Hybrid Approach based Mobile Agent for Intrusion Detection System: HAMA-IDS

Boukhlouf Djemaa, Kazar Okba
Computer science department
University of Biskra
07000 Algeria
{djem_info, kazarokba}@yahoo.fr

ABSTRACT: *Information systems are more and more opened on Internet today. This opening, a prior beneficial, nevertheless raises a major problem: it ensues from it an increasing number of attacks. The IDS was developed with the aim of detecting abnormal functioning of information systems and networks, indicating that actions not corresponding to the safety policy are led by one or several users.*

Centralized IDS suffer from significant limitations when used in high speed networks, especially when they face distributed attacks. In this paper we propose a distributed hybrid approach based on mobile agents for the detection of intrusion: HAMA-IDS (Hybrid Approach based on Mobile Agents for Intrusion Detection System). The proposed approach uses the platform Aglets for the creation and the distribution of four types of mobile agents. The Collector agent is used to the gathering of information, when the Analyzer and Redirector agent are responsible of the analysis (scenarios and behavioral analysis). The generator agent is responsible to the launch of these agents and to the management of messages received from these last ones.

Keywords: Mobile Agents, Intrusion detection system, Aglets, Hybrid approach

Received: 18 November 2011, Revised 3 January 2012, Accepted 13 January 2012

1. Introduction

The detection of intrusion consists in analyzing the information collected by the mechanisms of audit of security, in search of possible attacks. This concept was introduced in 1980 by JAMES ANDERSON. But the real departure of the domain was marked by the publication of a model of detection of the interventions by Denning in 1987 [9].

Several systems to detect intrusion are existed, some are based on the detection of abnormalities and the others are based on the signatures of attacks. These systems of detection bring to light the new sectors of research, which includes the artificial intelligence, Data mining, statistical techniques, structures of agent.

In this paper, we are interested in the exploitation of the technology of the mobile agents in a distributed system of intrusions detection. Therefore we propose a model HAMA-IDS (Hybrid Approach based Mobile Agent for Intrusion Detection System), which is based on a hybrid approach for the information analysis. The proposed approach uses four types of agents (generator Agent, analyzer Agent, redirector Agent, Collector Agent). The generator agent creates and distributes the various agents. The analyzer and redirector agents analyze the information collected by the collector agent basing on the approach of hybrid analysis.

This paper is organized of including the proposed approach, and in the following section, we present some concepts concerning an IDS and mobile agents, then in the section three we describe the model HAMA-IDS.

2. Background and motivation

To present the characteristics of the system of intrusion detection, we use the classification proposed in [3]. This one, represented on the figure 1, uses the following criteria of classification:

- The principle of intrusion detection
- The behavior after detection
- The source of the data
- The frequency of use.

Before describing the model HAMA-IDS, we present some necessary concepts which form a base of the model.

2.1 Mobile Agents

An agent [6] is an autonomous entity, reactive and capable of communicating with systems based on the knowledge.

There is an outfit of reasons which justify the choice to use the mobile agents are according to [3][7], we use the following ones:

- Reduce the load of networks,
- Surmount the latent period on the network,
- Run in a asynchronous and autonomous way,
- Adapt itself dynamically to the environments of execution,
- Heterogeneous,
- Strong and tolerant.

These properties allow [3] [4][5] [8]us to imply the mobile agents in the field of the intrusion detection. To do it, we used the platform of mobile agents called: Aglets.

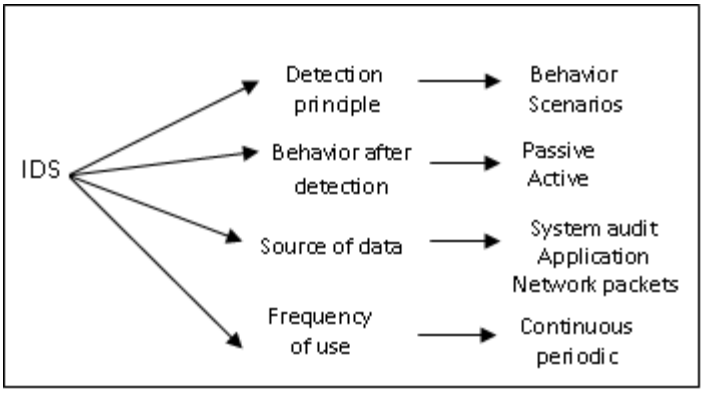

Figure 1. Taxonomy of intrusion detection systems [2]

2.2 Aglets

The platform “Aglets” [6] allows to manipulate and to execute the mobile agents. Indeed, Aglets (Agents Applet) are Java mobiles objects which can move from one machine to another. Aglet which is carried out on a host can stop its execution, to be off-set towards a distant host and continues this execution on the new environment.

A system of Aglets allows [6]:

- To provide an easy and complete model to program the mobile agents.
- To support the dynamic and powerful communication.

- To conceive a reusable and extensible architecture.
- To conceive a harmonious architecture with the existing technology of Web/Java.
- To provide the mechanisms of security with the mobile agents.

2.3 Intrusion detection methods
Two families of methods are proposed:

2.3.1 Behavioral Approach (detection of abnormality)
This approach [3] consists in detecting an intrusion according to the past behavior of the user. For this purpose, it is beforehand necessary to raise a user profile from its habits and to activate an alert when events except profile occur. It is a question of choosing a method of description of the normal behavior of a user (Expert systems, Statistical Prospinning, Neuronal networks…)

2.3.2 Misuse approach
It consists of detecting intrusion or attacks exploiting vulnerabilities of systems. It bases itself on the fact that any known attack produces a specific signature in the recordings of audit. Thus, it requires knowledge a priori attacks to be detected. An alarm is emitted when the track of a known attack is detected in the recordings of audit.

This approach [1] uses several techniques: Expert systems, Pattern matching, Genetic algorithms…

2.3.3 Hybrid approach
Certain systems use a combination of the behavioral approach and the approach by scenarios [10] to remedy the inconveniences of each.

3. The proposed approach

This section recapitulates the conception of the proposed distributed system of intrusion detection, by using autonomous and mobile agents. The agent-based unified modeling language (AUML) [11] [12] is used for the modeling of the proposed system. Agents use is justified by the advantages of the cooperative work offered by the agents and the mobility offered by Aglets where the hybrid intrusion detection system can take advantage of them.

3.1 The intrusion detection model
The model used in our system is based on the hybrid approach of intrusion detection. For this reason two types of analyses are made: Pattern matching and behavioral analysis.

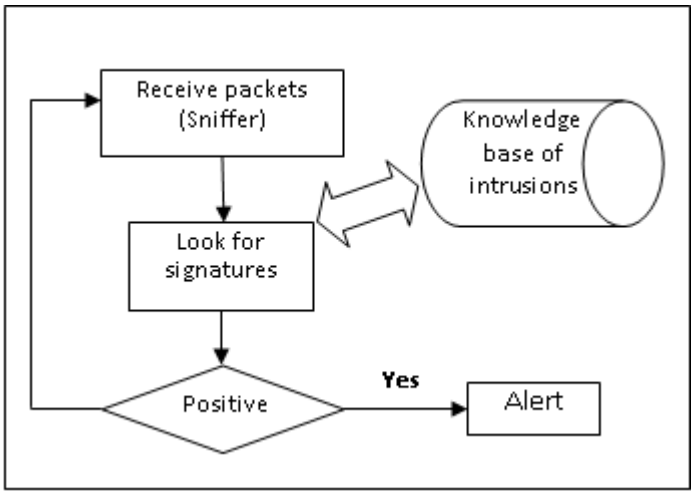

Figure2. Pattern matching organigram

3.1.1 Pattern matching

In our approach, the technique used for the analysis by scenario is based on the pattern matching which is represented by the figure 2.

The *sniffer* has for role to capture the information circulated in the network, this information is used by the pattern matching for comparison with those of the base D.B Sig to detect if there is or not of possible attacks.

3.2 Behavioral analysis

This analysis is based on the statistical calculations inspired by the work of Denning on 1987 [9]. We mention for example:

- An abnormal rate of erroneous passwords by a user not known by the system
- The connection of a user legally to the system at the unusual time
- An attack by denial of service which is going to give rise to a rate of use abnormally raised by certain resources of the system.

After the detection of one attack by this technique, it is necessary to update the database of signatures (D.B Sig) to the worried in a future analysis.

3.2 The global architecture of HAMA-IDS

In the figure 3 is presented the architecture of HAMA-IDS. A sniffer is used to gather the information necessary for the analysis by the analyzers and redirectors agents. There are two databases shared between these agents as indicated on the figure 3. The database *D.B Sig* contains signatures of attacks, and the database *D. B stat* contains information on the behavior of the system which is gathered by using statistics inspired from [1]. The communication between the agents is asynchronous which is supported by Aglets; where the agent sends the message and continuous its work. The different components of our system are detailed in the section 3.3.

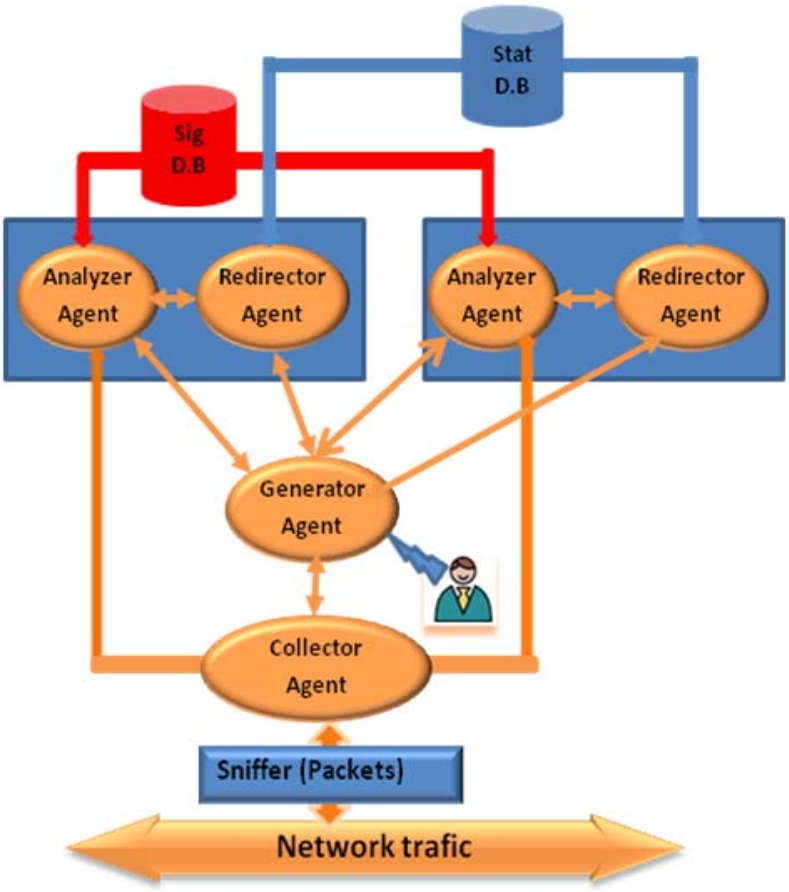

Figure 3. General architecture of HAMA-IDS

3.3 Structural scheme of HAMA-IDS

In this section, we give details entities of our intrusion detection system. We specify some information of our agents and objects manipulated by these agents. We also give their diagrams of class.

3.3.1 Generator Agent

It is the stationary entity which constitutes the heart of the system. Among its roles we can quote: creation and ending of the various agents, management of the alarms, interaction with the various agents, update of databases, and detection of the connections. The diagram of class corresponding to this agent is presented in the figure 4.

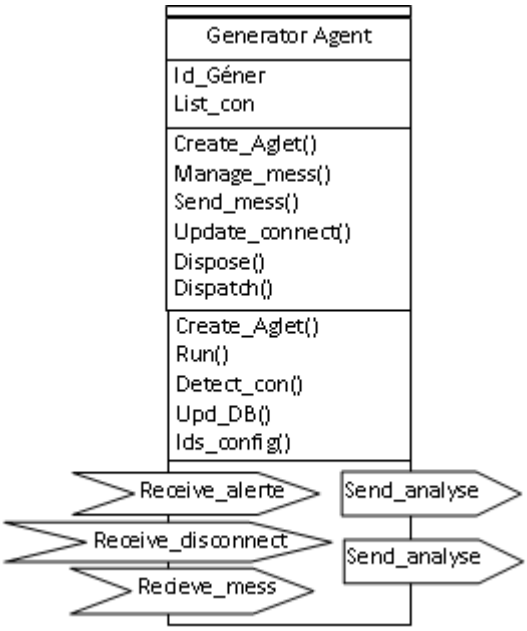

Figure 4. Class diagram of Generator Agent

3.3.2 Collector Agent

Its role is the collection of information (Packets) and the preparation of these last ones. A sniffer is used for the listening of the network traffic. The class diagram of this agent is shown in the figure 5.

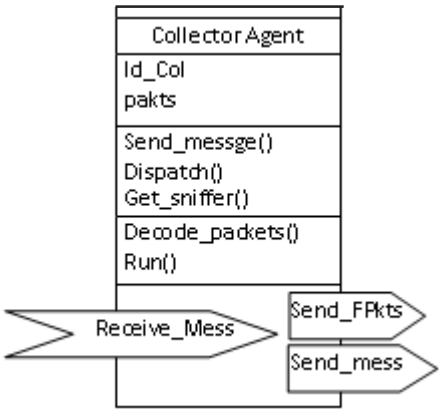

Figure 5. Class diagram of Collector Agent

3.3.3 Analyzer Agent

It is a mobile agent which can move between the posts for the analysis of received packets from the collector agent. This analysis is based on the use of the signatures database B. D Sig (pattern matching analyzes). If the analyzer agent detects an

attack it sends an alarm message to the generator agent. If the packets do not contain intrusion's signature, it sends packets to the redirector agent.

The class diagram of analyzer agent is represented in the figure 6.

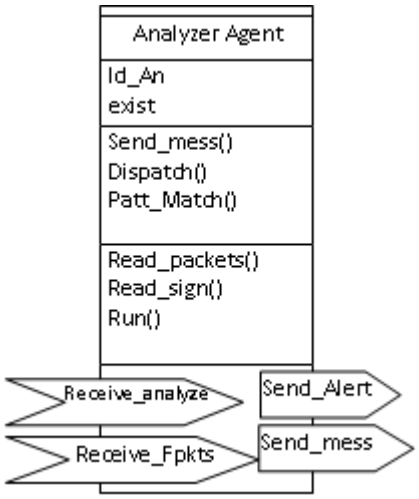

Figure 6. Class diagram of Analyzer Agent

3.3.4 Redirector Agent

It is a mobile agent its role is the analysis of the received packets using the B.D Stat database (behavioral analysis) which is based on predefined statistics. In the case of detection of intrusion it sends an alarm message to the generator agent. The figure 7 represents the class diagram of this agent.

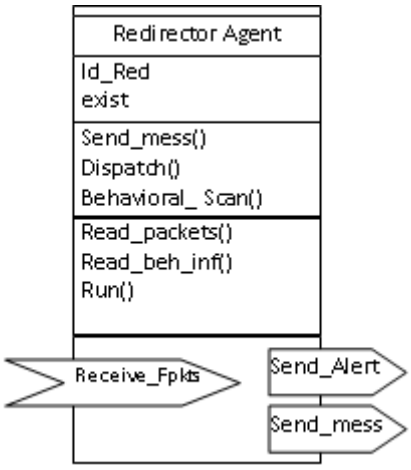

Figure 7. Diagram class of Redirector agent Agent

3.3.5 Manager class

This class is added for the identification of the users when they connect. It represents the officer of security of the system. The figure 8 shows the diagram of this class.

The figure 9 presents a class diagram for the conceptual level of our system, showing the various classes of HAMA-IDS.

3.4 The functional scheme of HAMA-IDS

Here we describe the main activities of the IDS illustrated by diagrams of sequence.

Figure 8. Manager Class

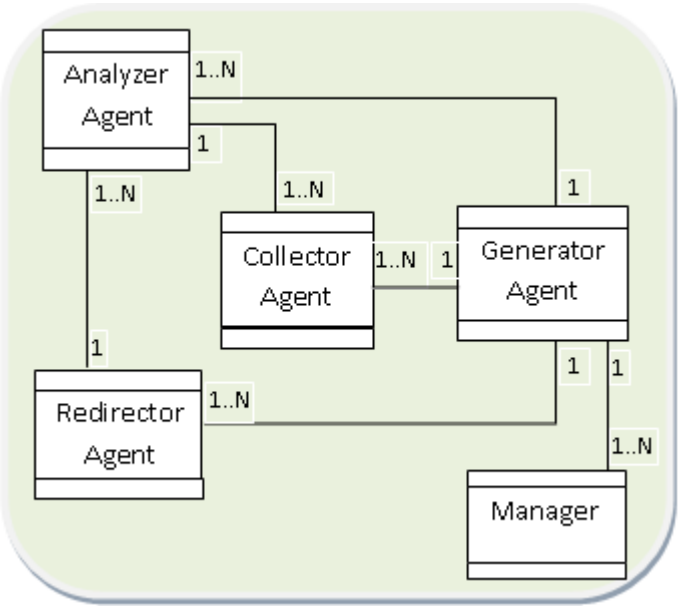

Figure 9. The class diagram of HAMA-IDS

3.4.1 Activity1: The collect of information

This activity is illustrated by the diagram of sequence in the figure 10 Where:

The operations are:

-Detect_con (): obtain the address of the detected station if the user is known else disconnect.
-Update_connect (): update the list of connected stations.
-Get_sniffer (): read the output of the sniffer.
-Decode_packets (): prepare packets.

And the events are:

From the Generator agent to the collector agent

-Send_Collecte: ask the collector agent to begin the collection of information of the detected station.

3.4.2 Activity2 : Analyze and detection of intrusion (Pattern matching)

Activity2 is illustrated by the figure 11 Where:

The operations are:

-Read_packets (): read packets.
-Read_sign (): read the list of the signatures of attacks.
-Patt_Match (): analyze by Pattern Matching.
-Upd_DB (): update the database of signatures.

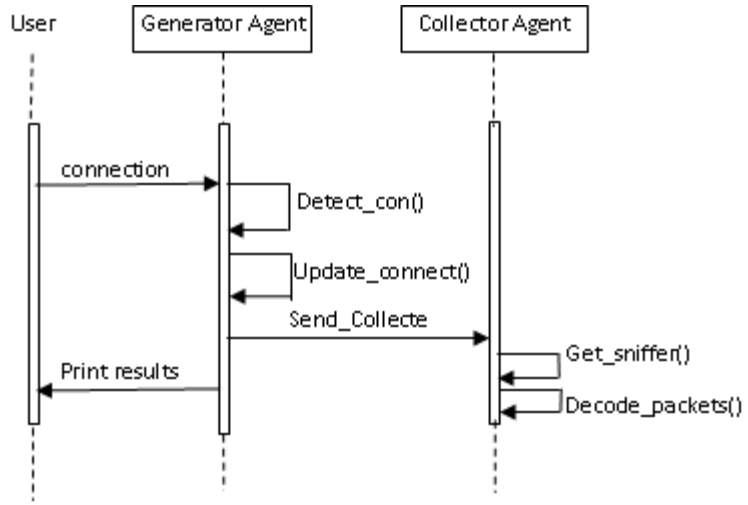

Figure 10. The sequence diagram of activity1

The events are:

From the generator agent to the analyzer agent

-Send_Analyze: ask the analyzer agent for start the analysis of the station.

Of the analyzer agent to the generator agent

-Send_Alert: send a message concerning the detected attack

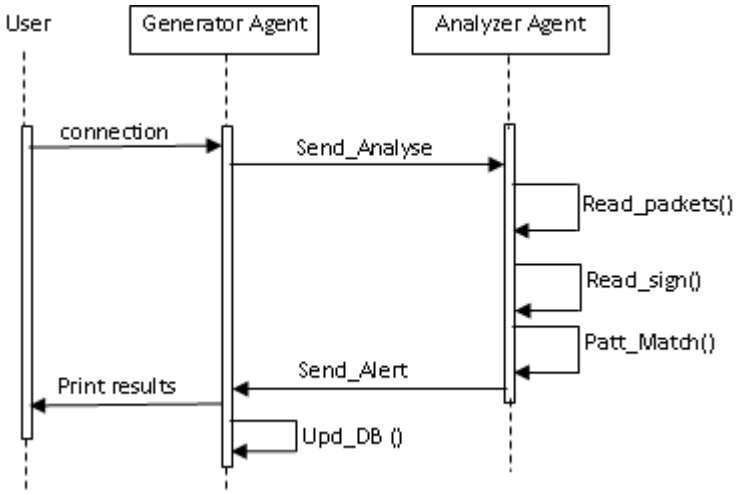

Figure 11. The sequence diagram activity2

3.4.3 Activity3 : Analyze and detection of intrusion (statistic analyze)

The diagram of sequence of this activity is presented in the figure 12 where:

The operations are:

-Read_packets (): read packets.

-Read_beh_inf (): read the predefined statistics.

-Behavioral_scan (): behavioral analysis

The events:

From the generator agent to the redirector agent:

-Send_Analyze: demand of analysis.

Of the redirector agent to the generator agent:

-Send_Alert: send of a message concerning the detected attack.

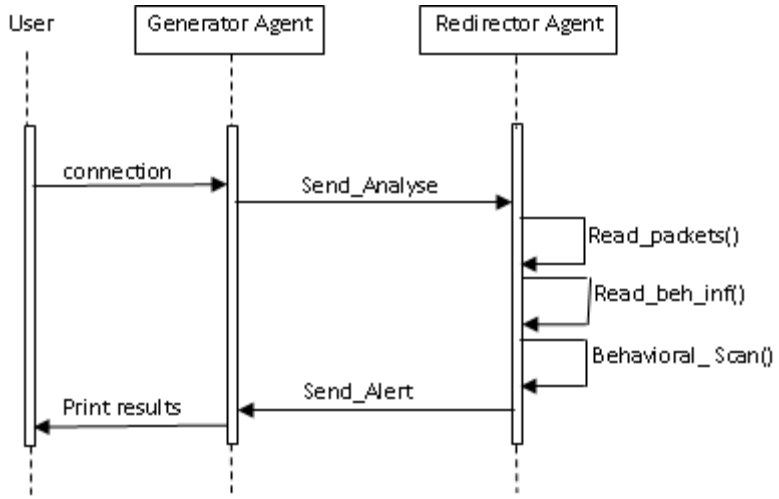

Figure12. The sequence diagram of activity3

Figure13. General interface of the system

4. Implementation and test

We exploit the plat-form of Aglets to create and distribute the mobile agents. This requires the installation of the agent server of

"*Aglets*" [14]. The IDS system requires also the tool of development JAVA (The JDK 5.0) of Sun Microsystems.

For testing the prototype, we are using a local area network consisted of at least two stand-alone machines. On each machine, agent's server "*Aglets*" (the TAHITI server) is installed. We use the Java [13] programming language in our implementation.

The general interface of the system is illustrated in the figure13.

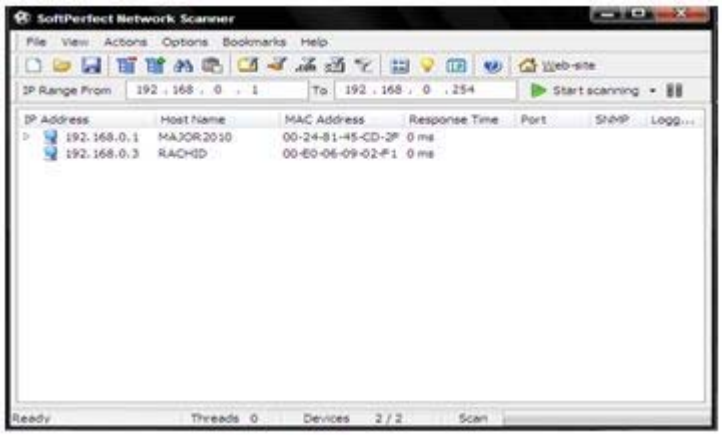

Figure14. SoftPerfect software interface

In order to capture the Ip adresses of the different Pcs we use SoftPerfect [15] software. The menu of the last one is shown in the figure 14.

The main menu is represented in the figure 15. First we can detect the Ip adresses of the different machines witch are connected to the network after that; we can launch the scan of the network.

We are applyed our system using three Pcs witch are connected between them. In order to test our system, we are simulated a SYN flood attack using the HPING tool [7] which is able to send custom TCP/IP packets to network hosts.

Figure 15. The main menu

A SYN flood is a type of Denial of Service attack. To realize this kind of intrusion the attacker tries to create a huge amount of connections in the SYN RECEIVED state until the backlog queue overflows. The SYN RECEIVED state is created when the victim host receives a connection request (a packet with SYN flag set) and allocates for it some memory resources.

The system detects this attack on one of them. A message is sent to the Generator agent and we have the alert as follows:

Figure 16. Alert of HAMA-IDS

If the intrusion doesn't exist in the database of intrusion (DB_IDS), it is updated with adding all the properties of this new intrusion.

5. Conclusion

In this paper we proposed a hybrid approach based on the mobile agents for the detection of intrusion (HAMA-IDS). The architecture allows the treatment of information directly to the place where it is available via the utilization of mobile agents (aglets). Thus, the method is based on the platform Aglets for the creation and distribution of agents. These last ones can move from post to post in order to analyze packets collected by the collector agents. The hybrid analysis is assured by the analyzers and redirectors agents, so that they detect possible attacks.

The proposed approach has the following particularities:

- The application of the mobile agents for the intrusion detection facilitates the distribution of the IDS (Unlike the centralized systems)
- The use of a hybrid approach takes advantages of both methods of intrusion detection (scenario and behavioral method)
- The platform Aglets gives the possibility of using methods for the management of the mobile agents and for their distribution.

However the security protection of the agents used in the model is an important problem, which will be addressed in a future work.

References

[1] Boudaoud, K. (2002). Detection of intrusions: A new approach by multi - agents systems, thesis of doctorate, Lausanne, EPFL (in french).

[2] Boudjelida, A. (2008). Increased Naïfs Bayesiens Networks TAN for Systems of intrusion Detection, Prepared Memory for obtaining Of the Diploma of Magister ISI. (in french).

[3] BARIKA, F.A.M. (2003). Toward an Intelligent IDS based on Mobile agents, Memory of DEA University of Tunis Superior Institute of Management. (in french).