Journal of Engineering and Technology Research Vol.2(10), pp. 200-206, October 2010
Available online at http:// www.academicjournals.org/JETR
©2010 Academic Journals

Full Length Research Paper

New distributed platform for intrusion detection based on multi-agents system

Driss Raoui*, Siham Benhadou and Hicham Medromi

High National School of Electricity and Méchanics (ENSEM), Hassan II University, Aïn Chock, P. O. Box 8118, Oasis-Casablanca, Morocco.

Accepted 16 August, 2010

The development and evolution of computer networks, in terms of number of users and services, are making them ever more complex and therefore vulnerable to new types of attacks. Given this complexity of attacks, intrusion detection systems, to monitor the activities of a network or a sensitive computer and to detect abnormal usage of computer resources, are expected to evolve and adapt to changes in user behavior. To improve and strengthen the mechanism of intrusion detection, we propose in this paper a new real-time distributed architecture, based on the multi-agent aspect consisting of two levels of analysis benefiting from reactive and cognitive capabilities of agents and using rules and safety procedures to detect complex attacks and intrusions that can represent low threats.

Key words: Security, intrusion detection, multi-agent system, analyzer, AUML.

INTRODUCTION

With the development of Internet, computer systems are becoming more open and collaborative enabling, facilitating communication and exchange of information by improving the transmission speed and technology of interconnection. Consequently, computer networks have become increasingly complex and therefore the number of vulnerabilities found on computer systems may be important. Thus, attacks against these vulnerabilities can be both varied and complex (Solange, 2004). To ensure optimum operation of the network and systems, it is necessary to identify potential threats. Technology can be implemented to ensure system security information in many ways. Among these methods, we found the intrusion detection system is used to monitor the activity of a network or system to detect real time abnormal use of computing resources, log these events, and analyze this information in search of violation or abuse, warning generating alerts and sometimes reacting against intrusion (Zalewski, 2008).

Currently, intrusion detection systems lack methods and mechanisms to detect complex attack scenarios. They are exposed to many challenges as the network evolves and new attacks emerge. Existing intrusion detection systems are not adapted to the increasing complexity of attacks and changing network dynamics and user behavior.

STATE OF ART

Intrusion detection system

An intrusion detection system (Intrusion Detection System) is designed to automate the detection of a violation or attempted violation of security policy implementation within an information system. It is composed of separate elements providing the real time or delayed analysis of security events, aggregation and correlation of these events and the implementation of processes which alerts the appropriate response (Northcutt et al., 2001). The integration of an intrusion detection system in a security platform therefore allows the collection of accurate and practical information on the status of threats to

*Corresponding author. E-mail: raoui.driss@gmail.com.

information systems. There are two distinct major families of IDSs:

The N-IDS (Network Based Intrusion Detection System): it provides security at the network level.
The H-IDS (Host Based Intrusion Detection System): it ensures the security level for hosts.

The network-based intrusion detection system (NIDS) requires dedicated hardware and is a system capable of controlling packets on one or more network links in order to discover if a malicious or abnormal act occurs. This type of IDS has the advantage more that a single sensor, this is because if it is properly placed, can detect attacks that target multiple hosts. However, it has its own limitations. For example, it cannot detect attacks carried out locally that have no manifestations on the network card (e.g., attacks executed by a local user from the console).

The host-based intrusion detection system (H-IDS) monitors the host on which the sensor is installed. The event stream can be system call sequences, log records from one or more services, operating system logs, or any other log for activities within the monitored machine. Normal activities as well as intrusions may consist of a single event or of a series of events. For example, an FTP session might generate log records on the host that runs the FTP server indicating the start of the session, successful authentication, transferred files, examined directories and termination of the session. These records may be mixed with the records of other simultaneous FTP sessions as well as records from other services. The main advantage of HIDS is that it can theoretically detect intrusions when a local legitimate user tries to perform some illegal actions and can help detect attacks such as Trojan or other attacks that may involve software integrity breaches without leaving traces on network traffic. Although the HIDS has the advantage of not requiring additional hardware, it can cause a significant degradation in the performance of its host due to the overhead of the HIDS operations. Another limitation is the difficulty to port it from one platform to another.

Analysis methods

The primary classification of IDS remains the method of analysis. Two methods exist today: the scenario and behavioral approaches (Müller, 2003).

The scenario approach looks in the activity of the monitored element fingerprints (or signatures) of known attacks. This type of IDS is purely reactive and it can only detect attacks that has been signaled.

The behavioural approach detects anomalies. The implementation always includes a learning phase during which the IDS will see the normal operation of the elements monitored. It is thus able to report deviations from the reference function. The mechanism of intrusion detection and analysis are centralized, which means that data collection is local.

The complexity of coordinated attacks does not facilitate their detection by a single entity. Indeed, each entity having a limited local view of the network, it is very difficult to detect such attacks. Detecting such attacks requires a correlation of different tests performed at different points in the network. The various entities must then communicate their analysis and cooperate to effectively detect attacks.

Multi-agent system

A multi-agent system (MAS) consists of a set of IT processes taking place simultaneously, so several officers living at the same time, share common resources and communicate amongst themselves (Boudaoud, 2000). These agents are characterized particularly by their ability autonomy, adaptation, communication or coordination to react against complex attacks in a dynamic environment. Architecture of multi-agent hybrid system allows the officer to have a reactive behavior when situations require, and deliberative behavior in other circumstances.

A reactive agent only reacts to changes in the environment. A deliberative agent performs some deliberation in choosing his action. It must use planning techniques to predict the actions to bring him to his goal. The agent may combine information about his goals with information on the results of its actions to choose actions that will enable it achieve its goals is such a way that it allows him to improve and adapt to their environment.

A PLATFORM FOR INTRUSION DETECTION

Motivation of the proposed approach

Many network attacks are characterized by abnormal behavior in various network elements. It is therefore very important to distribute the functions of detecting several entities that oversee different parts of the network (Benhadou et al., 2009).

Excessive exchange of information between the distributed entities can congest the network. It is important to let the entity overseeing a network element perform a local analysis and detect intrusions at this level. Thus the distributed entities must be independent (Raoui et al., 2009). The functions of intrusion detection must be modified to adapt to changing user behavior and evolution of complex networks by sending the tasks delegated to autonomous entities. The objective is to design a solution for intrusion detection that is soft and flexible to adapt to this dynamic environment and the increasing complexity of attacks.

Proposal

We distributed intelligent intrusion detection based on multi-agent system consisting of two levels of analysis. On one hand, it allows the distribution of the monitoring / detection of several entities and

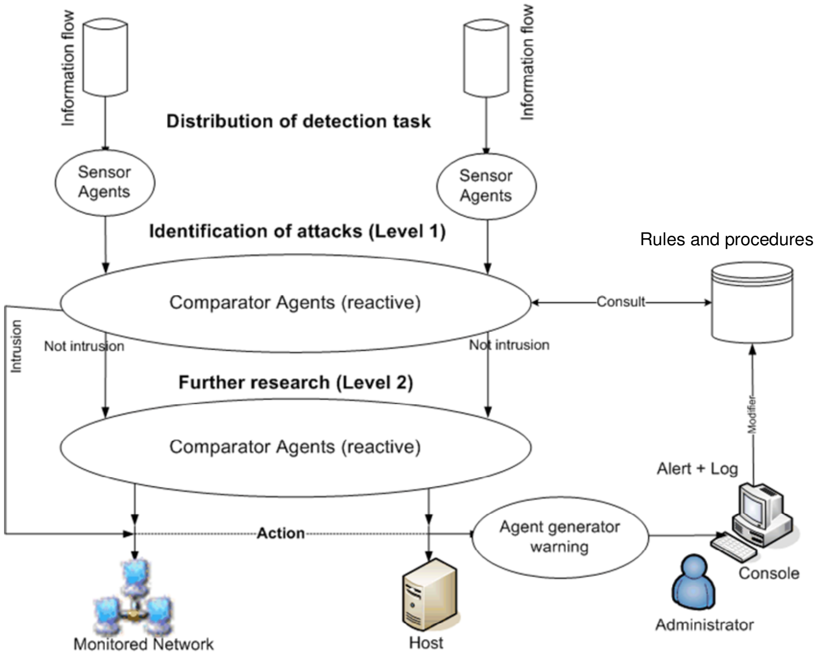

Figure 1. Proposed platform of intrusion detection.

enforces rules and safety procedures to eliminate the strong and known attacks and on the other hand, benefit cognitive abilities of its staff to conduct a more thorough assessment of intrusions that can represent low threats. Making decision is distributed to ensure a high level of intrusion detection.

Architecture of proposed platform of intrusion detection

The proposed architecture consists of several agents distributed at different network points with different roles. These agents combine the responsive capabilities with cognitive abilities. It consists of two levels; the first level is based on rules and safety procedures. This approach shapes the rules that describe the unintended uses, relying on past intrusions or known weaknesses. The effectiveness of this approach is based on rapid response officers to eliminate the known attacks.

Its aim is to block intrusions complex unknown by the system or represent low threat level 2. This device identifies these events and automatically determines whether action is needed due to cognitive abilities of its staff. Figure 1 shows the block diagram of the distributed platform based on multi-agent system.

Principle of operation

The proposed intrusion detection system consists of several agents, monitoring the network or sensitive positions, with the following characteristics:

The analyzer based on a distributed approach, using multi-agent system, includes:

Agents; responsible for collecting sensor data exchanged on the network or those who arrive at a sensitive position and will be transmitted to comparators.

Comparators agents with reactive capacity; responsible for comparing the flow of events with the rules and procedures describing the unintended uses.

If a rule is violated when there is interference and the degree of threat that may represent the intrusion, the officer will compare the direct traffic to the cognitive agent to search further, or it blocks traffic and cuts the connection.

Cognitive agents with adaptive and learning function; their role is to check whether the event may represent a low threat and react quickly when an intrusion blocks traffic and prevent the agent generator warning.

Agents generating alerts; their role is to generate an alert message to the appropriate administrator and store information about the event in a log file.

Description of the method of detection

Used analysis method

Gather the event flow passing through the agent sensor. Analyze the agent, compare the data collected and compare them to a database of rules and procedures to determine the degree of threat represented by the intrusion.

Check if the level of intrusion is acceptable or not and determine the direction of traffic, if it will continue its path towards cognitive agent or close the connection.

Make the cognitive agent further investigate the flow of event, determine its condition and decide if the traffic will continue its path toward the target or be blocked

Store information on the event at risk in a file log and generate a notification message intrusion by generating agent alert.

Fuel basic rules and procedures by the security administrator.

IMPLEMENTING A PLATFORM

Design model

In this section we propose a design based on the AUML language. Agent UML is an extension of UML to take

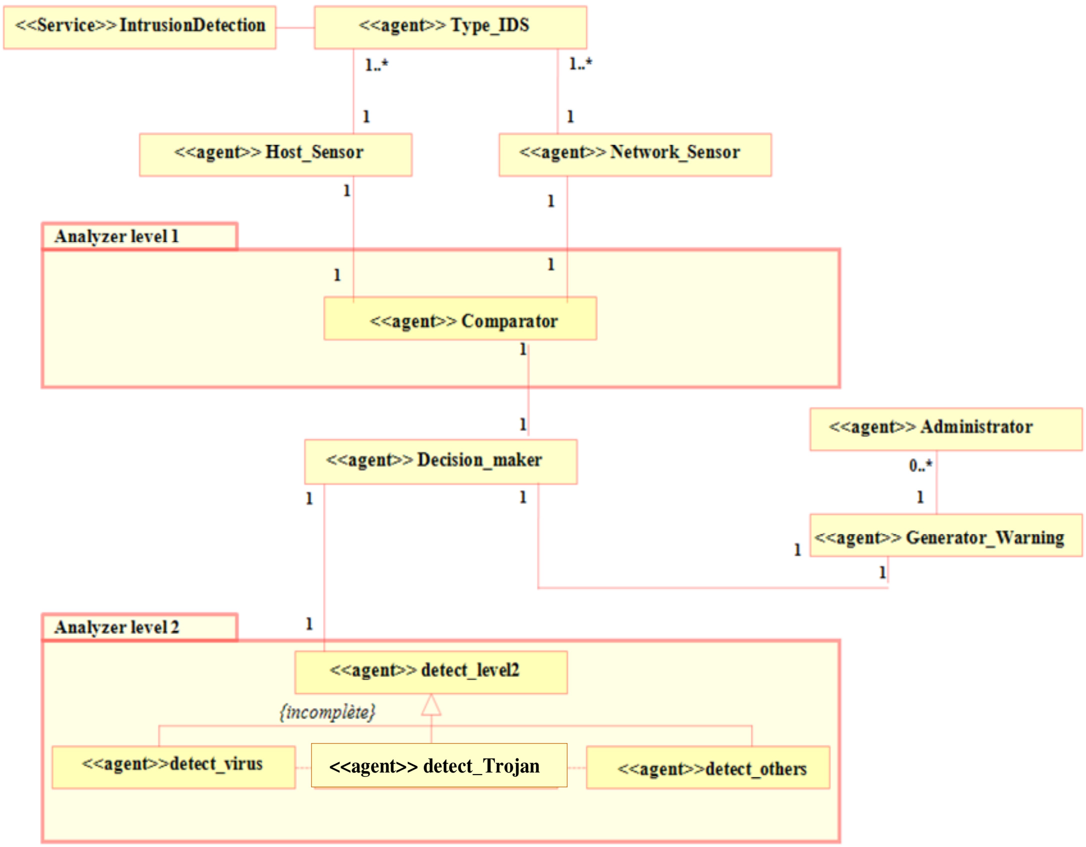

Figure 2. Agent class diagram conceptually.

representations proposed by UML (Huget, 2002). It contains ten types diagrams symbolizing many different views to represent particular concepts of information system. They fall into two main groups:

(i) Behavioral diagrams or dynamic diagrams: Sequence diagrams, collaboration diagrams, activity diagrams, state chart, use case diagrams.
(ii) Structural diagrams or static diagrams: Class diagrams, object diagrams, packages, component diagrams, deployment diagrams

These diagrams are not necessarily all products at modeling. The design of the proposed architecture is described through the two class diagrams and sequence agents to illustrate respectively the static and dynamic platform.

Static aspect

Agent UML allows the representation of several levels of abstraction in the design class diagrams. We consider these two levels: the conceptual and implementation levels.

The conceptual level

It is high enough for the multi-agent system eliminating all surface information for understanding the structure of the system. The agent class diagram in Figure 2 shows the conceptual level of the platform.

The implementation level

This gives in detail the contents of agents. Figure 3 shows a portion of the class diagram for the agents level implementation.

Dynamic aspects

The sequence diagrams in AUML represent message exchanges between agents. The sequence diagram given in Figure 4 shows the interaction between different agents over time in the case of recovery of information flows at the analyzer level 1. The sequence diagram shown in Figure 5 shows the interaction between different agents over time in the case of recovery of information flows at the analyzer level 2.

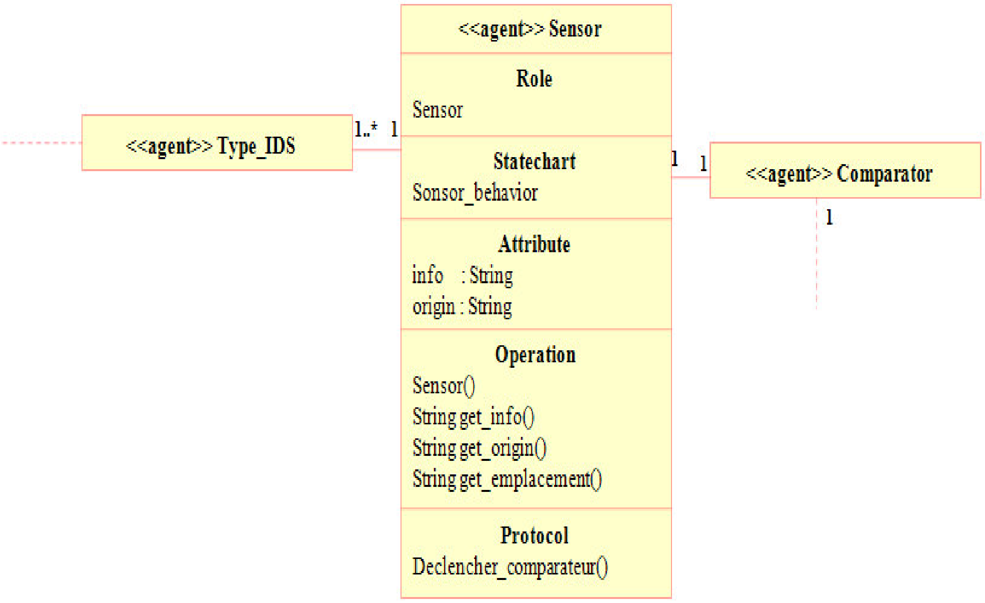

Figure 3. Class diagram level implementation agents.

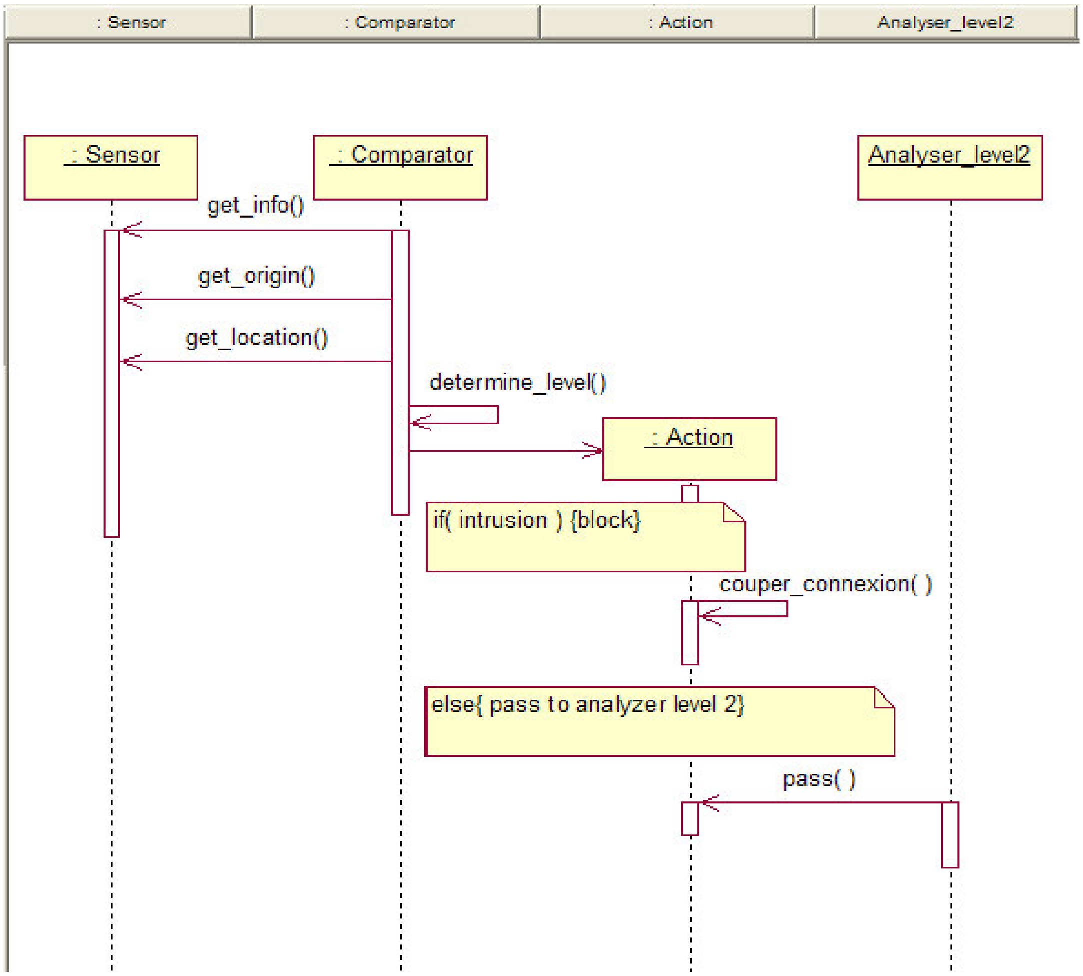

Figure 4. Sequence diagram.

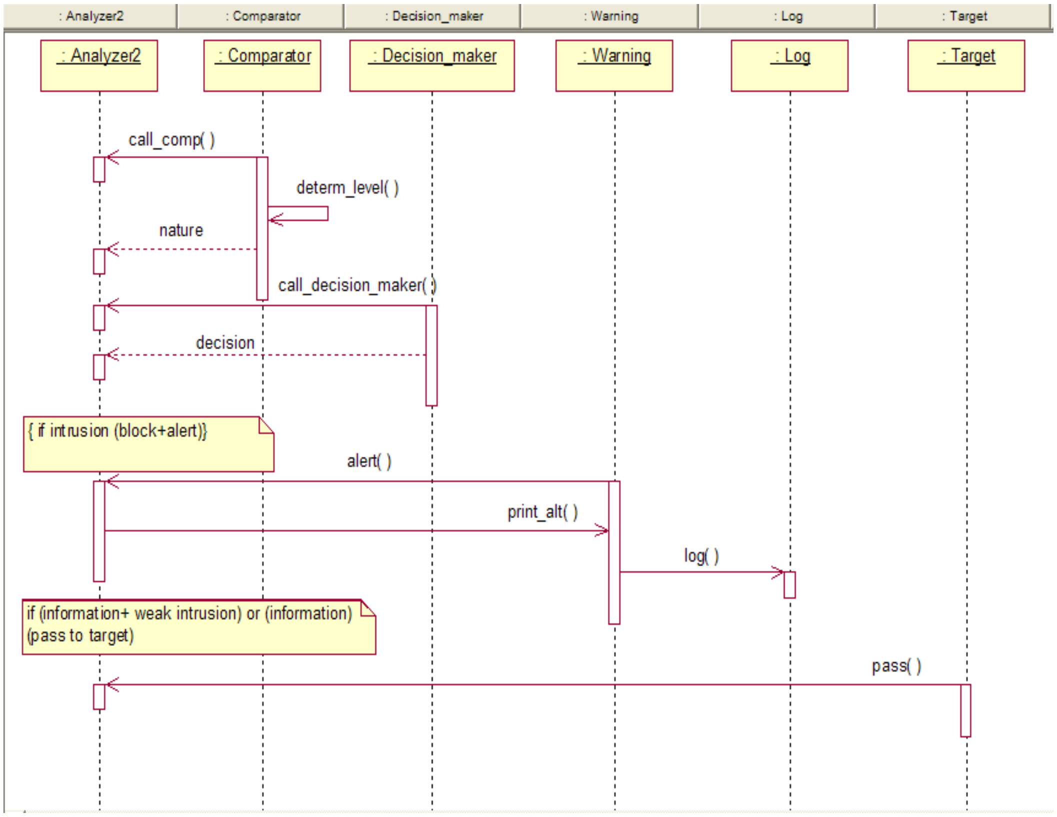

Figure 5. Sequence diagram.

Implementing the simulation platform

After the design phase of the proposed model, we developed a simulation application using an open source distribution (Java and Linux). The simulation platform was developed using a new methodology in the assessment mechanism system intrusion detection to reflect the goals already set.

The result achieved from the application of simulation is that it allowed us to test the efficiency of the analyser level. In fact, we sent some attacks in which the rules were applied on the analyser level 1 and it reacted and blocked those attacks, thanks to the capacity of the reactive agents.

At the same time, for testing the intelligence of the agent's analyser level 2, we sent some attacks which are unknown by the database rules and are not used with the analyser level. In contrast, with the knowledge used by the analyser level 2, they were able to block those attacks. Furthermore, we tested the pertinence brought by the analyser level 2 to our security platform and it was a real success.

Conclusion

In this paper, we presented a new mechanism for detecting intrusions formed by an intelligent, distributed architecture based on multi-agent aspect of two levels of analysis, which allows quick response against the attack complex, assesses the state of the flow captured by reference to rules and procedures. On the other hand, it detects unknown attacks on the system and reinforces the level of security provided to the target monitored using the cognitive agents of the second analyzer.

Looking ahead, we are currently working on adapting the behavior of agents to automate the generation mechanism of a rule which corresponds to an attack not known. This process allows the automatic feeding of the basic rules and new rules on security procedures dedicated to the recognition of an intrusion or unknown attack. Also, most of the systems of intrusion detection are based on operating systems; they can sometimes themselves targets of attack. We plan to replace the Parser level 1 by hardware (PLC) to protect intrusion detection systems from attacks to which they may be subjected to.

REFERENCES

Solange GH (October 2004).« Sécurité informatique et réseaux » DUNOD Edition.

Zalewski M (Febrary 2008).« Menaces sur le réseau -Sécurité informatique : guide pratique des attaques passives et indirectes ».

Northcutt S, Novak J, Mc Lachlan D (2001). « Détection des intrusions réseaux », Editor: Campus Press,

Müller K (Mai 2003).« IDS – Systèmes de Détection d'Intrusions, Partie I », http://www.linuxfocus.org/Français/May2003/article292.shtml.

Müller K (July 2003). « IDS – Systèmes de Détection d'Intrusions, Partie II », http://www.linuxfocus.org/Français/July2003/article294.shtml.

Boudaoud K (2000).« Un système multi-agents pour la détection d'intrusions », LIP6-OASIS.

Benhadou S, Raoui D, Medromi H (2009). «Nouvelle méthodologie distribuée de sécurité à base de système multiagents », ICeP'09 Marrakech, September 25th – 27 th, 2009.

Raoui D, Benhadou S, Medromi H (2009). « Conception d'une plateforme distribuée, temps réel de détection d'intrusions », Wotic'09 Agadir, December 24th – 25th,2009.

Huget M (2002). Une application d'AgentUMLau Supply Chain Management, JFIADSMA.