method PC 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 information gathered. 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 Figure 3, 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 Figure 3, the timestamp of the preparatory alert has to come before the resulting alert (Silva and Guelfi 2010; Pontes and Guelfi 2009; Ning et al. 2002).

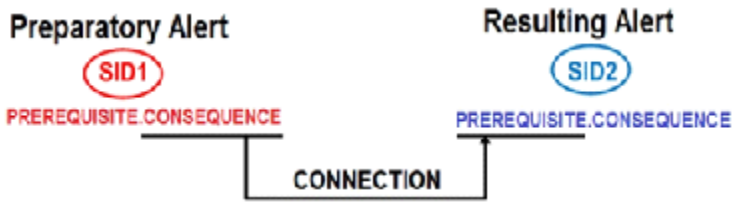

Figure 3. Connections between alerts - consequence of preparatory alert (SID1) is connected to prerequisites of resulting alert (SID2) (Pontes et al. 2011A)

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 an 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 and 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 and Guelfi 2010B).

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 2010, Silva and Guelfi 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 Figure 4: (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.

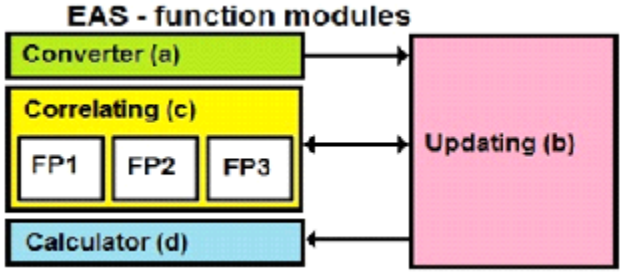

Figure 4. EAS's architecture (Pontes et al. 2011)

For the EAS to assess FPs, three steps are defined (FP1, FP2 and FP3): FP1 is done after correlating alerts from the IDPS, in order to identify eventual isolated alerts and FPs related to normal behavior of the system; FP2 identifies residual isolated alerts; FP3 identifies isolated alerts just after multi-correlation, FP3 assess rates between FPs and isolated alerts.

2.1.1 Converter module (a)

Converter module (a) makes conversion and fields classification, reordering signatures of the IDPS in a data base. In this table, fields are classified as main fields and secondary ones, which can be sub classified as: causes (P), consequences (C) or both (PC). Fields are going to feed the correlating module (c). Main fields contain details regarding alerts, showing source and destination of attacks, as depict by Table 1. In the other field it is listed attributes from signatures concerning specific details of alerts, as CLASSTYPE, MSG, REFERENCE, and other details.

Field	Description
Proto	Alert´s protocol
Origem	Alert´s source IP
porta_o	Alert´s source port
Direção	Alert´s direction
Destino	Alert´s destiny IP
porta_d	Alert´s destiny port
SID	Alert´s ID

Table 1. Alert main fields

2.1.2 Correlating Module (c)

This module creates two tables for correlating tuples and detected alerts. Inside the Correlating Module (c) it is necessary to run the sub modules FP1, FP2 and FP3. In Table 2 (Standard Tuples Table), there are tuples which could be whether causes or

consequences of detected alerts. In Table 3 (Correlating Table), the detected alerts (SID) are recorded in rows and some attributes (SERVICE – main service regarding the alert; VULNERAB – main vulnerability of the alert; EXCLUSIVE – exclusive Operating System (OS) of the alert; VIA – way in which vulnerabilities are exploited) are recorded in the fields CLASSTYPE, REFERENCE and MSG.

Tuples	Description
exe_usu	user-execution
inv_usu	user-invasion
exi_ser	true-service
exi_hos	true-host
ace_inf	information-access
ace_rec	feature-access
ace_ser	service-access
exi_vul	true-vulnerability

Table 2. Standard tuples table

Tuples	Description
inv_adm	administrator-invasion
exe_adm	administrator-execution
ind_sis	system-unavailability
ind_red	network-unavailability
ind_ser	service-unavailability
ind_inf	information-unavailability
ind_rec	feature-unavailability
dis_inf	information-availability

Table 3. Example of correlating table (highlighted link between preparatory alert SID 15930 whit resultant alert SID 1594)

Tuples are recorded whether with "P" (cause), or "C" (consequence) or "PC" (both cause and consequence). For correlating different types of alerts, a tuple recorded as "C" or "PC" can be linked to another, which has the same tuple "P" or "PC" (see Table 3), ever since the timestamp of the first alert (preparatory) is before of the second one (resulting). As a result, Correlating Module (c) creates a graph called c1.

2.1.3 Sub Module FP1

Activities of the Sub Module FP1 are: cutting links, adding links, identifying isolated-FP1 and identifying FP-FP1. Cutting links is a filter for the graphs (c1), as many links are whether not real, or are in a wrong position, so they can be discarded from the graphs when no one of the following criteria are satisfied: (a) contents of the MSG field of the preparatory alert have bonds to MSG field from the resulting alert; (b) the source IP (or destination) of alerts points toward a specific address, as destination address (or source) of other alerts; (c) alerts runtime (timestamp) are close to each other. Even though, this is not a definitive feature, as after all alerts may occur with distant timestamps when a preparatory attack is happening; (d) the SERVICE field of the preparatory alert is whether the same or has bonds to the SERVICE field from the resultant alert; (e) the content of the VULNERAB field of the preparatory alert indicates some kind of relation with the VULNERAB field from the resultant alert; (f) the content of the VIA field of the preparatory alert is identical or has some bonds with other field from the resultant alert; (g) inside of the Local Area Network (LAN), alerts come from the same source; (h) field PORTA_O of a preparatory alert is inside of a range which matches to ranges of the PORTA_D field of a resultant alert.

Adding links: it is possible to come out links between nodes which were not originally linked. Those links are made manually by the same criteria used for the cutting links. Identifying isolated- FP1: isolated alerts are shown in nodes without arrows and are eliminated from the graph. Identifying alerts FP-FP1: based on deleting sequences of nodes which represent normal behavior for the OS, e.g. ICMP requests. As a result, alerts FP-FP1 are eliminated and a new graph is created (FP1).

2.1.4 Sub Module FP2

It is in charge of identifying isolated-FP2: the same adopted criteria for isolated is used. Possible isolated alerts from the previous module FP1 are deleted and a new graph (FP2) is created.

2.1.5 Sub Module FP3

The sub module FP3 is in charge of mapping, the ascending/descending analysis, validating nodes, validating links, identifying FP-FP3, identifying isolated FP3 and mapping isolated FP1-FP2-FP3. Mapping means to correlate the IDPS alerts with the OS logs, by the analyses of timestamps and using a table with IDPS alerts linked to logs from the OS. Ascending/Descending Analysis completes the mapping processes, as it compares services and operations from IDPS signatures with information from detected logs of the OS.

Table 4 describes fields which are used in the mapping process for the ascending/descending analysis. Two modes are used in the ascending/descending analysis: node validation and link validation. In the node validation it is checked if the IDPS alerts have events (processes, files, registry operations) with confirmation status in the OS. The adopted criteria to validate alerts are as follows: (1.1) when source and/or destination of connections are the gateway machine; (1.2) when the main service of the alert is present in fields PROCESS_IN, IMAGE_PATH or COMMAND_LI with the same timestamp. (1.3) when the main operation regarding alerts is present in fields OPERATION or DETAIL with same timestamp; (1.4) when secondary services of the alert are one of the fields PROCESS_IN, IMAGE_PATH or COMMAND_LI with same timestamp; (1.5) when a secondary operation of the alert is present in fields OPERATION or DETAIL with same timestamp; (1.6) when the main operation of the alert is present in the fields PROCESS_IN, IMAGE_PATH or COMMAND_LI with same timestamp; (1.7) when the main service of the alert is present in the OPERATION or DETAIL fields, with same timestamp; (1.8) when a secondary operation of the alert is present in the fields PROCESS_IN, IMAGE_PATH or COMMAND_LI with same timestamp; (1.9) when the secondary service of alerts is present in the fields OPERATION or DETAIL with same timestamp; (1.10) when whether the main or secondary service of the alert is present in the fields PROCESS_IN, IMAGE_PATH, COMMAND_LI, DETAIL or PATH, with different timestamp.

Field	Description	Local
process_na	Executed process	OS
image_path	Process path	OS
event_class	Event class (file, registry or process)	OS
operation	Event operation (read, write, create, etc.)	OS
Path	Event feature or event registry path	OS
Detail	Aditional information from an event	OS
Pid	Process ID	OS
parent_id	Parent process ID	OS
command_li	Process command-line	OS
process1	Alert main service	IDPS
process2	Alert secondary service	IDPS
operation1	Alert main operation	IDPS
operation2	Alert secondary operation	IDPS

Table 4. Description of fields used in the mapping process

Criteria 1.1 to 1.9 are classified as descending analysis. But criteria 1.10 is classified as ascending analysis and shows alerts which must be discarded from the graph, as it highlights services which are not part of settings for the gateway machine.

Validating links verifies whether the present events in the OS confirm possible links between nodes. Adopted criteria are: when the Process Identifier Number (PIN) of the resultant node is son of the preparatory node; (2.2) in case it appears coincident details listed in the content of the field DETAIL from the preparatory and resultant nodes; (2.3) when contents of the field PATH of the resultant node is equivalent or complementary to the preparatory node. After that a new graph (FP3) is generated. The FP3 graph contains alerts from the IDPS which were already mapped to the logs from the OS, with alerts which do not fit to the criteria 1.10.

For identifying FP-FP3, alerts which were not validated in the previous phases (nodes validation and links validation) receive a label as FP-FP3 and are discarded from the graph (FP3). For identifying isolated FP3, by excluding alerts FP-FP3, it is possible to identify and delete new isolated alerts from the graph (FP3). For mapping isolated FP1, FP2, FP3, the next phase concerns the remaining isolated alerts which have last from the phases FP1, FP2, FP3, and which are analyzed just on the node validation mode. As a result, Correlating module (c) sends all data to the Updating module (b), which sends the data to the Calculator module (d) for control and monitoring.

With the employment of the EAS it was possible to improve the current results of security events correlation considering the following issues: (1) traceability for causes and consequences within the PC-correlation method which confirm that individual alerts can be grouped in a single attack, since they are part of the same attack strategy; (2) the process of results validation

regarding the correlation. The results of correlating phase were evaluated in three steps (FP1, FP2 and FP3) using tables and graphs. The stepwise analysis allowed comparing results. EAS reached an increase of 112.09% in the identification of FP alerts after the multi-correlation (Silva 2010), (Silva and Guelfi 2010).

Even though correlation approaches security events and cyber attacks that may occur in CMfg environments, (Silva and Guelfi) does not approach forecasting methodologies for predicting security events and cyber attacks.

2.2 Forecasting Approach (Pontes and Guelfi 2009)

The forecasting approaches in IDS lie mainly on stochastic methods (Ramasubramanian, and Kannan 2004; Alampalayam and Kumar 2004; Chung et al. 2006). With no attention about predictions, references (Ye et al. 2001; Ye et al. 2006, 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. 2006) 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 sufficient; 2) Ordering (transaction (Wong et al. 2006)) provides additional advantage to the frequency property, but it is computationally intensive. Frequency property by itself provides good intrusion detection (Ye et al. 2001; Ye et al. 2006, Wong et al. 2006). References (Ye et al. 2001; Ye et al. 2006, 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 SEMATECH 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 (Roberts 1959):

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

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 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 (Cisar and Cisar 2006) 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 (Viinikka et al. 2006; Ishida et al. 2005; Pontes and Zucchi 2010). Diverse moving averages, combined with Fibonacci sequence forecasting approach, were also used by (Pontes and Guelfi 2009) 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} , … , e_{M-9} . Then the formula is (NIST SEMATECH 2009):

$$SMA = e_M , e_{M-1} , \ldots , e_{M-9} / 10 \qquad (2)$$

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,

$$SMA_{\text{current hour}} = SMA_{\text{last hour}} - (e_{M-n} / n) + (e_M / n) \qquad (3)$$

Nevertheless, the forecasting approaches which use moving averages to cope with cyber attacks in IDS are limited to analyze cyber attacks individually, e.g. in just one IDS (Jemilli et al 2006; Leu et al 2005). Therefore, there is no collaboration among the forecasters. Besides: the concept of sensors is not adopted in (Ye et al. 2003; Vinika et al. 2006; Cisar and Cisar 2007; Pontes et al. 2009).

Intrusion Forecasting Systems (IFS) (Pontes and Guelfi 2009) can work proactively in cyber defense contexts - as early warning systems - in order to indicate or identify attacks in advance. IFS can also represent an improvement of IDPS, which is based on postmortem approaches (threats and attacks are identified and/or blocked only after they can inflict serious damage to the computer systems). IFS predicts attacks by the use of different forecasting techniques (for example, 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 attacks.

Figure 5 depicts the DIFS and the forecasting levels. Similarly to forecasting methodologies used in other fields, DIFS also spreads agents and/or sensors widely to make predictions about the different kinds of cyber attacks. 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 attacks trends may be exchanged from one level to another.

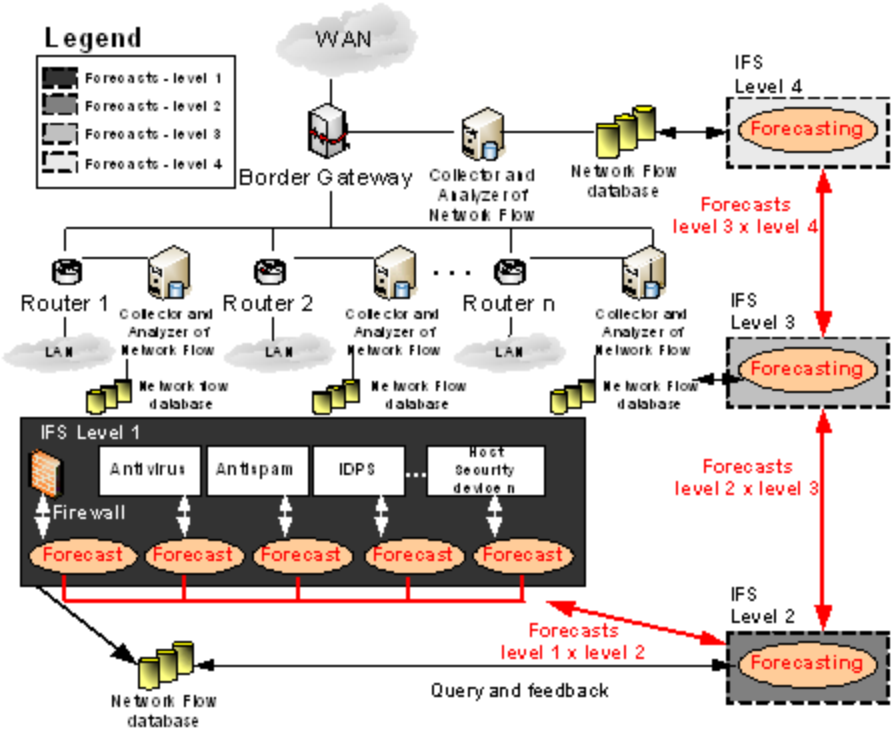

Figure 5. Intrusion Forecasting System (IFS) (Pontes and Guelfi 2009)

3. The Two Stage System (TSS) for Forecasting in Cyber Security (Pontes et al 2011)

In this section we approach the main proposal of this paper. Figure 6 presents the sequence of tasks done by the TSS:

(1) The first task is the multi-correlation, running the EAS, removing FP and tracing sophisticated attacks. During step 1, OS's logs, IDPS's logs and other logs are analyzed by the EAS. According to Figure 6, diverse logs represent the Entry 1 for the TSS. After processing data from Entry 1, as a result the EAS produces a set of events which represents the real attacks (without FPs - Entry 2).

(2) As illustrated by Figure 6, the second task is done by the IFS, applying forecasting techniques over the events from Entry 2 (historical series). Several forecasting techniques may be adopted in this task (e.g. EWMA, Fibonacci sequence, Markov chains, etc). Task 2 considers just data from Entry 2. As a result for Task 2, the TSS is going to provide forecasts regarding the real cyber attacks.

Therefore both the EAS multi-correlation and the IFS work as subsystems for The TSS proposed in this paper.

Figure 6. Sequence of tasks: (1) EAS multi-correlation – (2) IFS (Pontes et al. 2011)

3.1 Test-Environment For The Two Stage System (TSS)

The prototype for the TSS was employed in a wired LAN, specifically in a computer working as gateway for the Internet (level 3 of the DIFS). Although level 3 of the DIFS architecture was approached, level 1, 2 and 4 were disregarded. The reason for implementing only level 3 is the representativeness of the gateway level. The representativeness is given by the following aspects: (a) all internal and external traffic from LAN to WAN goes throughout the gateway; (b) at the gateway level it is possible to assure timestamp conditions for correlation processes, as all the components for the prototype can be set at the same machine.

Figure 7 illustrates the wired LAN for the tests, which is based on: diverse machines, settings, protocols and services. Furthermore there are several OSs and access to the Internet, with no filters (rules in the firewall), Virtualized OSs (Linux Fedora), using VMWare. For the virtualized machines, the host OSs are Windows 7 and Windows XP.

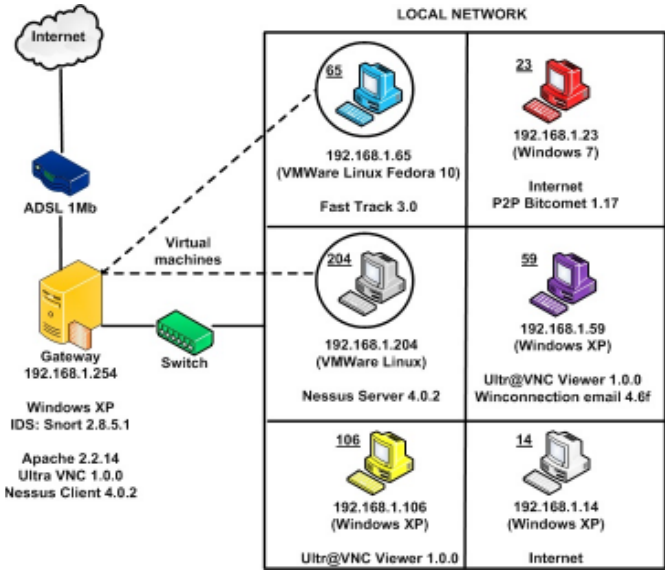

Figure 7. Test-environment – computers, OSs and services (Pontes et al. 2011)

According to Figure 7, the following hardware were used for our prototype: 1) gateway - Intel Core 2 Duo 2.66 GHz, 3 GB RAM, with the EAS and the IDPS installed; 2) machine number 65 – Virtual machine with VMWare Workstation 6.0.2 768 MB RAM – Fedora 10 (Fast Track); 3) machine number 204 – Virtual machine with VMWare Workstation 6.0.2 512 MB RAM – Fedora 10 (Nessus Server 4.0.2); 4) machine number 14 – Intel Core 2 Duo 2.5 GHz, 4 GB RAM – Windows XP Professional (browser's Internet access); 5) machine number 23 – Intel Pentium 4 3.2 GHz, 4 GB RAM – Microsoft Windows 7 (browser's Internet accesss, Bitcomet 1.17); 6) machine 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); 7) machine number 106 – Intel Pentium 4 2,4 GHz, 2 GB –Windows XP Prof. (Ultr@VNC Server 1.0).

The gateway is able to register alerts using the Network IDPS (Snort) and logs from its own OS. Table 5 details services used in the test-environment, like the IP source address for each service and the destination. The IP source addresses represent the machines which executed the attacks. In this environment, multi-correlation was done between alerts from an IDPS and the OS' logs from the gateway. Table 6 presents services used in the prototype. EAS was developed by the authors, in Visual FoxPro. Finally, Table 6 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

Services	IP Source Address	Destination Address
Diverse services using 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 5. Services in the test environment (Pontes et al. 2011)

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

Table 6. Employed tools (Pontes et al. 2011)

with no simulation was brought up as well. Unlike (Pontes and Guelfi 2009; Pontes et al. 2009; Pontes and Zucchi 2011). 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.

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 and Guelfi 2009; Pontes et al. 2009; Pontes and Zucchi 2011), 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 paper due space limitations, but the reader may consult (Silva and Guelfi 2010; Pontes and Guelfi 2009; Pontes et al. 2011; Pontes and Zucchi 2010) for more information relating to EAS and IFS, respectively.

4. Results

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 7 summarizes the prototype and some results.

	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 7. Prototype results (Pontes et al. 2011)

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 (Figure 8, Figure 9, Figure 10 and Figure 11). Figure 8 depicts the amount of FP which was detected, considering a preliminary correlation without multi-correlation. Notice there are 17 alerts (nodes) with 69 correlations among them (connections between alerts represented by arrows). Figure 8 denotes the first scenario for comparisons: the DIFS level 3 working without EAS.

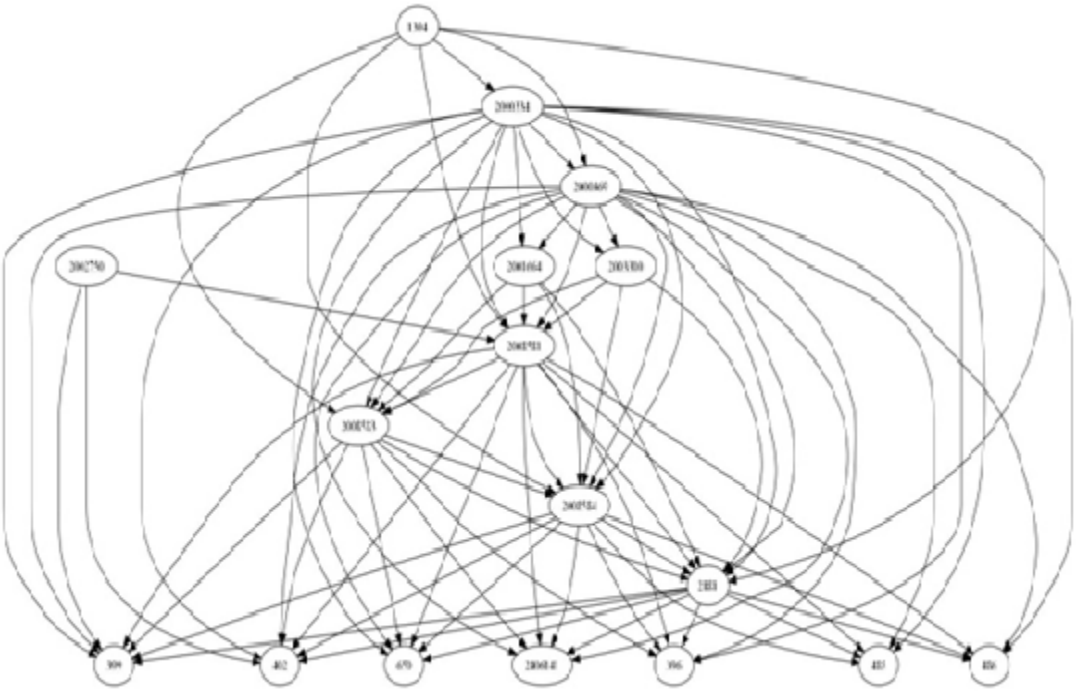

Figure 8. P2P graph attack (TP + FP alerts) (Pontes et al. 2011)

Figure 9 illustrates the forecasting for cyber attacks before the use the EAS, specifically for P2P events. Thus Figure 9 takes into account the same scenario of Figure 8. 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.

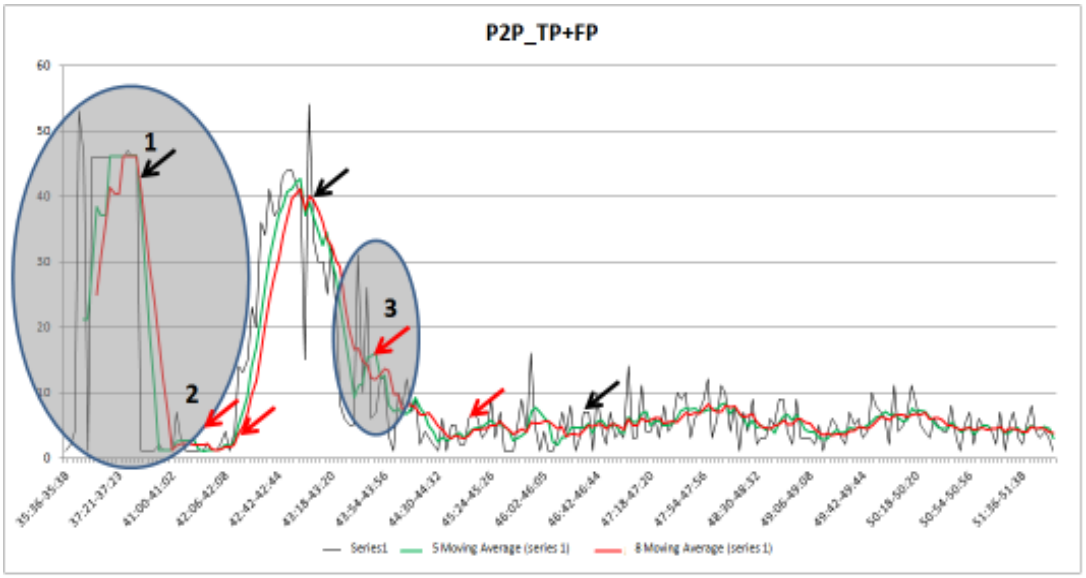

Figure 9. True positives + false positves for P2P attack (Pontes et al. 2011)

Figure 10 represents the graph after applying the EAS multi-correlation. Notice there are just 8 alerts (nodes) with 22 correlations among them (connections between alerts represented by arrows). Figure 9 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.

Figure 10. P2P graph attack (only TP alerts) (Pontes et al. 2011)

Figure 11 depicts the application of forecasting techniques (diverse EWMA), i.e. the IFS, after the employment of EAS multi-correlation. In Figure 11 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 multi-correlation, hence, another false threshold was wipe out as consequence.

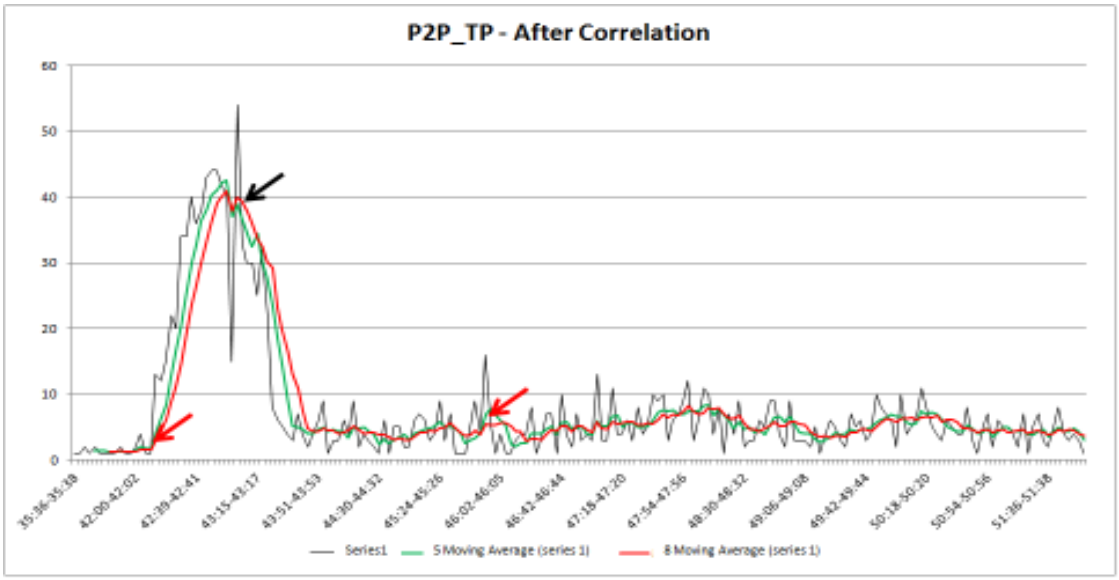

Figure 11. True positives for the P2P attack – after the correlation filtering (Pontes et al. 2011)

Figure 12 is analogous to Figure 9, but it concerns another kind of cyber attack: SNMP attack. Figure 12 represents the use of the IFS before the EAS multi-correlation.

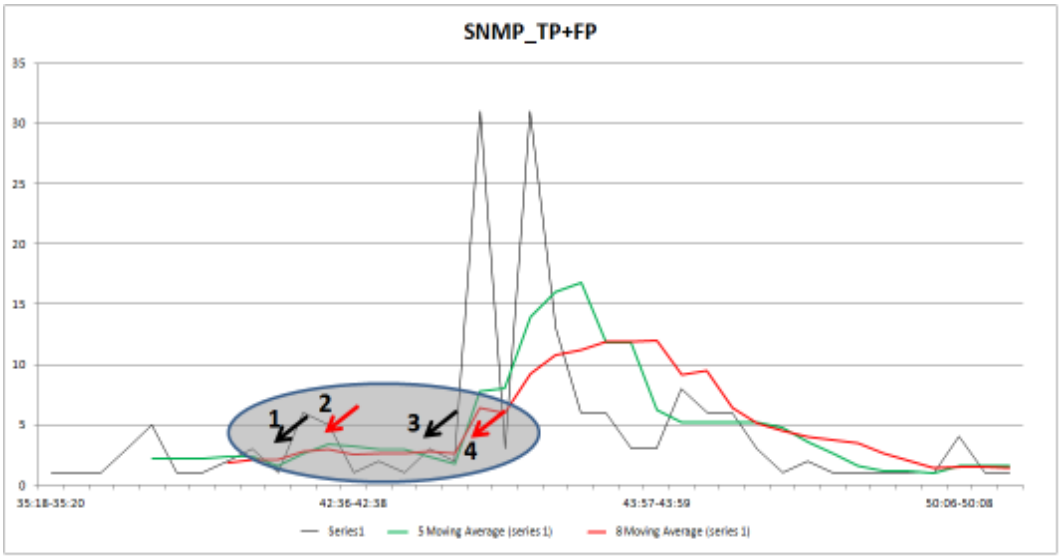

Figure 12. True positives + false positves for SNMP attack (Pontes et al. 2011)

Comparing Figure 12 (IFS before EAS), with Figure 13 (IFS after EAS multi-correlation), it is possible to verify the reduced number of events in Figure 13, as FP are not as many as before the filter. Results of forecasts in Figure 13 are also different if compared to Figure 12.

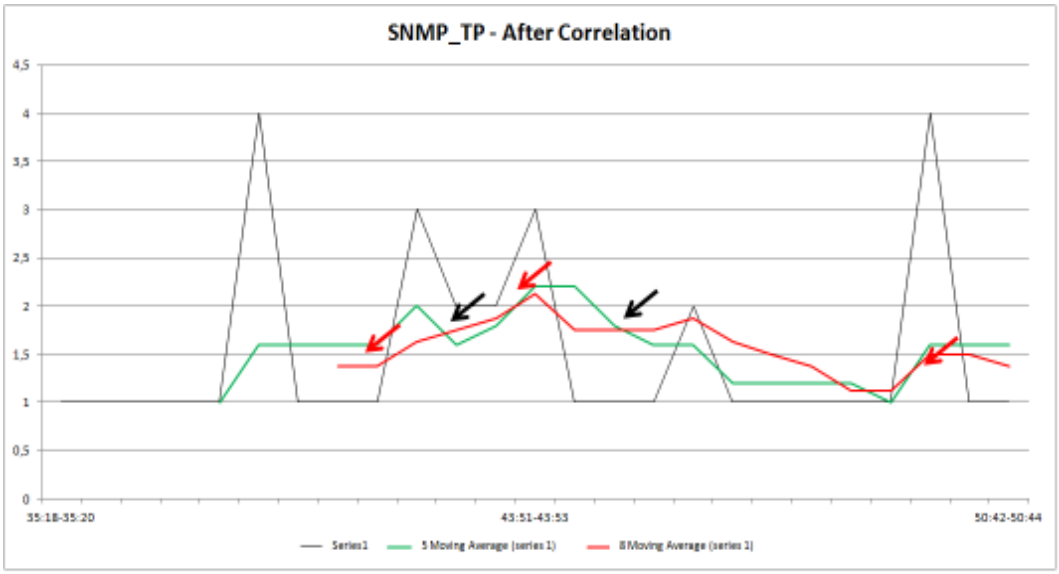

Figure 13. True positives for the SNMP attack - after correlation filtering (Pontes et al. 2011)

Figure 14 brings out results of forecasts with IFS before the use of the EAS multi-correlation, this time for the AWStats cyber attacks.

Figure 15 illustrates results of the use of EAS multi-correlation, and after the IFS. Notice once more the reduction of FP, therefore, elimination of false thresholds of the forecasts.

5. Conclusion

As current manufacturing processes depend on computer network systems, like CMfg, this paper has approached security

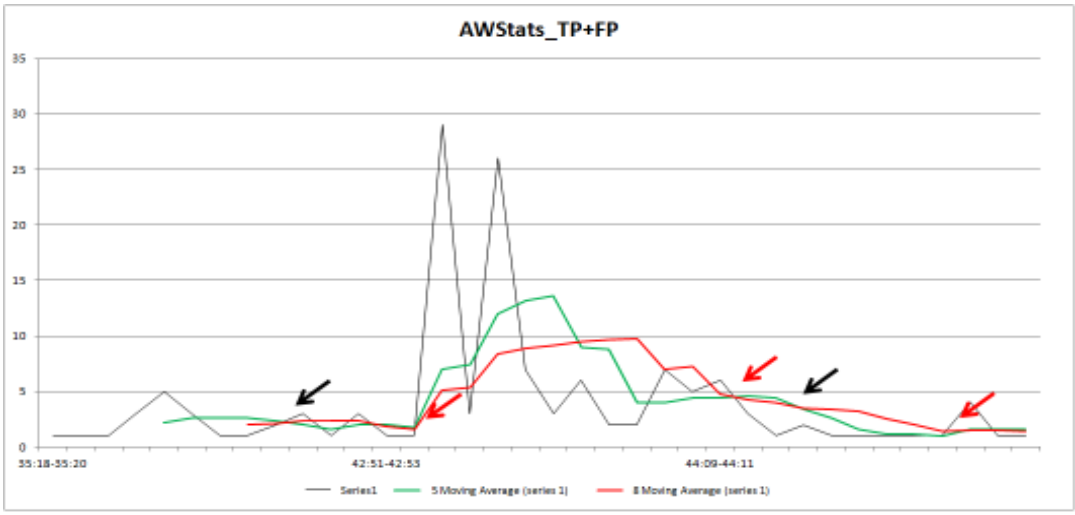

Figure 14. True positives for the AWStats attack (Pontes et al. 2011)

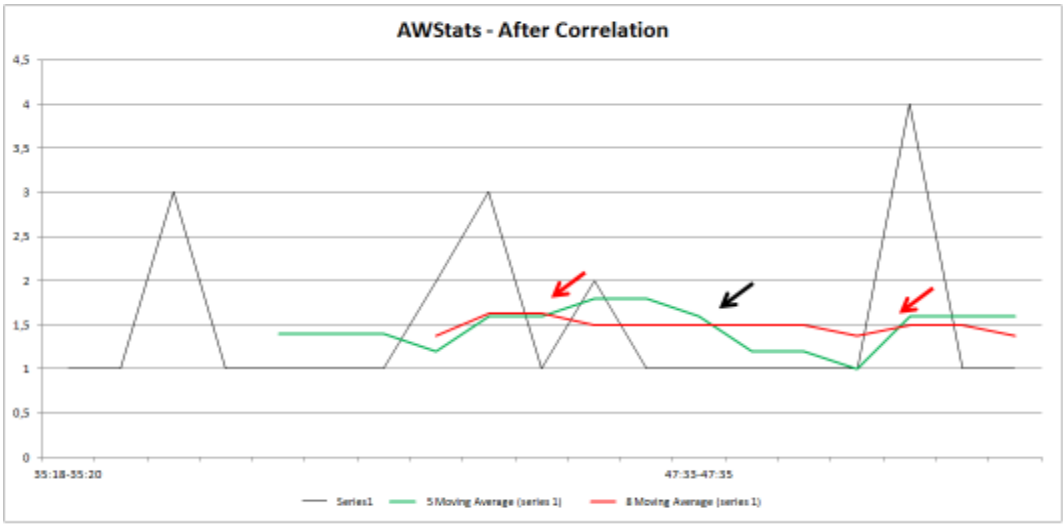

Figure 15. True positives for the AWStats attack - after correlation filtering (Pontes et al. 2011)

issues for those processes, specifically the forecasting of cyber attacks with the use of multi-correlation techniques. As a conclusion, for the approach proposed in this paper, it was presented the TSS with the EAS making the multi-correlation (step 1), and afterwards the application of the forecasting techniques over the generated data by the EAS (step 2).

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, OSs, and only one 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 7 - during the whole experiment, no TP alert was correlated exclusively as result of a FP alert.

Considering that in our earlier works the forecasting models were applied to a wide range of attacks, this paper differs since it focus specific kinds of attacks, called preparatory attacks. As a conclusion we could notice that this approach acts as a filter, checking whether the forecasting technique suffers deviations when applied in different kinds of attacks.

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. This feature contributes to the CMfg model the security of cloud computing means less impact to the manufacturing processes.

The accuracy of the results can be improved whether the multi-correlation is extended to entire LAN. Regarding the forecast's results, among the suggestions for future works, there are the aggregation of the fractal approaches, according to (Mandelbrot and Hudson 2006), and the use of other kinds of forecasting techniques, such as Markov chains, stochastic processes, according to (Armstrong 2002). 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.

The correlation and the consequent separation of the attacks improve forecasting accuracy, as many FP alerts (preparatory attacks) are eliminated. But there is no guarantee that higher percentages of accuracy in forecasting can be achieved simply by defining the preparatory attacks.

References

[1] Abad, C., Taylor, J., Sengul, C., Yurcik, W. (2003). Log correlation for intrusion detection a proof of concept. p. 10. *In*: the *19th IEEE ACSAC 2003*. University of Illinois as Urbana-Champaign. p. 8-12.

[2] Alampalayam, P., Kumar, A. (2004). Predictive security model using data mining, *In:* Proc *IEEE Globcom*.

[3] Armbrus, M., et.al, (2009). Above the Clouds: A Berkeley View of Cloud Computing, Technical Report No. UCB/EECS-2009-28, *Electrical Engineering and Computer Sciences*, University of California at Berkeley, CA, USA

[4] Armstrong, J. S. (2002). Principles of forecasting: a handbook for researchers and practitioners. Springer, USA.

[5] Bleier, T., Freund, F. (2005). Earthquake [earthquake warning systems], *Journal IEEE Spectrum*, 42 (I) 22-27.

[6] Chen, T., Zhang, J., Chunhua, H., Wu, B., Yang, S. (2001). Intelligent machine tools in a distributed network manufacturing mode environment, *Int J Adv Manufact Technol* 17. 221–232

[7] Chung, Y., Kim, I., Lee, C., Im, E. G., Won, D. (2006). Design of on-line intrusion forecast system with a weather forecasting model, *In*: the Springer *ICCSA*.

[8] Cisar, P., Cisar, S. M. (2006). EWMA Statistic in Adaptive Threshold Algorithm, *In: T*he *IEEE INES*, 2007, p 51-54. DARPA, MIT - Lincoln Laboratory, (1998), www.ll.mit.edu/

[9] 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.

[10] Tao, F., Hu, Y. F., Zhou, Z. D. (2008). Study on manufacturing grid&its resource service optimal-selection system, *International Journal of Advance Manufacturing Technology.* 37 (9–10) 1022–1041.

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

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

[13] Jemilli, F., Zaghdoud, M., Ahmed, M. B. (2006). DIDFAST.BN :Distibuted intrusion detection and forecasting multiagent system using bayesian network. *In*: The IEEE ICTTA, p 3040-3044.

[14] Lai-Cheng, C. (2007). A high-efficiency intrusion prediction technology based on markov chain. *In*: the *IEEE CISW*.

[15] Lajara, R., Alberola, J., Pelegri, J., Sogorb, T., Llario, J. V. (2007). Ultra low power wireless weather station, *IEEE SENSOR COMM*, Valencia, Spain, p. 469-474.

[16] Lan, H. (2009). Web-based rapid prototyping and manufacturing systems: A review, *Journal of Computers in Industry* 60, p 643-656.

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

[18] Lorenz, E. N. (2005). Designing chaotic models, *Journal of the Atmospheric Sciences*: 62 (5) p. 1574–1587.

[19] Luo, Y., Zhang L., He D., Ren, L. Tao, F. (2011). Study on Multi-View Model for Cloud Manufacturing, *In: Proceedings of Advanced Materials Research.* 201-203. 685-688

[20] Mandelbrot, B., Hudson, R. L. (2006). The behavior of markets: a fractal view of risk, ruin and reward, *John Willey*.

[21] Manikopoulos, C., Papavassiliou, S. (2002) Network Intrusion and Fault Detection: A Statistical Anomaly Approach. *In: IEEE Communications Magazine* 40, p. 76-82 New Jersey Institute of Technology, NJ, EUA, 2002. p. 7.

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

[23] Mehrabi, M. G., Ulsoy A. G, Koren, Y. (2000). Reconfigurable manufacturing systems: key to future manufacturing, *Journal of Intelligent Manufacturing* 11. 403–419

[24] Mizoguchi, F. (2000). Anomaly Detection using Visualization and Machine Learning, *In*: the *IEEE 9th International WET ICE*, 2000, p. 76-82. Science University of Tokyo – Information Media Center; Noda, Japan, p. 6.

[25] Morin, B., Debar, H., (2003) Correlation of Intrusion Symptoms: An Application of Chronicles. France Télécom R&D; *In:* The *6th International Conference on RAID*, 94-112. Springer-Verlag - Berlin Heidelberg , 2003, G. Vigna, E. Jonsson, and C. Kruegel (Eds.).

[26] Ning, P, Cui, Y. (2002). An intrusion alert correlator based on prerequisites of intrusions. *Technical Report TR-2002-01 North Carolina State University*; Raleigh, NC, USA, p. 16.

[27] NIST/SEMATECH, (2009).e-Handbook of Statistical Methods, www.itl.nist.gov/.

[28] Pietraszek, T, Tanner, A. (2005). Data mining and Machine Learning – Towards Reducing False Positives in Intrusion Detection. IBM Zuurich Research Laboratory, Ruschlikon, Suécia. *Information Security Technical Report*, 10, ed. 3, p. 169-183.

[29] Pontes, E., Guelfi, A., Silva, A., Kofuji, S. (2011). A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI). *In:* Savino, M. (Ed), *Risk Management in Environment, Production and Economy*, (p. 149-170), Croácia, Intech.

[30] Pontes, E., Guelfi, A., Silva, A., Kofuji, S. (2011). Applying Multi-Correlation for Improving Forecasting in Cyber Security. *In: 6th ICDIM 2010*, University of Melborne, Mebourne, Australia, September, p. 1-6.

[31] Pontes, E., Zucchi, W. (2010). Fibonacci sequence and EWMA for intrusion forecasting system. *In: 5th ICDIM 2010*, Lakehead University, Thunder Bat, Canada, July, p. 1-6.

[32] Pontes, E., Guelfi, A. (2009). IFS – Intrusion forecasting system based on collaborative architecture. *In:* the *4th ICDIM 09*, University of Michigan, USA, Nov., p. 1-6.

[33] Pontes, E. A., Guelfi, E. (2009). Third generation for intrusion detection: applying forecasts and ROSI to cope with unwanted traffic. *In:* Proceedings of *4th IEEE ICITST* 09, London, UK, November, p. 1-6.

[34] Pontes, E. A., Guelfi, E., Alonso, E. (2009). Forecasting for return on security information investment: new approach on trends in intrusion detection and unwanted traffic. *In: IEEE Journal Latin America Transactions*, 7, p. 438-445.

[35] Prechter, R., Frost, A. J. (2002). Elliott Wave Principles, *John Wiley*.

[36] Ramasubramanian, P., Kannan, A. (2004). Quickprop neural network ensemble forecasting framework for database intrusion prediction system. *In:* the Springer *7th ICAISC*, p 9-18.

[37] Roberts, S. W. (1959). *Control Chart Tests Based On Geometric Moving Average*, Technometrics, p.239-251.

[38] Scarfone, K., Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS), *NIST SP 800-94* [Online]. Available: http://csrc.nist.gov/publications/.

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

[40] Silva, A. A. A., Guelfi, A. E. (2010). Sistema para identificação de alertas falso positivos por meio de análise de correlacionamentos e alertas isolados. *In:* Tthe *9th IEEE I2TS 2010*, Rio de Janeiro, Brazil.

[41] Tao, F., Zhang, L., Venkatesh,V. C., Luo Y., Cheng, Y. (2011). Cloud manufacturing: a computing and service-oriented manufacturing model. *In:* Proceedings of the Institution of Mechanical Engineers, Part B: *Journal of Engineering Manufacture*.

[42] Tian, Y., Yin, G., Taylor, D. (2002). Internet-based manufacturing: A review and a new infrastructure for distributed intelligent manufacturing, *Journal of Intelligent Manufacturing* 13, p. 323-338, Netherlands.

[43] Valdes, A., Skinner, K. (2001). Probabilistic Alert Correlation. SRI International. *In:* the *2001 International Workshop on the RAID*, pp. 54-68. Springer-Verlag Berlin Heidelberg , Lee, W., Me, L. and Wespi, A., (Eds).

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

[45] Whitel, D.C. (2003). The "Smart" Plant: Economics and Technology. *In:* Proceedings of 2003 FOCAPO; Ft.Lauderdale, FL.

[46] Wong, W., Guan, X., Zhang, X., Yang, L. (2006). Profiling program behavior for anomaly intrusion detection based on the transition and frequency property of computer audit data. *In:* the *ELSEVIER Computer & Security*.

[47] Xu, Xun, (2011). From cloud computing to cloud manufacturing, *Journal of Robotics and Computer-Integrated Manufacturing* 28, p. 75–86

[48] Ye, N., Li, X., Chen, Q., Emran, S. M., Xu, M. (2001). Probabilistic techniques for IDS based on computer audit data. *In:* The *IEEE Transactions on Systems, Man and Cybernetics*, p. 266-274, IEEE.

[49] Ye, N., Vilbert, S., Chen, Q. (2006). Computer intrusion detection through EWMA for autocorrelated and uncorrelated data. *IEEE Transactions on Reliability*, p. 75-82, IEEE.

[50] Yin,Q., Shen, L., Zhang, R., Li, X. (2004). A new intrusion detection method based on behavioral model. *In:* the *IEEE WCICA*, p 4370-4374.

[51] Zhang, L., Guo, H., Tao, F., Luo, Y. L., Si, N. (2010). Flexible Management of Resource Service Composition in Cloud Manufacturing. *In:* Proceedings of the 2010 IEEE IEEM.

[52] Zhay, Y., Ning, P., Xu, J. (2006). Integrating IDS alert correlation and os-level dependency tracking. *Technical Report TR-2005-27 North Carolina State University*, Mehrotra, S., et al. (Eds.): ISI 2006, LNCS 3975, p. 272–284.

[53] Zhay, Y., Ning, P., Iyer, P., Reeves, Douglas, S. (2004). Reasoning about complementary intrusion evidence, *In: 20th Annual CSAC*. North Carolina State University;USA, p. 39-48.

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