Distributed Network Security Management Using Intelligent Agents

K. Boudaoud
Corporate Communication Department
EURECOM Institute
Sophia-Antipolis, France
Email : boudaoud@eurecom.fr

N. Agoulmine
PRISM Laboratory
University of Versailles-Saint Quentin en Yvelines
Versailles, France
Email : naz@prism.uvsq.fr

J.N De Souza
Department of Computer Science
Federal University of Ceará, Fortaleza, Brazil
E-mail: neuman@ufc.br

Abstract: The openness of business toward telecommunication network in general and Internet in particular is performed at the prize of high security risks. Every professional knows that the only way to secure completely a private network is to make it unreachable. However, even if this solution was undertaken for many years, nowadays it is not possible to close private network especially for business purpose. Existing security solutions are in general very complex and costly. Thus there is a need to think about new type of security mechanism based on recent technologies. One such technology, which is gaining ground, is Intelligent Agent Technology. Thus, the purpose of this paper is the investigation of novel architectures and mechanisms based on IA Technology in order to purpose efficient, flexible, adaptable and cost effective solutions.

Keywords : Distributed Computing, Security Management, Distributed Intrusion Detection, Intelligent Agent Technology.

1- Introduction

The ongoing Explosion in use of Internet combined with the deregularisation of telecommunication is an indication of the scale of the revolution that is happening. However, this explosion is introducing a huge problem of security for both the networks and services. The needs of remote access from customers, users and service provider to a particular environment requires that the precautions must taken in order to make a balance between the security demands and the access flexibility.

The existing security solutions are very complex and costly. What is rapidly needed is a flexible, adaptable and affordable security solution, which provides greater autonomy. Therefore, it is necessary to review the way security system architectures are designed in investigate new technologies that could help make easier and cost-effectiveness new solution

In this context, we are investigating the concept of Intelligent Agent (IA) a candidate paradigm to develop needed solutions. Agent technology has already been used in many different application areas, supporting different functionality. However, it is the emergence of distributed systems and the Internet technologies that has made the realisation of Intelligent Agent technically possible. IA represents transportable and even active objects. With this, IAs can realise global tasks, which are carried out autonomously and co-operatively.

The introduction of intelligent agent concept in a network seems so promising to embed adaptive features thereby enabling network entities to perform adaptive behavior and becoming “intelligent”. The term intelligence is used in the sense that network entities provide reasoning capabilities, exhibit behavior autonomy, adaptability, interaction, communication and co-operation in order to reach some goals.

This paper investigates some scenario for the use of IA technology in the context of security management. It is organized as follows. Section 2 provides a short description on Network Security Management. The agent concept is outlined in section 3 and the DIANA agent architecture is briefly presented in section 4. In section 5, the proposed MA-based Security Management Architecture is described. Finally, Section 6 provides concluding remarks.

1. Network Security Management

Security management is a task of maintaining the integrity, confidentiality and availability of systems and services. The reality of the present time is that increasing number of people, organizations, and enterprise are installing and subscribing to the Internet, consequently raising the concerns of security. Thus, the security management is an issue of paramount importance.

First of all, it is necessary to identify the risks by identifying the attacks and intrusions that the networks are exposed to. Applying security management is a two-fold activity. Firstly, the security architecture is to be deployed to protect networks against the attacks by detecting attacks. Secondly, when attacks are detected the security architecture is to respond to attacks and to take security measures, preferably in real time.

An intrusion or attack [2] can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion detection is a practical approach for enhancing the security of computer and network systems. The goal of IDS is to detect attacks especially in real-time fashion. There are systems based on host-audit-trail and/or network traffic analysis to detect suspicious activity. These systems use one or both of two approaches of intrusion detection. The first approach is the behavior-based intrusion detection, which discovers intrusive activity by comparing the user or system behavior with a normal behavior profile. The second approach is a knowledge-based intrusion detection approach, which detects intrusions upon a comparison between parameters of the user’s session and known pattern attacks stored in a database. The behavior-based intrusion detection approach allows detecting unknown intrusions contrarily to the knowledge-based intrusion detection approach, which detects well-known intrusions. We focus our work on network intrusion detection systems and we present below two specific systems **DIDS** (Distributed Intrusion Detection System) and **CSM** (Co-operating Security Managers).

DIDS operates on a local area network (LAN) and its architecture combines distributed monitoring and data reduction with centralized data analysis [3]. A DIDS director, a LAN monitor, and a series of host monitor constitute it. The LAN monitor reports to the DIDS director unauthorized or suspicious activities on the network. The host monitors collect audit data for the individual host and perform some simple analysis on the data. The relevant information is then transmitted to the DIDS director. This director is responsible for analyzing all these data and detecting possible attacks. A shortcoming of DIDS is that the centralized nature of DIDS will limit its usefulness in wide area networks where communication with a central director from all hosts may swamp portions of the network.

CSM was designed to perform intrusion detection in a distributed environment [4]. A CSM must be run on each computer connected to a network to facilitate the co-operative detection of network intrusions. It consists of following parts:

- a local intrusion detection component. It performs intrusion detection for the local host and is responsible for proactive detection of attacks on other host ;
- a security manager which co-ordinates the distributed intrusion detection between CSMs ;
- an intruder handling component. Its role is to take actions when an intruder is detected ;
- a graphical user interface ;
- a command monitor which intercepts the commands executed by a user and sends for analysis ;
- a TCP communication module.

CSM takes an approach that uses no established centralized director but each of the individual managers assumes this role for its own users when that manager suspects suspicious activity. The most important feature of CSM is that the co-operation among CSMs permits them to handle certain type attacks in a proactive manner (e.g. doorknob rattling attack). In a heterogeneous environment, two CSMs can communicate because communication takes place via messages that relay information that need not be system-specific. However CSM cannot simply be ported from one computer system to another because the action-based intrusion detection module is heavily system-specific.

Looking at these approaches undertaken to counter security attacks, some features of these approaches can be derived as main requirements:

Distribution of activities: this aspect is found mainly in all the approaches. It is very important to distribute the control of security management among a number of entities that can monitor the network and system behaviors at different points.

Autonomy: the CSM and DIDS approaches have shown the necessity to have a certain level of autonomy in the various entities that constitute the system. They differ in the sense that the final decision in the DIDS system is taken by a centralized manager, whereas in the CSM some decisions can be directly taken in the entity.

Co-operation: the CSM has shown also the necessity of security manager co-operation in order to detect security attacks that can not be detected by individual manager.

2. Intelligent Agent Concept

Intelligent agent technology is a growing area of research and new application development in telecommunications. Having highlighted the main requirements for security management, the intelligent agent concept seems to be a candidate approach to fulfill these requirements. What is the Intelligent Agent concept [5][6][7][8][9]? Until now, there is no an internationally accepted definition of an intelligent agent concept [10]. The term Agent is a concept used in different area and having different meaning depending on the context [11]. Nevertheless, different types of agents reflect a set of properties, which common among them and are described below [12]:

- **Autonomy**: is the ability of an agent to operate without direct intervention of humans or other agents and to have some kind of control based on its internal and/or external environments
- **Co-operation**: an Agent is co-operative and is able to have a social ability. This sociability allows an agent to interact with other agents for the purpose of performing tasks that are beyond the capability of a particular agent. This capability goes from delegation (distribution of sub-tasks) to peer-to-peer inter-working.
- **Proactiveness:** it is the agent's ability to anticipate situations and change its course of action to avoid them. Proactive agents are capable of exhibiting goal-direct behaviors by taking some initiative [13][14].
- **Reactivity**: this kind of behavior means that the agent reacts in real-time to changes that occur in its environments.
- **Adaptability**: is the ability of an agent to modify its behavior over time to fulfill its problem-solving goal.
- **Intelligence**: the term "Intelligence" means that the agent is able to exhibit a certain level of intelligence priority, ranging from predefined actions (planning) up to self learning (define new actions).
- **Flexibility**: is the ability an agent should have to adapt itself to cope with the environment in which it is situated.
- **Mobility**: an Agent is mobile. It is capable of moving from one localisation to another in order to perform a particular task or to react to a particular event

Having studied the properties of the IA and the aspects and requirements of a security management, it can be concluded that IA provides a more coherent and flexible approach of security management. The security management architecture based on the concept of IA can be conceived as if it were made of the autonomous IAs co-operating with each other to achieve Global Security Policy. The section 5 describes the security management architecture.

3. DIANA Agent Architecture

In this section, we present the DIANA[1] agent architecture [15]. The DIANA Architecture is the shell of our system. The key characteristics of these agents are their ability to acquire new capabilities and skills, without interrupting their operations, permit network management applications to be easily adaptable when changes occur. The DIANA agent architecture consists of two main component types: the Brain, which is responsible for managing agent skills and the skills, which provide the agent with capabilities and behaviors.

3.1 The Agent's Brain

The Brain (Figure 1) offers two types of necessary facilities for the agent operation: *local* and *inter-agent facilities*.

[1] The development of this architecture was supported by Swisscom and by the Institut Eurécom.

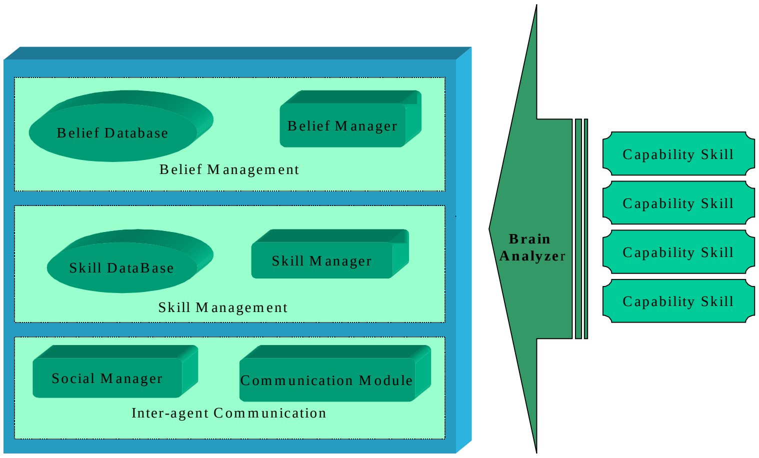


Figure 1: DIANA agent architecture

The main role of the Brain is to manage both agent's *Belief Database* and agent's *Skill Base*. "An agent *belief* expresses its expectations about the current state of the world and about the likelihood of a course of action achieving certain effects"[8]. Beliefs hold network management information as well as information about the agent itself and the other agents. These beliefs can be accessed concurrently by several skills, therefore, the *Belief Manager* maintains the integrity and the coherent access to the Be*lief Database.*

Skills can be downloaded dynamically into the agent inside its *Skill Base*. The main role of the *Skill Manager* is to check the availability of pre-requisite skills required by newly loaded skills and if they are not yet loaded, it must search for them either locally or on distant agents. It is also responsible for disposing off no useful skills to keep the agent's size as small as possible. During its operation, the skill can update or delete existing beliefs or create new ones. A skill operation may depend on beliefs created by other skills, and the *Skill Manager* is therefore in charge of dispatching asynchronously these beliefs to the interested skill in a transparent way. It holds all the necessary information about the skills in the *Skill Base*.

The ***Brain Analyzer*** is responsible for the parsing of the messages that the Brain receives, either from the skills or from the inter-agent communication

Both the ***Communication Module***, which is responsible for managing interactions with the other agents and the *Social Manager*, which holds information about the other agents, support inter-agent communication facilities in the agent.

3.2 Capability Skills

A capability skill, which is a piece of software specialized in a network management area, uses information and services offered by lower-level skills and offers in its turn new services to higher-level skills. The skill inform the Brain about the pre-requisite skills needed for its operation and the services offered to other skills. Therefore, the role of the Brain is first to manage the availability of pre-requisite skills. Then to decide which skill is concerned by a service request to forward it to that skill to be performed. And finally to notify the skill of an information or a requested service.

5. Proposed Multi Agent Security Management Architecture

In our proposed approach, we define a new architecture, called MA-SM (Multi Agent Security Management). It is viewed as a collection of autonomous and intelligent agents located in specific network entities. These agents co-operate and communicate in order to perform intrusion detection tasks efficiently and achieve consequently better performance.

5.1. Physical Architecture

The key characteristics of the security architecture are flexibility, adaptability, and distribution of security mechanisms. The MA-based Security Management Architecture consists of four main components as described in the following figure:

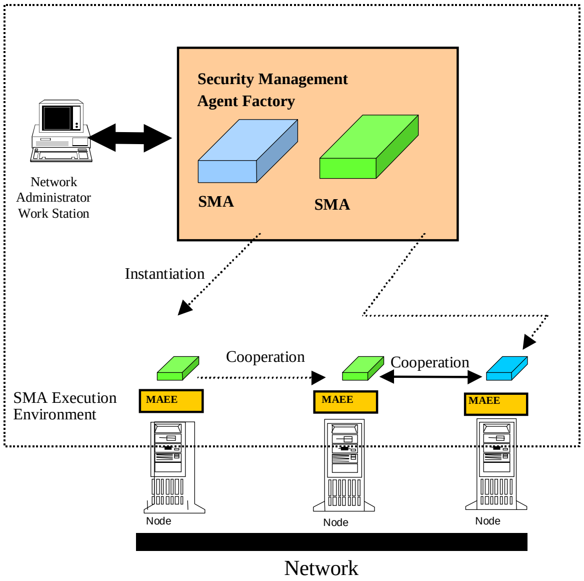


Figure 2: Intelligent Agent Security Management Architecture

- The **Management Agent Factory** (**MAF**) is an environment, in which security management intelligent agents are created, initiated, resumed, and controlled. The environment also serves as an access point for network security administrator.

- The **Security Management Agent** (**SMA**) is an intelligent agent that collects, filters management information and performs security management activities. The management activities are defined by the administrator and reflect the Security Policy. Thus, network

environment is populated by a set of SMA that co-operate with each other in order to perform global security management activities (described in the following Figure).
We have identified two SMA types: *Master SMA (MSMA)* and *Slave SMA (SSMA).* The SSMA is responsible for managing the security of his domain constituted of several hosts. There are several SSMA that performs some analysis before informing the MSMA when they suspect an attack. The MSMA is responsible for coordinating SSMA tasks and correlating information received from SSMA. The MSMA, in his turn makes his own analysis to confirm or detect an occurred attack and take appropriate actions (like informing the security officer (S.O)). The SSMA can communicate and co-operate before sending their reports to the MSMA. We identified a specific agent named *External Agent*, which its role is to manage all activities going in or out the monitored network.

- The **Management Agent Execution Environment** (**MAEE**) is a set of components necessary for the execution and the migration of IAs.

- The **Network Administrator Workstation** (**NAWS**) is an interface with which a security administrator (a person) interacts with the architecture. A security administrator must specify the security policy to apply and to create, instantiated, control the Intelligent Agents. For these operations, the security administrator needs to access the **MAF**, and NAWS facilitate security administrator with an access to **MAF**.

5.2 Security Policies:

The architecture relies on many IAs for assuring intrusion detection. The IAs operate autonomously but according to a predefined security policy. These policies can be defined at the initialisation of the IA or dynamically according to the global business policy.

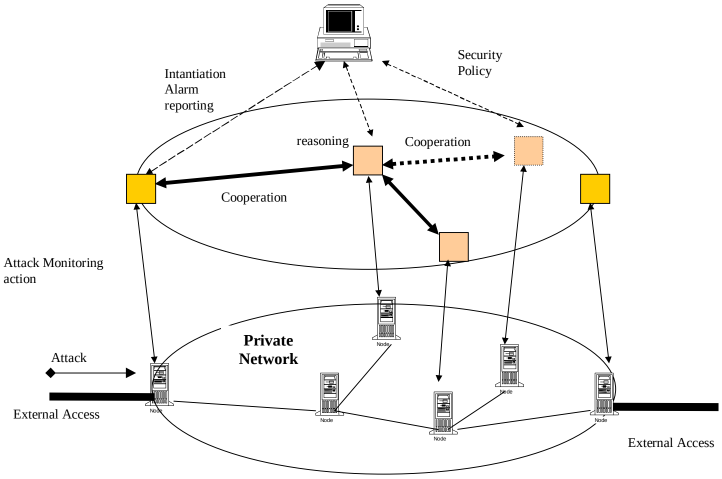


Figure 3: Security Intelligent Agent Monitoring of Telecommunication Services

The first step to specify this security policy is to use access control rules. The access control rules provide a flexible means of specifying management policy as a relationship between initiator domain and target domain in terms of the operations client can perform on remote hosts. Constraints (contextual information) also make up a part of the access control rules and specified in the rules. Access control procedures (i.e. validation of Initiator-bound Access Control Information (ACI), identification of the Target etc.) are performed according to the established Security Policy, which is specified by access control rules.

The access control rules is the part of the ACI, which represents the permitted operations and the conditions upon their execution in a security domain. There are five classes of access control rules that are to be applied:

Globally deny rules: These deny access to all targets. If a global rule denies access, then no other rule shall apply. If a global rule does not deny access, then the item deny rules are imposed.
Item deny rules: These deny access to particular targets. If an item deny rule denies access, then no other rule shall apply. If an item deny rule does not deny access, then the global grant rules are applied.
Global grant rules: These grant access to all targets. If a global rule grants access, then no other rule shall apply. If a global rule does not grant access, then the item grant rules are imposed.
Item grant rules: These grant access to particular targets. If an item grant rule grants access, then no other rule shall apply. If an item grant rule does not grant access, then the default rules are applied.
Default rules: These rules are to be applied when no other rule has specifically granted or denied access. The default rules shall grant or deny access.

The IAs should monitor the network in order to detect security-relevant events and then react according to the behaviour specified by the administrator. The IAs may also report the administrator Workstation the security-relevant events. In case of a special event, the IAs may also co-operate to check or have some information in order to have a more precise status on the special event. For example, if an agent detects an “unauthorizedAccessAttempt”, it can co-operate with others agents to check if there are other login attempts on their hosts. An example of this functionality is given below.
Suppose that an intruder came from an external network, in the night or in the weekend, obtained an access, and had an unauthorised activity. The agent that is monitoring all the incoming connections detects an “unknownAddress” and an “outOfHoursActivity” event. This agent can track the intruder by migrating to the host were the intruder is working. If the intruder “travel” from one host to another host, migrating agent can follows intruder’s activities by co-operating with the others agents, responsible for monitoring these hosts. If one of the co-operating agents detects, for instance an “unauthorizedAccessAttempt”, or an “suspiciousActivitiy”, the first agent can migrate to the host on the entry of the internal network and close the connection or to ask another agent to do it.

5.3 Required Skills

In order to support the previous functionalities of SMA and according to the DIANA agent architecture, a number of skills have been identified for the purpose of security management. These skills are:

- **User Interface Skill**: this skill permit the security officer to transmit to the agents, particularly to the MA, some requests, like a new security policy or a new intrusion to detect or a new security event to monitor, ...It sends the security officer requests to the *Security Manager Skill.*

- **Security Manager Skill**: it is responsible for managing the security of the agent domain. When an intrusion is detected, it takes appropriate actions like for example interrupting a connection and/or informing the Security officer. In the case of the master agent, it is responsible for delegating detection tasks to the different SA.

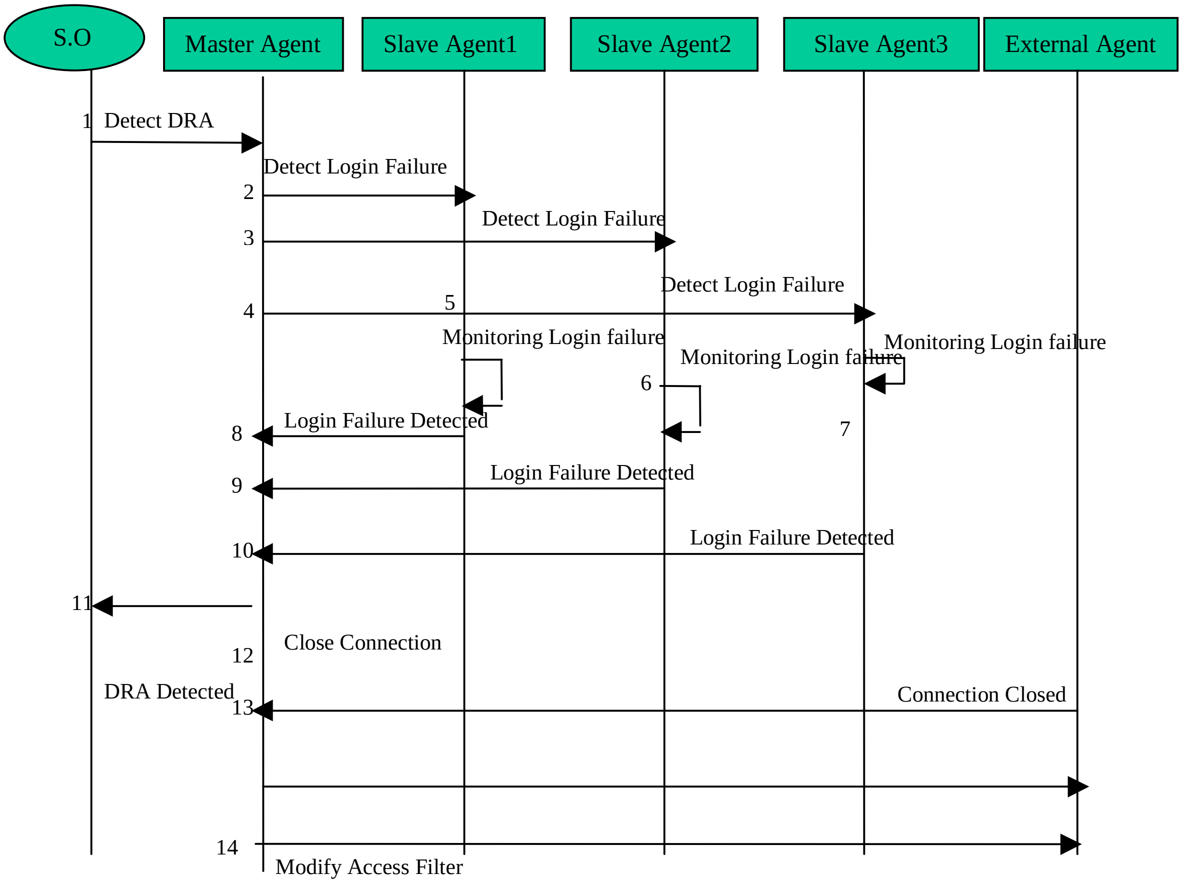
- **Intrusion Detection Skill**: it is responsible for performing intrusion detection for the agent domain. In the case of the master agent, it is also responsible for coordinating the information collected by the different SA. When an intrusion occur, it sends an alarm to *the Security Manager Skill.*

- **Instrumentation Skill**: it is responsible for instrumenting the necessary beliefs about the security events monitored by the *Syslog Skill.* These beliefs are then used by *the Intrusion Detection Skill.*

- **Syslog Skill**: its role is to report security events to the *Instrumentation Skill.* For example it reports all the “login failure” events. It collects its information from the log files and it is system-dependant.

5.4 Example of Agents Interactions Diagram

In this diagram, we show the interactions between the different agents in order to detect the network attack called *Doorknob Rattling*. In this attack, the intruder attempts to log in to several hosts with any user-id/password combination in order to obtain an access to an account.



This diagram presents the various interactions between the agent in order to detect in a distributed manner the Login Failure Attack. The different messages exchanged between the agent permit to have a global view of what is happening in the network. This is the only way that permits to detect attacks in different points of the network. The agents should keep a history of the alarm message so that to correlate them together to identify any attack pattern.

6 Conclusion

This paper has first introduced security management problems in the context of deregulated telecommunication and generalization of Internet access. The generalization of network access renders corporate information infrastructure very fragile. In this work, the objective is to investigate the use of agent technology to propose new types of solutions. The idea is to propose flexible and efficient solutions for a problem that is difficult to handle with conventional approaches. The proposed architecture is based on various agents disseminated across the network and host. The global security management activity is distributed among the various agents. Each agent has a particular skill that permit to exhibit a particular behavior. The combination of skills and cooperation activities between agent is the key idea of this approach. By cooperating between each other, agents are able to detect security attacks that will not be possible by a centralized approach.

This work is only at its beginning; in the following we are in the process of enhancing the various skills that could be integrated in each agent and experimenting the approach in a real context.

7 References

[1] L. Glasser, « An overview of DAI », Kluwer Academic Publisher 1996.

[2] R.Heady, G.Luger, A.Maccabe, M.Servilla. « The architecture of a network level intrusion detection system », Technical Report, University of New Mexico, Department of Computer Sciance, August 1990.

[3] L.T. Heberlein, B.Mukherjee, and K.N.Levitt, « Network Intrusion Detection », IEEE Network journal, May/June 1994, pp. 26-41.

[4] Maj.Gregory B. White, Eric A. Fisch, and Udo W. Pooch, « Cooperating Security Managers: A Peer-Based Intrusion Detection System », IEEE Network journal, January/February 1996, pp. 20-23.

[5] Y.Yemini and al, «Network Management by Delegation», in Integrated Network Management II, Krishnan & Zimmer (Eds), pp 95-107, Elsevier Science Publishers, 1991.

[6] C.G. Harrison, D.M. Chess and A.Kershenbaum, «Mobile Agents: Are they a good idea? », IBM T.J.Watson Research Center, March 1995.

[7] T.Magedanz, K.Rothermel and S.Krause, «Intelligent Agents: an Emerging Technology for Next Generation Telecommunications? ». In Proceedings of the IEEE INFOCOM ’96, San Francisco, USA, March 1996, pp464-472.

[8] J.P.Muller, « The Design of Intelligent Agents – A Layered Approach» LNAI state-of-the-art Survey, Springer, Berlin, Germany, 196.

[9] OMG (Object Management Group) Working Group, «Mobile Agent Facility Specification ». Technical report, Crystaliz, Inc., General Magic, Inc., GMD Fokus, International Business Machine Corporation, Nov 1997, OMG TC Document arbos/97-10-05.

[10] H. S. Nwana and M. Wooldridge, «Software Agent Technologies». BT Technology Journal, 14(4): 68-78, October 1996.

[11] S.Corley and al, «The Application of Intelligent Agent Technologies to Network and Service Management», 5th IS&N Conference, Antwerpen, Belgium, 25-28 May 1998.

[12] R.Oliveira, «Network Management with Knowledge of Requirements: Use of Software Agents». Phd Thesis, 1998.

[13] M. Wooldridge and N. R. Jennings, « Intelligent Agents: Theory and Practice ». Knowledge Engineering Review, 10(2):115-152, 1995.

[14] H. Labiod,« Error Control in Wireless ATM networks », Thesis 1998.

[15] M. Cheikhrouhou, P.Conti, J.Labetoulle, K. Marcus, « Intelligent Agents for Network Management: Fault Detection Experiment », Proceedings of the sixth IFIP/IEEE International Symposium on Integrated Network Management (IM'99) (to appear), Boston, May 1999