Conceptual Modelling of Complex Network Management Systems

Francisco Maciá-Pérez, Iren Lorenzo-Fonseca, Jose Vicente Berná-Martinez*, Jose Manuel Sánchez-Bernabeu
Department of Computer Science and Technology, University of Alicante, Alicante, Spain.

* Corresponding author. Tel.: +34-965903400; email: jvberna@dtic.ua.es
Manuscript submitted October 7, 2014; accepted April 22, 2015.
doi: 10.17706/jcp.10.5.309-320

Abstract: Society, as we know it today, is completely dependent on computer networks, Internet and distributed systems, which place at our disposal the necessary services to perform our daily tasks. Moreover, and unconsciously, all services and distributed systems require network management systems. These systems allow us to, in general, maintain, manage, configure, scale, adapt, modify, edit, protect or improve the main distributed systems. Their role is secondary and is unknown and transparent to the users. They provide the necessary support to maintain the distributed systems whose services we use every day. If we don't consider network management systems during the development stage of main distributed systems, then there could be serious consequences or even total failures in the development of the distributed systems. It is necessary, therefore, to consider the management of the systems within the design of distributed systems and systematize their conception to minimize the impact of the management of networks within the project of distributed systems. In this paper, we present a formalization method of the conceptual modelling for design of a network management system through the use of formal modelling tools, thus allowing from the definition of processes to identify those responsible for these. Finally we will propose a use case to design a conceptual model intrusion detection system in network.

Key words: Network management systems, frameworks and models, conceptual model, business process modeling notation, multi-agent system, service oriented architecture.

1. Introduction

It is impossible to discuss today's society without making reference to the exchange of digital information. In virtually all areas of human activity is present the computing, being the computer networks the basis on which they are sustain. Each day hundreds of millions of data are exchanged between ICT, it should be noted that the number of searches in 2013 with Google [1] exceeded 2 trillion (Europe scale), thus suggests the exchange of data, to which we refer, should be performed on a strong networks structure, without which this would not be possible.

The most recent statistical data [2] show us that currently more than one-third of the world's population lives connected to the Internet, which has caused the increase in the use of ICT, both in the business world and the everyday life [3] and therefore an increase also the use of all kinds of electronic services of quite a different kind and which affect us to a greater or lesser scale, and make us dependent every day, such as banking services, e-commerce , entertainment or even medical diagnosis [4], [5]. Our homes, jobs, study centers or even vehicles [6] worth of networks and distributed services to offer greater possibilities and

characteristics. However, all these existing distributed systems require a set of sophisticated management systems for its maintenance, sustainability, security and proper functioning.

Often these systems of management of the own distributed systems are not taken into account during the development of the systems themselves and have to be developed to ex post facto as occurs for example with intrusion detection systems, monitoring systems and services activity, antivirus, systems of regeneration of network nodes, etc. In this work we propose a conceptual model as a basis for the systematic design of these network management systems. It should be noted that these management systems are secondary tasks but that many times their cost is even greater than the own main system they support and ignore them can produce the main failure of the system. It is therefore necessary to define a correct and methodical model capable of laying the foundations for the design of a comprehensive efficient and robust framework.

Now there is talk of system-of-systems, which embrace the diversity of technology, operators, and connections, each of them has its own configuration and its own communication, although currently there is a notable trend to homogenize the protocols. In spite of this, this heterogeneity has become an important factor in the complexity of the systems and increases the difficulty to generalize the management actions across distributed systems with different features and architectures [7]. Furthermore, both behaviour and workload that cause users is constantly changing, as well as both hardware and software upgrades and modifications are often doing that the system itself includes a great deal of uncertainty [8], [9]. The complexity in the management of distributed information systems comes from by both of its huge scale, its dynamics and heterogeneity.

Various initiatives have emerged to try to propose methodologies, protocols or standards that allow the management of the means and resources of these distributed systems. A clear example is the initiative proposed by the ISO, which under the direction of the OSI group has created a model of network management as a way to understand the major functions of network management systems. This model called FCAPS [10], currently known as FAB [11], categorized the network management functions in 5 groups [12], [13]: fault, configuration, accounting (or usage statistics), performance and security. Another proposal of the ITU-T is the model protocol Telecommunications Management Network (TMN) for the management of open systems in communication networks [14], [15] that identifies four logical layers in the network management: business, services, network and network elements. Of them have emerged as CMIP standards (ITU-T X. 711, 1997- ISO/IEC 9596-1, 1998) or SMNP [16] with the purpose of giving support to the management of the means of dissemination of distributed systems.

Security management is another of the great cores in the management of distributed systems [17]. Cyber-attacks have increased significantly in recent years worrying. Until 2003 the growth in the number of attacks referred to the CERT (CERT -Computer Emergency Response Team) has been alarming and exponential. The CERT maintained control of the statistical attacks only until the year 2003 due to the widespread use of automated tools of attacks has made the figures of banal incidents, providing little information with respect to the evaluation of the scope and impact of the attack [18]. This complex situation in the information systems and networks has brought about the development of research [19]-[25], with the purpose to create security mechanisms, identifying three essential security measures: prevention, detection and evasion [26]. Security in a system includes the fight against the malice of users, the errors or simply bad luck. It is a discipline focused on the tools, processes, and methods required for the design, implementation, testing, and adaptation of systems. Requires personnel with interdisciplinary experience, with knowledge of cryptography, security of computers, hardware knowledge and formal knowledge in economics, psychology, organization and legislation [27].

At present, the Cloud Computing and the Smart concept, are becoming new paradigm of information

technologies at the global level [28] that have been incorporated into companies of great timing such as Amazon, Microsoft, Google or IBM [29]. The need to provide greater efficiency in infrastructure and services in the systems [30], and particularly in the cities, have coined the fashion term Smart City, which is a model of large scale management of resources, services and processes and ultimately of a network of relatively large quantities. This implies that the new scenario that occurs now is even more distributed and with greater uncertainty since many devices and systems that will be part of our applications are totally unknown to us. This complexity makes it even more the security control in its various aspects [31] related to both the illicit activities of users, viruses or malware as of one's own integrity of the systems related to monitoring of the services, the proper operation of the applications, broken hardware, etc.

1.1. Scope of This Work

Thus, reasons that we can identify the need for methodologies, tools, techniques, and conceptual models to help lay the modelling foundations of network management systems that allow the management of distributed systems, in all aspects in the management that intervenes, and without a significant cost on the realization of a distributed system. Management and administrative functions are secondary to the primary functionality of a distributed system and therefore should be a task, which although it is complex, can be carried out easily.

1.2. Structure of This Work

The rest of the article is organized as follows: in Section 2 we provide a methodology for the conceptual modeling of a network management system, which will allow us to define, in a precise, formal tools and approach to covering the stage of analysis and requirements capture. A case study as an experiment, which has served as a validation of the proposed model is showed in Section 3. Finally, our conclusions and future work in Section 4.

2. Conceptual Model

If the uncertainty principle ("what you're studying, you change", Heisenberg) is a problem derived from the observation of any system, a Network Management System (NMS) not only cannot escape from this principle, but that represents one of its leading exponents. In the end it is a network service of the same nature as those that you want to manage, execute and depends on the same resources that will be affected in case of failure or malfunction, each action to manage the system will have a direct and immediate impact on the own NMS. For this reason, far from to avoid or minimize this principle, the approach followed to develop our conceptual model for the NMS (CMNMS) is precisely the assumed by fully from the start in such a way that, for us, to define a conceptual model of a NMS is converted to shape the main basis of the system you want to manage, or, what is the same, modeling the network of computers to manage incorporating intrinsic form a network management system and becoming commonplace as well the principle of uncertainty, i.e. CMNMS ≡ Network Model + CNMS.

Taking into account that a model must be a valid simplification of a reality, adaptable to our interests, we will have to make sure that reflected all the important elements for the development of the NMS and try to ignore all the details of the network that are superfluous.

The Conceptual Model (CMNMS) focuses on describing the main tasks of the NMS, allowing you to view the system through the processes (P) that are carried out within the same and identifying their requirements, this model as we represent as follows in Fig. 1.

The goal of this model, through the analysis and capture of requirements, is to describe the domain of our problem. The source of fundamental knowledge on which it will support the analysis is the experience and knowledge accumulated by the experts: networks and systems administrators in general. Since the

ConcepModNMS, transferred to the vision that the experts can have of the system, is to represent in a simplified manner a way of thinking, the more comfortable approach to follow is to identify the different objects to manage (information, files, applications, resources, etc.) those responsible for them, the activities involved and the steps to be followed in each one of them. In addition, when the NMS must defend the interests of an organization, public or private, these experts will have to make sure that all of this takes place in a manner aligned with the overall policies of the organization.

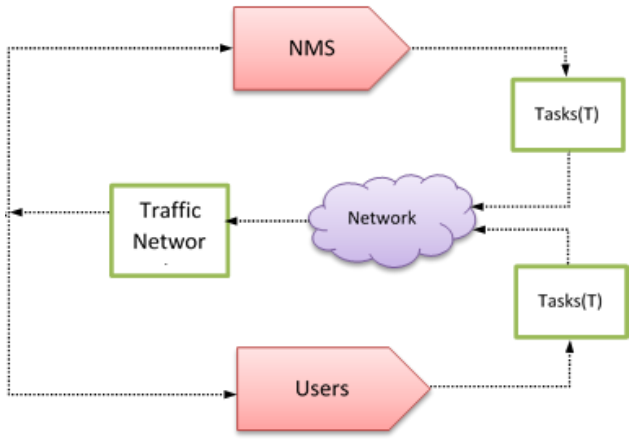

Fig. 1. Conceptual model (NMS ConcepModNMS).

Once identified as it will be a model, it is important to be able to define a method that enables us to get it in a systematic way and, if possible, to facilitate put it formally to the ambiguities introduced are minimal and your understanding is simple. For this reason, the proposed conceptual model is based on a method of formalization of CMNMS and a set of modeling tools, which will support us for this development, as a (1).

$$\text{Conceptual Model}=\langle\text{Formalization Method CMNMS, Formalization Tools}\rangle \quad (1)$$

In Fig. 2, we propose a method in which identify the conceptual modeling phase that will serve as support to different models that take as a basis the CMNMS and a set of modeling tools.

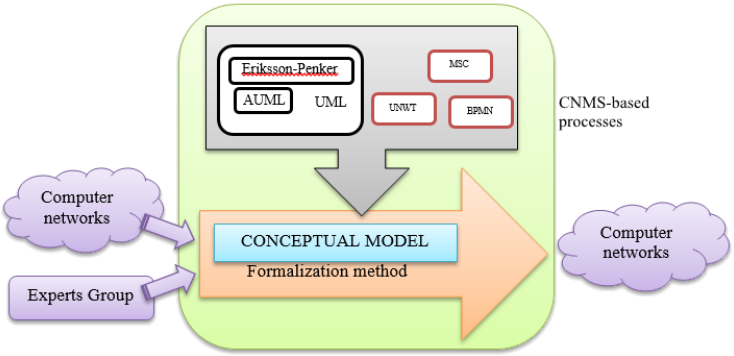

Fig. 2. Main elements employed in the conceptual modeling of the NMS.

In this way, the method of formalization consists, basically, in the development of a conceptual model formally described as in (2).

$$\text{Formalization Method CMNMS}=\text{Procedure for Models}C\ M\ /\ M \in \{\text{ConcepModNMS}\} \quad (2)$$

On the other hand, the tools used are defined by the formalisms that are used for the specification of each

model, such as UML [32]-[34] and its notations arising from, or the language Message Sequence Chart MSC or the now historic Object-Modeling Technique (OMT). Is expressed as in (3).

$$\text{Formalization Tools}=(\text{UML, BPMN, MSC, OM}) \tag{3}$$

Thus the proposed formalization method will be through the use of the UML language as a common language and basic definition, using different variants are better adapted to our interests, for example: the UML extension for Erikson-Penker processes, but any of the other languages, both MSC or WTO, can be used depending on the tools used by the organization.

Taking into account the characteristics of the model and the need to align with the interests of the organization, through the modeling processes [35] emerges as a very appropriate methodology, widely tested in the business domain and a set of formal tools that are well suited to our needs [36].

The concept of process has often been defined because it is the foundation of the new approaches to business organization as a basic principle of obtaining satisfactory results in an efficient way [37]. The standards family ISO (International Standardization Organization) 9000 conceptualized as a process: a set of mutually related activities or that interact, which transformed input elements into results [38].

This definition is enriched with important concepts managed within the Business Process Management (BPM). BPM is the business methodology whose objective is to improve efficiency through the systematic management of business processes [39], [40]. Within this describes a process through the following features:

1) Has a goal.
2) Has a specific input.
3) Has a specific output.
4) Uses resources and can be change their states.
5) It is composed of activities that are executed in a specific order.

According to this, we define formally the set P composed of all the processes p identified and defined in the system, where each $p\in P$ is composed at the same time, by a tuple consisting of a set A_p of actors αi responsible for the development of the process p, a set R_p of ri resources involved in the same and a sequence sorted in workflow WF_p of ti tasks, where $A_p\subseteq A$ and $R_p\subseteq R$. Formally we will call the next tuple $p=\langle A_p, R_p, WF_p\rangle$.

To define the sequence ordered of tasks has been chosen by the definition of a graph in which nodes are tasks, $ti\in T_p$, $T_p\subseteq T$ and the edges with a set IT_p of indexes that the preservation microfilming. Formally expressed as (4)

$$WF_p=\langle T_p, I_{Tp}\rangle/T_p\subseteq T\wedge_{Tp}\subseteq N \tag{4}$$

From this moment, and with the purpose of simplifying its notation, it is understood that the definition of the task flow $WFpi$ of any process $pi\in P$ may come given by the enumeration of a series of tasks $ti\in T$ in addition to the enumeration of a set of processes $pj\in P$. With this simplified notation, what is really expressing is that each task th belonging to the set of tasks that are part of the task flow WF_{pj} of one of the processes pj (which were part of the definition of the task flow $WFpi$ of the process pi) also belongs to the task flow WF_{pi}. Formally, given two processes $pi\ pj\in P$, $\forall pj\in WF_{pi}$ if $th\in T_{pj}\rightarrow th\in T_{pi}$. As a corollary is that: $T_{pj}\subseteq T_{pi}$.

To represent the relationships between processes is proposed by of Eriksson-Penker notation. This is an extension of UML to business processes and has a great power for the descriptive specification of processes and procedures. In this way it is achieved a formal and graphical representation.

In the business extension of Eriksson-Penker notation we can describe a process in a UML class diagram

with the symbol of processes shown in Fig. 3. In UML the process token is a stereotype of an activity of the activity diagram. The process takes resources of entry on the left-hand side and indicates the output resource by the right side (shown as units of the process according to the standards of the UML syntax). The aim of the process can be expressed as an object <<goal>> at the top of the symbol of process. The resources that are part of, or are involved with the process are displayed below the symbol of processes. The resources that are used or needed by the process are related to this through the unit <<supply>> and those that control the process make use of the dependency stereotype <<control>>. These resources can be objects, information or actors, because they include everything you need the process to run. However, due to of the importance of the actors resources for the model (will be at the spotlight in the next modeling stage), are taken into account in a set apart from the rest of the resources.

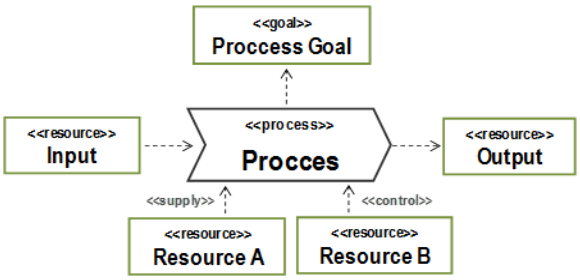

Fig. 3. Main elements employed in the conceptual modeling of the NMS.

To be more precise, each resource $r \in R$ as we formalized as a pair consisting of a label and a relationship, formally $ri=\langle E, Re\rangle$. See Table 1.

Table 1. Formalization Resources

E	Label	Specifies the name of the resource
Re	Relationship	Type of dependency that has the resource with the process. (Input| Output| Supply | Control | Achieve)

Within the type of unit includes the relationship <<*achieve*>> to identify the goals of the process.

The task flow WF_p associated with a process p, is formally described graphically within the Eriksson-Penker notation. This is an extension of the activity diagrams, we include the stereotypes and relationships characteristic of these diagrams, identifying the activities with the tasks that we defined within our model. This shows the work flow of a process through the relations between these and with the specific tasks of the thread $p1$ (See Fig. 4), which is composed of four tasks associated with these process:

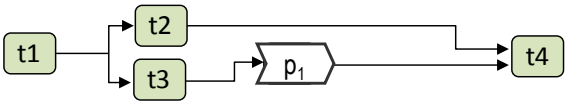

Fig. 4. Tasks flow representation.

The result of this modeling stage is the formal description of all the processes involved in the management of computer networks, synthesized in the set P, along with a first approximation of the actors (A) and involved resources (R). With this objective we start off of the concept of a computer network and applies the expert knowledge and the policies of the organization that used the NMS to obtain a model of NMS based on processes using tools such as BPM and notation Eriksson-Penker (see Fig. 5).

3. Case Study

To show both the validity and viability of the proposed model we will use a case study developed within our research group and related to the creation of intrusion detection systems. As we have previously

discussed the security of the network systems is highly complex and many times are third party tools responsible for carrying it out. That is why it is necessary to be able to design robust security systems, reliable and well designed from its inception.

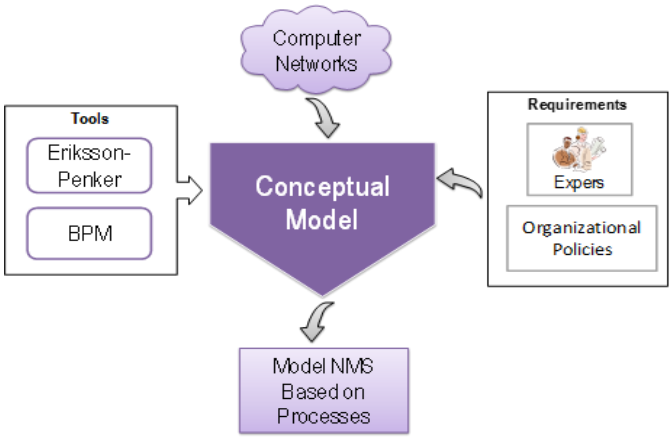

Fig. 5. Main elements involved in the conceptual modelling.

3.1. Model Description of Intrusion Detection System

Security is one of the fundamental aspects of any system that it's impossible to have completely specified over the same conception. Among other things because the quantity and type of attacks evolves, changes and depends on the activity of the system itself. That is why, in many occasions, after a basic security in the system itself, the most complete protection mounts using external applications such as antivirus, firewalls or intrusion detectors. In our case, one of the lines of research in our group is in generation of intrusion detection system or IDS in the balancing the capacity of detection compared to the performance of the systems. That is why the definition of a model for Intrusion Detection System Network is a crucial step in its development especially if it aspires to achieve proposals with broad power of generalization. It is imperative that its definition is rigorous and with the slightest ambiguity as possible, therefore, it is also important clarifications on a formal basis, following the formal framework specified in the previous chapters we'll show you a modeling of intrusion detection system or MIDS [43], and, given that the main goal is to show the viability of the framework to specify systems network management does not show the full model but if parts of the various sub models described that will uncover the expressive capacity of the formal framework. We also won't go into the discussion of the various advantages and disadvantages of the different techniques that can be used during the detection of intruders, since that is a problems that escapes from this work. In our case we have selected as a strategy for the detection of intruders the reduction features using PCA algorithm and the use of SOM for intrusion detection [44] that had already been treated in previous works.

3.2. Conceptual Model

In general terms the overall system IDS analyzes a network traffic and executes tasks on the network to maintain the control over the actions of the hackers. Given that we are looking for not sacrificing detection capability or efficiency of classification over performance, our MIDS will consist of several main processes like an engine of reduction that allows them to resize the network traffic data to analyze and thereby achieve a good performance, a detection engine that analyzes the reduced traffic and betray the presence of intruders and a motor response to generate the relevant actions to control the intruders. We can therefore establish as a first approximation of the IDS conceptual model shown in Fig. 6.

The reduction Engine (PRE) is the first process that is carried out within the MIDS. Their goal is to find a

data model that will reduce the size of the original traffic, apply it and keep it updated to the changes in the environment. The Detection Engine Process (PDE) detects intrusions that may contain the reduced traffic produced by the above process, conducting the most characteristic feature of the model, the classification of network packets. Finally the detection reports are analyzed by the Response Engine (PReE) to act on the network in case necessary through the actions of response.

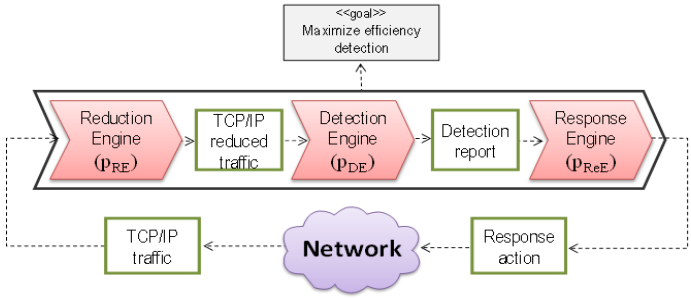

Fig. 6. General model IDS.

We can examine on the threads of each main process. In our case, after analyze various alternatives, we have chosen as algorithm of reduction of the Principal Components Analysis (PCA) for its training without oversight, guarantee of minimum loss and its rationale in characteristics of linearity. In Fig. 8 we can see the defined workflow for the Reduction Engine process. It is composed of a first data capturer process (Ps) from TCP/IP packets. This process is coordinated by an actor Sensor (αSensor). Later a reductive process (PR) is responsible for the implementation of the PCA filter and gets the reduced TCP/IP traffic. As before, a reducing agent (αReducer) is responsible for supervise the process. The PCA filter uses a training process (PPCAT) allows you to be constantly updated with zero maintenance. In this training process involves a packages manager process that will produce a set of training packages that will be used by the PCA process to obtain a PCA Model to serve as a reducer. The agent responsible for the training will be the agent Coach PCA (αPCATrainer).

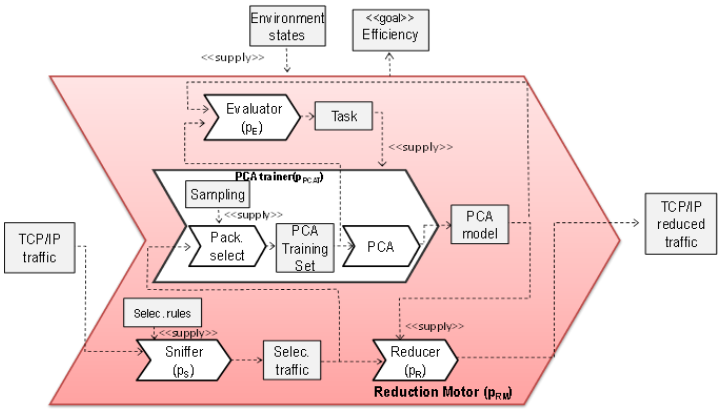

Fig. 7. Workflow engine of reduction (WFMP).

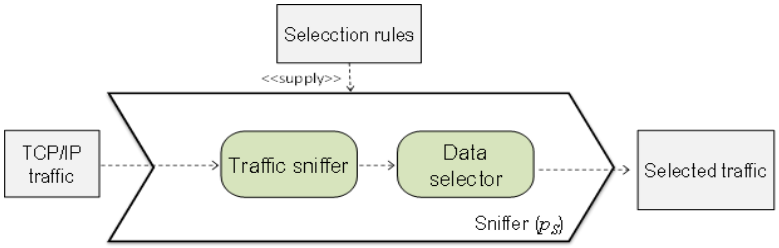

Fig. 8. Capturer process (WFC).

Continued to deepen each thread we can complete the description of PRE. For example, the fetcher process picks up TCP/IP packets from the network and take of them important data for the classification and thus obtaining a selected traffic. The capturer process filtered the characteristics described in the Selection Rules being the actors responsible for these tasks are αCapturer and αDataSelector respectively. In Fig. 8 we can see the concrete specification of the capturer process.

This is the method of successive refinement would we describe each thread that form the Reduction Engine, the detection engine and finely the Response Engine. In this conceptual model of the IDS would get all the processes involved, a first approximation of the responsible agents, resources and task flows, thus having a formal model that specify the conceptual operation of the system. As a matter of space didn't go into details but as detection engine was selected a SOM (Self-Organizing Map) by being an architecture of unsupervised training, easy implementation and deployment, which has demonstrated a high order of accuracy and generalization in the various investigations in which has been used [44].

4. Conclusions

In this work has been presented a conceptual model as a basis for the systematic design of complex systems of management of networks. This model provides a structured and rigorous methodology that facilitates the retrieval of modelled systems with standard tools and following a procedure which ensures formal basis. Likewise, the model allows to design this type of systems by modeling of the processes involved, considering a formal definition of the overall development objectives. Finally, the model offers specific methods which enable us to move forward in the development of the foundations of the application and convert a set of processes in a formal set viable with the existing technologies in each moment.

The proposed conceptual model for the start of the development of any system allows you to deal with the MNMS taking as reference the processes involved that generally develop systems administrators and carried out the analysis of the same thing using the UML extension Eriksson-Penker for notation of processes.

To illustrate the use of the formal framework proposed in this investigation, we present a case study: the conceptual modeling of an IDS. It has been found that the methodology allows you to define the system completely prior to deployment, incorporated into the model the desired properties such as flexibility, scalability, or modularity. The resulting model defines all the functional aspects of the IDS system used as a case study.

Acknowledgment

This work was performed as part of the Smart University Project financed by the University of Alicante.

References

[1] Google (November 2013). *Google Official History, Comscore*. Retrieved November 23, 2013, from: http://www.statisticbrain.com/google-searches

[2] ITU-T. (2013). *ITU Statistics — Global ICT Developments*.

[3] National Institute of Statistics. (October 2013). Retrieved October 25, 2013, from: http://www.ine.es

[4] Macia, F., Marcos, D., & Gilart, V. (2009). energy management system as an embedded service: Saving energy consumption of ICT. *Proceedings of 22nd International Conference ACS-LES ARCS 2009: Vol. 5455*.

[5] Macia, F., Marcos, D., Gilart, V., Mora, F. J., & Berne, J. V. (2009). Phoenix computing: IT Semantic management models (TIN2006-04081). *Proceedings of jspTIN2009*. Boadilla del Monte, Madrid.

[6] Wang, C., & Liang, Z. (2014). Android-based vehicular distributed intelligent video collection system.

Journal of Networks, 9, 2615-2621.

[7] Shan, H., Jiang, G., & Yoshihira, K. (2010). Extracting overlay invariants of distributed systems for autonomic system management. *Proceedings of the 4th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO2010)* (pp. 41–50). Budapest, Hungary.

[8] Jiang, G., Chen, H., & Yoshihira, K. (2006). Discovering likely invariants of distributed transaction systems for autonomic system management. *Clustering Computing, 9*, 385-399.

[9] Ge, Y., Jiang, G., & Ge, Y. (2013). Efficient invariant search for distributed information systems. *Proceedings of ICDM'13* (pp. 1049–1054). Dallas, Texas, USA.

[10] ISO/IEC JTC1/SC21/WG4 N571. (1998). Information processing systems — open systems interconnection, systems management: Overview.

[11] ITU-T, M. 3050. (2004). Enhanced telecom operations map (eTOM — the business process framework).

[12] ITU-T, M. 3010. (1996). Principles for a telecommunications management network.

[13] ITU-T, M. 3400. (1997). TMN management functions.

[14] ITU-T X. 700. (1992). Information technology — open systems interconnection. *Systems Management: Security Audit Trail Function*.

[15] ITU M3000. (2001). TMN and network maintenance: International transmission systems, telephone circuits, telegraphy, facsimile and leased circuits.

[16] RFC 3410, 2002. Retrieved August 12, 2013, from: http://www.ietf.org/rfc/rfc3410.txt

[17] Maciá, F., Mora, F. J., D., Gil, J. A., Ramos, H., & Lorenzo, I. (2011) Network intrusion detection system embedded on a smart sensor. *IEEE Transactions on Industrial Electronics*, *58*, 722-732.

[18] CERT Statistics. (October2012). Retrieved August 19, 2013, from: http://www.cert.org/stats/cert_stats.html#vulnerabilities

[19] Ghosh, A., & Schwartzbard. (1999). A Study in using neural networks for anomaly and misuse detection. *Proceedings of the 8th USENIX Security Symposium: Vol. 8* (pp. 12-12). Berkeley.

[20] Lippmann, R., & Lunningham, R. (2000). Improving intrusion detection performance using keyword selection and neural networks. *Computer Networks*, *34*, 597-603.

[21] Krugel, C., Kirda, E., Mutz, D., Robertson, W., & Vigna, G. (2005). Polymorphic worm detection using structural information of executables. *Proceedings of the 8th International Symposium on Recent Advances in Intrusion Detection (RAID)* (pp. 207-226). Seattle, USA.

[22] Liang, Z., & Sekar, R. (2005). Automatic generation of buffer overflow attack signatures: An approach based on program behaviour models. *Proceedings of the 21st ACSAC* (pp. 215-224). Tucson, AZ, USA.

[23] Debar, H., & Viinikka, J. (2005). Introduction to intrusion detection and security information management. *Foundations of Security Analysis and Design III*, 207-236.

[24] Polychronakis, M., Anagnostakis, K., & Markatos, E. (2007) Emulation-based detection of non-self-contained polymorphic shellcode. *Proceedings of RAID 2007*: *Vol. 4637* (pp. 87-106).

[25] Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: A review. *International Journal of Distributed Sensor Networks*, 7.

[26] Kruegel, C., Valeur, F., & Vigna, G. (2005). *Intrusion Detection and correlation. Challenges and Solutions*, Springer.

[27] Anderson, R. J. (2008). Network attack and defense. *Security Engineering: A Guide to Building Dependable Distributed Systems*, *1,* 633-678.

[28] Macia-Perez, F., Berna-Martinez, J. V., Marcos-Jorquera, D., Lorenzo-Fonseca, I., & Ferrandiz-Colmeiro, A. (2012). A new paradigm: Cloud agile manufacturing. *International Journal of Advanced Science and Technology*, *45,* 47-54.

[29] Jung, Y., & Chung, M. (2010). Adaptive security management mode in the cloud computing environment. *Proceedings of the 12th ICACT* (pp. 1664-1669). South Korea.
[30] Roscia, M., Longo, M., & Lazaroiu, G. C. (2013). Smart city by multi-agent systems. *Proceedings of International Conference on Renewable Energy Research and Applications* (pp. 371-376). Madrid, Spain.
[31] Jamil, D., & Zaki, H. (2011). Cloud computing security. *International Journal of Engineering Science and Technology, 3(4),* 2672-2676.
[32] Booch, G., Rumbaugh, J., & Jacobson, I. (1998). *The Unified Modeling Language User Guide*. Addison Wesley.
[33] Booch, G., & Rumbaugh, J. (2001). *The Unified Modeling Language.* Adisson-Wesley.
[34] Rumbaugh, J., Jacobson, I., & Booch, G. (2004) *The Unified Modeling Language. Reference Manual.* (2nd ed.). Addison-Wesley.
[35] White, S. A. (2009). Business process modeling notation v1.0. *For the Business Process Management Initiative (BPMI)*.
[36] Recker, J. C., Rosemann, M., Indulska, M., & Green, P. (2009). Business process modeling: A comparative analysis. *Journal of the Association for Information Systems*, *10,* 333-363.
[37] Beltrán, J., Carmona, M., Carrasco, R., Rivas, M., & Weaver, F. (2003). Guide to a process-based management. *Andalucia: Corporación Cooperativa*.
[38] ISO/TC 176/SC 2/N544R. (2009). Guidance on the process approach to quality management. Retrieved October 2, 2009, from: www.iso.ch/ISO/en/iso9000/200rev9.html
[39] Smith, H., & Fingar, P. (2002). *Business Process Management. The Third Wave.* Meghan-Kiffer.
[40] Rosen, M. (2004). *SOA, BPM and MDA*, *Surah Technologies*.
[41] Jeston, J., *et al.* (2006). Business process management. *Practical Guide to Successful Implementations*. Elsevier.
[42] Lohrmann, M., & Reichert, M. (2012). Modeling business objectives for business process management. *Lecture Notes in Business Information Processing*, *104*, 106-126.
[43] Lorenzo, I. (2010). Model-based intrusion detection techniques for reducing features. Solution to the dilemma capacity-efficiency. Ph.D. Thesis, Dept. Computer Technology, University of Alicante.
[44] Macia, F., Mora, F. J. D., Gil, J. A., Ramos, H., & Lorenzo, I. (2011). Network intrusion detection system embedded on a smart sensor. *IEEE Transactions on Industrial Electronics*, *58,* 722-732.

Francisco Maciá-Pérez was born in Spain in 1968. He received his engineering degree and Ph.D. degree in computer science from the University of Alicante in 1994 and 2001 respectively. He worked as a system's administrator at the University of Alicante form 1996 to 2001. He was an associate professor from 1997 to 2001. Since 2001, he is a professor and currently he is the vice president for information technologies at the University of Alicante. His research interests are in the area of network management, computer networks, smart sensor networks and distributed systems, which are applied to industrial problems.

Iren Lorenzo-Fonseca was born in Cuba in 1982. She received the engineering and master's degrees in computer science from the José Antonio Echeverría Institute of Technology (CUJAE), Havana, Cuba, in 2005 and 2007, respectively, and the Ph.D. degree from the Department of Computer Science and Technology, University of Alicante, Alicante, Spain, in 2010. She is currently a professor with the Computer Science Faculty, CUJAE. Her research interests lay in the area of IA, computer networks, and distributed systems.

Jose Vicente Berna-Martinez was born in Spain in 1978. He received his engineering degree and Ph.D. degree in computer science from the University of Alicante in 2004 and 2011 respectively. From 2006 to 2013, he was an associate professor at the University of Alicante, currently he is an assistant doctor. His research interests are in the area of computer networks, distributed systems, bio-inspired systems and robotics that are applied to industrial problems.

Jose Manuel Sanchez-Bernabeu was born in Alicante, Spain in 1982. He received the bachelor's degree in computer science from University of Alicante in 2010 and the master degree in computer technologies in 2014. Now he is a PhD student in information technologies. And he is a member of Middleware Group in the Department of Computer Technology in University of Alicante. He's working with M2M communications, smart cities and internet of the things.