AN IMMUNE AGENTS SYSTEM FOR NETWORK INTRUSIONS DETECTION

Noria Benyettou[1], Abdelkader Benyettou[2] and Vincent Rodin[3]

[1]University of Science and Technology of Oran Mohamed Boudiaf USTOMB, SIMPA Laboratory, BP 1505 el Menaouar Oran-Algeria,
[2]University of Science and Technology of Oran Mohamed Boudiaf USTOMB, BP 1505 el Menaouar Oran-Algeria,
[3]European University of Brittany, UMR CNRS 6285, Lab-STICC, CS93837, 29238 Brest CEDX3, France,
[1]n.benyettou@gmail.com,[2]a_benyettou@yahoo.fr
[3]Vincent.rodin@univ-brest.fr

ABSTRACT

With the development growing of network technology, computer networks became increasingly wide and opened. This evolution gave birth to new techniques allowing accessibility of networks and information systems with an aim of facilitating the transactions. Consequently, these techniques gave also birth to new forms of threats. In this article, we present the utility to use a system of intrusion detection through a presentation of these characteristics. Using as inspiration the immune biological system, we propose a model of artificial immune system which is integrated in the behavior of distributed agents on the network in order to ensure a good detection of intrusions. We also present the internal structure of the immune agents and their capacity to distinguish between self and not self. The agents are able to achieve simultaneous treatments, are able to auto-adaptable to environment evolution and have also the property of distributed coordination.

KEYWORDS

Intrusion Detection System, Artificial Immune System, Multi-Agents System.

1. INTRODUCTION

Networks safety and the intrusion detection systems are the subject of several works; first models goes back to1984, they are focused on statistical analysis, expert system, and classification rules (IDES [5, 13], Nides[3,13], MIDAS[8], DIDS [15], NADIR [9], ADAM [4]). These models are already based on the attacks indexed in knowledge base. However, with the networks widening they generate much false alarm, and became less and less reliable to new attack's forms. To overcome difficulties met by these models, new research works are interested in multi-agents systems and immunology principles such as (MAAIS [19], NIDIMA [14], DAMIDAIS [11], IMASNID [7], etc). These systems succeed in decreasing the false alarm rate thanks to the processes employed; namely communication process between the agents and the distinction process between self and not-self.

David C. Wyld et al. (Eds) : SAI, CDKP, ICAITA, NeCoM, SEAS, CMCA, ASUC, Signal - 2014
pp. 01–11, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.41101

That is why, we present in this document a new model a Multi-Agents System (MAS) inspired by an Immune algorithm for the Intrusion Detection. Our choice is justified by the distributed and opened character of networks. Given the failure of the exist methods to detects new attacks; we integrate into our agents the artificial immune system mechanism. Artificial immune systems are inspired by the coordination principles and the parallel functioning of the biological immune system (life cycle, immunizing, immature tolerance, mature and memory lymphocyte).

2. INTRUSION DETECTION SYSTEM CHARACTERISTICS

To neutralize in real time illegal intrusion attempts, intrusions detection system must be executed constantly in the host or in the network.

The major inconveniences of the existing IDS [6] are:

1. Their difficulties to adapt oneself to the changes of the network architecture and especially how to integrate these modifications in the detection methods.
2. Their high rate of false-positives (false alert).

The intrusion detection system is effective if it has the following characteristics [12]:

- Distribution: to ensure the monitoring in various nodes of the network the analysis task must be distributed.
- Autonomy: for a fast analysis, distributed entities must be autonomous at the host level.
- Delegation: each autonomous entity must be able to carry out its new tasks in a dynamical way.
- Communication and cooperation: complexity of the coordinated attacks requires a correlation of several analyses carried out in network nodes.
- Reactivity: intrusion detection major goal is to react quickly to an intrusion.
- Adaptability: an intrusions detection system must be open to all network architecture changes.

Concepts of robustness, emergence, auto-organization, adaptability, and communication and cooperation are part of the basis fundament of the multi-agents systems .For this purpose we judged that the multi-agents systems (MAS) are very suitable to answered to these characteristics.

3. ARTIFICIAL MULTI-AGENTS IMMUNE SYSTEM

3.1 Multi-Agent System

The agents are able to achieve simultaneous treatments, are able to auto-adaptable to the evolution of environment and have also the property of distributed coordination.

The Multi-agents systems can be viewed as a collection of autonomous artificial entities able to perform various tasks through interaction, coordination, communication, collective intelligence and emergence of patterns of behavior.

Artificial immune system (AIS) is a set of algorithms inspired by biological immune system principles and functions. This last exploits the characteristics of natural immune system, as regards the learning and the memorizing in order to solve complex problems in artificial intelligence field.

The biological immune system is a robust and powerful process, known for its distributed simultaneous treatment orders of the operations and adaptive within the limit of its function [17]. Biological and multi-agents systems have common characteristics.

Biological cells are modeled by the agents; each agent is equipped with a set of receiver in its surface and has an internal behavior. Agents are submitted to environment rules and also to other agent's influence [18]. This is why it seems natural to model an intrusion detection system by the MAS based on biological immune systems principles.

Table 1. IB and AI common points

Biological immune system (IB)	**Immune Agent (AI)**
Antibody	Detector Agent
Antigen	The binary string From ip frame
Immune memory	memory Agent
The binding between antibody and antigen	Any intervals matching rule
Immune cells Lifecycle	detector agent Time- life
antibody/antigen Affinity	frame/ agent-detector Affinity

Table1 summarizes the main common points between biological immunity and the immunity agents in our model.

4. IMMUNE COMPONENTS DESCRIPTION

In this section, the principal immune components which are used in our architecture will be defined.

Antigens: they are considered in different approaches [7][11] as bit strings extracted from ip-packets, including ip address, port number, protocol type. Set $U=\{0,1\}L$ ($L>0$), and $Ag \subset U$, and the set U can be divided into self and notself. The self indicates normal network behavior; on the other hand, notself indicates the abnormal network [16].

Antibodies: correspond to bit strings, they have the similar length as antigens; antibodies are constantly in search of antigens in order to match them and also to increase their lifespan.

Set $AB=\{ab/ab=<b,t,ag>, b,ag \in U \wedge t \in N\}$.

Where 'b' is the antibody bit string whose length is L, 'ag' is the antigen detected by the antibody and't' is the antigen number matched by antibody[2]. There exist three states for antibodies: immature, mature and memory. Antibodies are able to detect an intrusion, in our architecture they are represented by D-agents.

Immature stage: Correspond to the first stage of our cell. In this stage, the immature Antibodies (Imb) are randomly generated by the generator detector. Immature immunocytes set is :

$Imb=\{<b,t,ag> \in Match /b \in U, t<\theta, ag=\emptyset\}$ and $Match=\{<x,y>/x,y \in U, f\ match\ (x,y) = 1\}$, which will evolve into Imb through self-tolerance. If an Antibody is not matched with notself for step

evolution; then it will die after a certain period of time.

Mature stage: Correspond to the second stage of our cell. In this stage the mature Antibodies (Mab) have failed to match with notself during activation and evolution;

Mature immunocytes set is
Mab={<b,t,ag>∈ Match/ b∈ U, θ<t<θ', ag ≠Ø} and
Match={<x,y>/x,y ∈ U, f match (x,y) = 1}.

In our work, if a Mab is not matched with notself after certain period of time then they will die. Let us note that, dead is formulate by: Abdead ={<b,t,ag >∈ Match / b,ag ∈ U, t $\wedge \leq \theta$ }

Memory Stage: Correspond to the final stage of our cell. In this stage the memory antibodies (Meb) are the results of activation and evolution of the mature antibodies. Memory immunocytes set is

Meb= {<b,t,ag>∈ Match/b∈ U,t>θ',ag=(ag1, ...agn)}
and Match= {<x,y>/x,y ∈ U, f match (x,y) = 1}.

They have significant lifespan as long as they succeed matching with not-self.

Affinity characterizes the correlation between Antigens and Antibodies is to determinate the. According to Hamming Distance (HD) this major element is evaluated.

The calculation formula is evaluated according to Hamming Distance (HD).

Let us consider xi (i=1...L) the bit string of length L and yi (i=1...L) another bit string of the same length L. xi represents Antigen and yi represents an Antibody. α is the affinity matching threshold value and HD (x,y) is the different sum of the bits in the two strings.

The affinity function is calculated as follows:

$$\begin{cases} 1, HD(x,y) \geq \alpha \\ 0, otherwise \end{cases} \quad \text{and} \quad DH(x,y) = \sum_{i}^{L} = 1^{\alpha} \quad \text{with } \alpha = 1 \text{ if xi} \neq \text{yi, } \alpha = 0 \text{ else}$$

5. RELATED WORKS

The idea of using, the artificial immune systems for intrusion detection, in distributed networks, appears recently; to our knowledge, on of the first work, was develop by Hofmeyer and Forest in 1999 [1]. Their model is implemented on distributed network architecture and in each host, a frame which is received is represented by a binary string non-self.

This string is analyzed by another binary string self of the same size L. The self represent the immune detectors which are randomly generated by the system, and which must match with not-self, in order to evolve and to change state (immature / mature & naive, or death); after the mature detector is activate and had a co stimulation it become a memory detector with an infinite lifespan. This technique is responding quickly to a possible intrusion of the same type. But the communication between the host different network is not existing.

Another architecture is proposed by Sunjun, the Immune Multi-agent Active Defense Model for Network Intrusion (IMMAD) in 2006[16]. This model is built for monitoring multilayer of

network, by a set of agents that communicate and cooperate at different levels. The immune agent (IMA) is the security state of computers monitoring, is installed in each network node, and consists of self, immature or mature antibodies, memory antibodies, etc. This immunological mechanism permits him to detect an intrusion and send the message to Local Monitor Agent (LMA). LMA analyzes the state of the local area network, and vaccinate all the nodes in the same segment, after having evaluated the risk of intrusion, and it informs Central Monitor Agent (CMA) of the new type of intrusion. CMA supervises the whole of the network and increase security across the network.

Another architecture which seem to us interesting, is proposed by NianLiu in 2009. This architecture is called Network Intrusion Detection Model Based on Immune Multi-Agent (NIDIMA)[4]. This model ensures the security in the distributed networks against intrusions. In this architecture, each agent Security situation is composed of several agents immune (IA). The IA are distributed on each node of the network, they are the firsts to identify the events of intrusion and are blocking them. If the attacks are not known through learning and memory, it sends information to the agent SMC. The agent SMC analyzes the intrusion, which it received by each AI in network segments and it surfs at network segments to vaccinate them against another intrusion. Agent security situation evaluation gathers information of subnets and host from each agent security situation, and evaluates the risks to integrated the whole network. This information includes the type, quantity, strength and harmfulness of the attacks.

There exist many other models, but we decided to present those which seem to us closest to our architecture. Let us recall that our aim is to increase immunity and to decrease the rate of false alarm.

6. ARCHITECTURE OF MODEL

In this article, we employed a new model, based on Multi-Agent paradigm and Immune algorithm for Intrusion Detection. We describe a model through the dynamic behavior of immune agents, the distinction between self and notself. We expose the architecture of the distributed model, the agents' behavior for insuring the network security, in order to avoid false alert triggering. The system is installed in each Host/Server, and the system agents cooperate and communicate for best and more reliable intrusion detection.

6.1. The behavior of immune agent in this architecture

Detector agent (D-agent) is the principal component for the distinction between self and non self through the sensor/analyzer, which identifies the frame (these agents are in immature state).

The sensor /analyzer is composed of two bit strings: a random bit string which analyses frame by calculating the Hamming Distance (HD); and a stationary bit string which includes host and network information; the stationary part is identical in all D-agents of the same host. To avoid any false alarm, D-agent sends its 1st report (if HDint > Val) to Alert agent (A-agent) when it detects an anomaly.

A-agent will evaluate the intrusion importance according to the results obtained. However, it can not trigger the alarm, while it has not received any confirmation from several D-agents, within the same host or from other A-agent within the network [13]. (See Figure1).

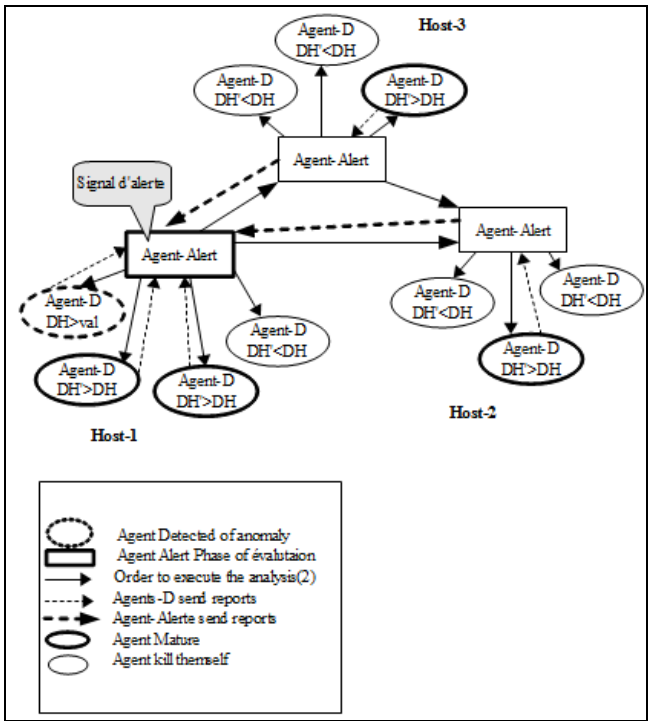

Figure1. Immune Agents Cooperation

Intrusion assessment allows to the A-agent to ignore warning message when the evaluation is tiny; or to be under-monitoring where the evaluation is important.

In this case, the A-agent sends to all D-agents the order to execute the analysis stage (2) for all treated frames.

When D-agent receives this order, a semi-sensor is generated at random, on the basis of the code of D-agent which has detected the anomaly. Thus all frames will be first analyzed by the sensor/analyzer, then by the semi-sensor in each analysis, a new Hamming distance (HD') is evaluated (mature state).

The D-agents which detect (HD'>HDint), send their reports to their A-agents and increase lifespan (Memory Phase), the other D-agents decrease their lifespan and when they reached a threshold they kill themselves. D-agents exchange between them the second analysis results, they trigger also the alert if the risk assessment is the same; (See Figure2).

This parallel analysis technique's allows a best management of false alarm and a better network supervision against the intrusion.

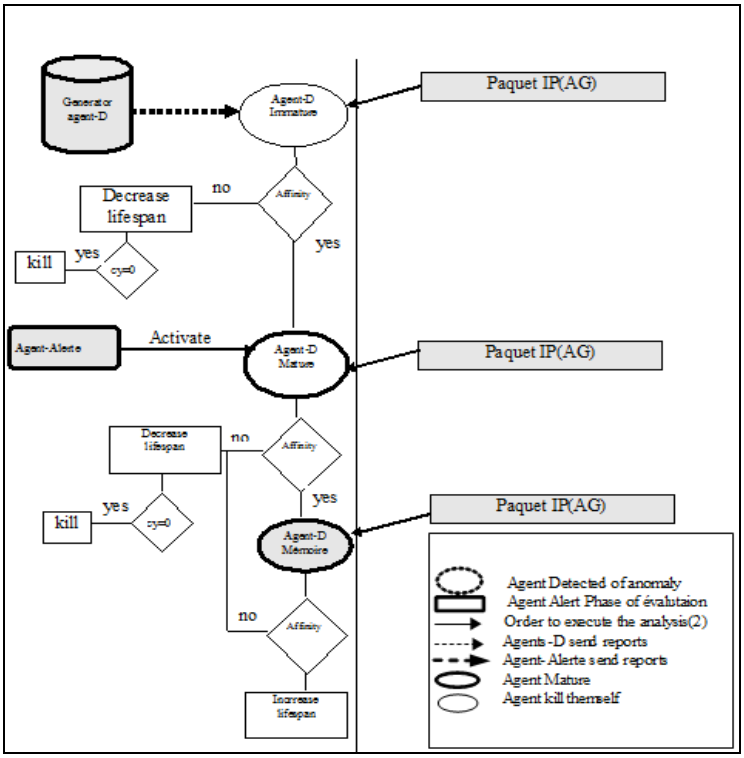

Figure 2. Dynamic evolution of Agent-D

6.2 Analysis process

Immune agents present in our model analyze the incoming IP-packet in by *D-agent* (memory) in order to detect intrusions known by the system (acquired immunity).

State Analyses by *D-agent* (memory):

- When an anomaly is detected the *D-agent* (memory) blocks the frame, and
- If not, IP-packet is transferred to a second analysis (*D-agent* (mature)).

***D-agent* (mature) State Analyses**

In this stage, *D-agent* (mature) analyses the IP-packet by the (sensor/ analyzer). Two cases could occur:

Case 1: When an anomaly is detected,

- *D-agent* sends its 1st report to *A-agent* if (HD_{int}> Val).

According to the results obtained *A-agent* will evaluate the intrusion importance. This evaluation is considered as important if the intrusion is detected by several *D-agents*, from the same host.

Intrusion assessment allows *A-agent*

- To ignore the warning message if this evaluation is insignificant or;
- To Activate all *D-agents* (mature) to execute (semi-sensor)

When *D-agent*s receive this order, they generate at random a semi-sensor on the basis of *D-agent* code (which has detected the anomaly).Thus IP-packets will be first analyzed by the sensor/analyzer, then by the semi-sensor in each analysis, and a new Hamming distance (HD') is evaluated.

The *D-agents* which will detect ($HD'>HD_{int}$),

- Send their report to their A-agents
- Block this ip-packet and increase their lifespan. When their life time reached (Tm=θ'), they become memory *D-agent*s (with Tm=Te).

The other *D-agent*s decrease their lifespan, they kill themselves when the threshold becomes null (Tm=0).

*A-agent*s exchange between them analysis results and they trigger the alert if the risk assessment is similar (see Figure3).

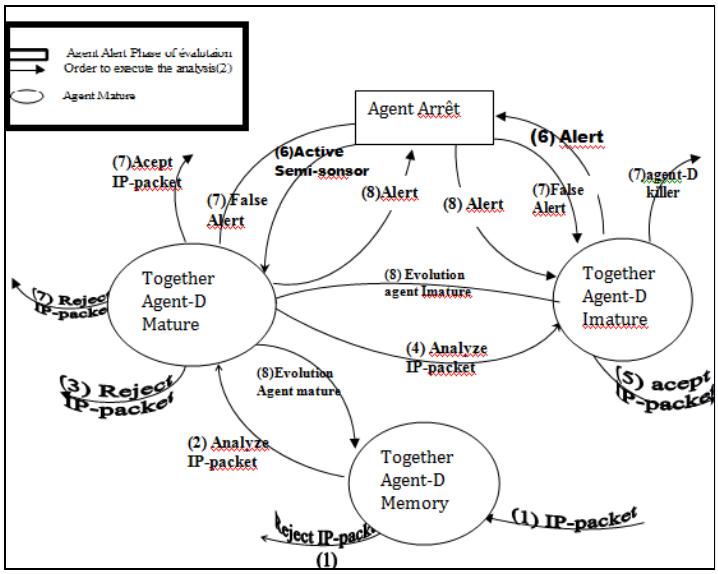

Figure 3. IP-Packet analysis Process

Case-2: if no anomaly is detected

- IP-packet is transferred to the *D-agent*s $_{(Immature)}$ (fourth analysis stage).

Immature *D-agent* State Analyses

In this state the *D-agent* $_{(Immature)}$ analysis the IP-packet,

- if no anomaly is detected , IP packet is authorized to pass,
- if an anomaly is detected by this agent, it sends alert to *A-agent*s. Thus, two cases could occur:

Case-2.1: *A-agent* rejects this alert

- Then IP-packet is authorized to pass
- The *D-agent*s $_{(Immature)}$ concerned by this alert decrease their lifespan, when they arrived at a threshold they kill themselves (see figure 2 & 3).

Case2.2: *A-agent* accepts this alert,

- *D-agents* (mature) state analysis is activated.
- If the analyses by semi-sensors detect an anomaly,
- *D-agents* (mature) send alert to their *A-agents* and Block this IP-packet furthermore they increase their lifespan.
- *A-agent* sends message to all *D-agents* (Immature) concerned by this detection
- *D-agents* (Immature) increase their lifespan; When their time-life is (Tm= θ'), they became *D-agents* (mature) with TI=Tm
- The other *D-agents* (immature, mature, memory) decrease their lifespan and when *D-agents* (Immature) lifespan arrived at a threshold they kill themselves.

- If the analyses by semi-sensor do not detect any anomaly
  - *D-agents* (mature) conclude that it is a false alarm and send message to their *A-agents*
  - *D-agents* (mature) authorize IP-packet to pass
  - *A-agent* sends message (false alert) to *D-agents* (Immature)
  - *D-agents* (Immature) decrease their lifespan and when arrived at a threshold they kill themselves

This model is based on collective decisions result of *D-agents* from the same host and *A-agent* in the networks.

7. SIMULATION EXPERIMENT

The experiment applies part of the data from KDDCUP99 in MIT LINCOLN lab, The KDD cup 1999 is a dataset used for benchmarking in order to evaluate different feature selection method for Intrusion detection system. The training set is normal network data without any attack, and test set includes normal data and attack data. The attack data is classified into 4 categories (Probing, Denial of Service (DoS), User to Root (U2R), and Remote to Local (R2L)) . In our experiment, we only used 10 percent of the raw training data (kddcup.data_10_percent) for training and the test data set for testing. For each connection, there are 41 features. The immune agents are created by Jade platform and Tool - NetBeans.We simulate the attacks of 10 simultaneous PC case study the known attacks by this model and new unknown attacks

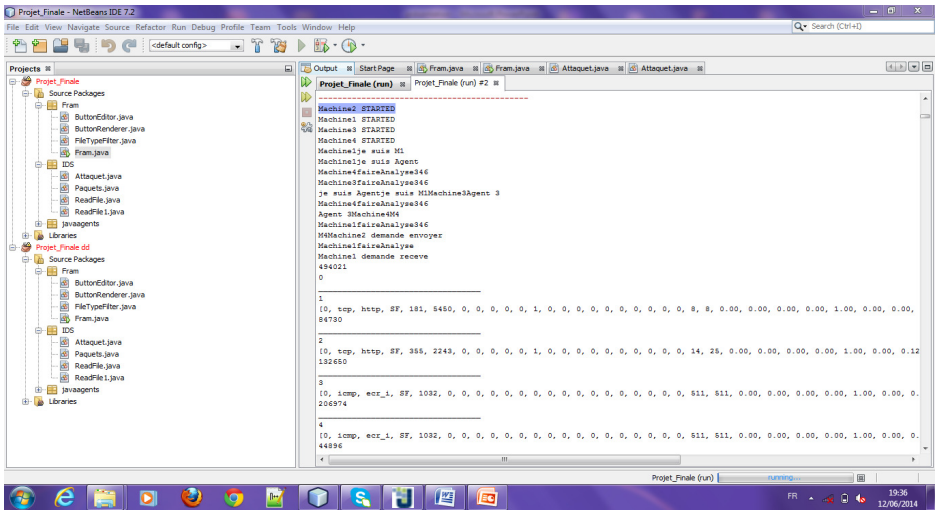

Figure4 Simulation detection of attack type

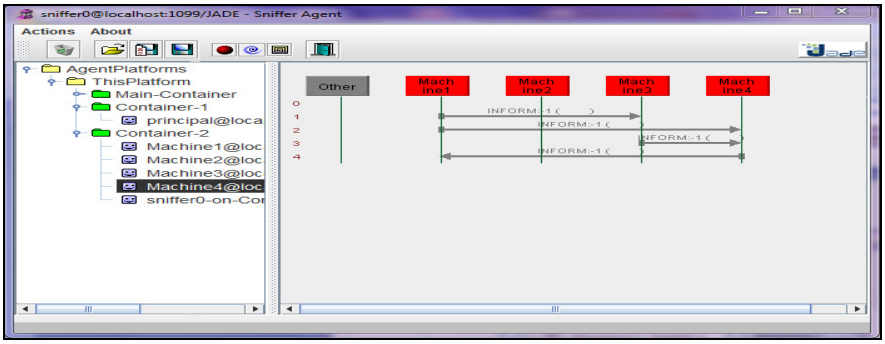

Figure 5 communication between immun-agents in jade

8. CONCLUSION

In this paper we raised problems involved in existing intrusion detection system to cope with the techniques employed by the Hackers. These techniques consist in circumventing the measurements of security by fraudulent behaviors in spread networks; consequently networks became more vulnerable to new types of attacks. A good intrusion detection system must take into account complexity and increasing dynamicity of networks. We proposed a new model of artificial immune system for intrusion detection based on multi-agents systems.

This model is inspired from biological immune principles, by the cooperation of immature D-agent, mature D-agent and memory D-agent.

The D-agent structure allows him to accomplish a double analysis for all frames. This analysis technique permits accelerating the immune response and detecting the intrusion to the shared resources. Furthermore, this distributed analysis mobilized several kind of agent in order to analyze the different sort of intrusion.

Our system adapts to the growing change of the environment of the network thus, it answers favorably at problematic.

REFERENCES

[1] A.Hofmeyer& S.Forrest, Immunity by Design An Artificial Immune System, In Proceedings of 1999 GECCO Conference, 1999

[2] C.ChungMing& all:Multi-Agent Artifial Immune Systems(MAAIS)for Intrusion Detection: Abstraction from Danger Theory, KES-AMSTA2009,LNAI5559,pp.11-19,2009

[3] D.Anderson& all: Next-generation Intrusion Detection Expert System (NIDES): Software Users Manual, 1994

[4] D.Barbara & all: ADAM: Detecting Intrusions by Data Mining,Proceedings of the IEEE Workshop on Information Assurance and Security, West Point, NY, June 5–6, 2001

[5] D.E. Denning and P.G. Neumann. Requirements and model for IDES|a real-time intrusion detection expert system. Technical report, Computer Science Laboratory, SRI International, Menlo Park, CA (USA), 1985.

[6] F.Majorczyk& all: Experiments on COTS Diversity as an Intrusion Detection and Tolerance Mechanism. Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS). March 2007.

[7] D. Wang, T. Li, S. J. Liu, G. Liang and K. Zhao. An Immune Multi-agent System for Network Intrusion Detection. In Proceedings of the 3rd International Symposium, ISICA 2008, Wuhan

(China), 19-21 December, 2008. Springer, Lecture Notes in Computer Science, Vol. 5370, Advances in Computation and Intelligence, pages 436-445, 2008.

[8] H.Arlowe.D& all.: The Mobile Intrusion Detection and Assessment System (MIDAS), in Proceedings of the Security Technology Conference, Location TBD, October 10-12, 1990, 54-61

[9] J.Hochberg& all: NADIR: An automated system for detecting network intrusions and misuse, Computers and Security 12(1993)3, May, 253 - 248

[10] J. Kim &all: Towards an artificial immune system for network intrusion detection: an investigation of clonal selection with a negative selection operator. Proc.Congress on Evolutionary Computation, South Korea, 2001, vol. 2, pp.1244-1252.

[11] J. Yang, X. Liu, T. Li, G. Liang and S. Liu. Distributed agents model for intrusion detection based on AIS. Knowledge-Based Systems, Elsevier, Volume 22, Issue 2, pages 115-119, March 2009.

[12] K. Boudaoud, Z. Guessoum. A Multi-agents System for Network Security Management. In Proceedings of the 6th IFIP Conference on Intelligence in Networks (SmartNet), pages 407-418, Vienna, (Austria), 18-22 September 2000.

[13] N.Benyettou, A.Benyettou,V.Rodin An Immune Multi-Agents System used in the Intrusion Detection System in distributed Network.ICARIS 2012, 11th International Conference on Artificial Immune Systems, Poster session, page 36 (conference programme), Taormina (Italy), 28-31 August 2012.

[14] N. Liu, S. Liu, R. Li, Y. Liu. A Network Intrusion Detection Model Based on Immune Multi-Agent. International Journal of Communications, Network and System Sciences (IJCNS), Volume 2, Number 6, pages 569-574, September 2009.

[15] R.Snapp& all.: DIDS (Distributed Intrusion Detection System) - Motivation, architecture and an early prototype, Proc. of the 14th National Computer Security Conference, Washington, D. C., Oct. 1991, 167 – 176.

[16] S. Liu, T. Li, D. Wang, K. Zhao, X. Gong, X. Hu, C. Xu and G. Liang. Immune Multi-agent Active Defense Model for Network Intrusion. In Proceedings of the 6th International Conference, SEAL 2006, Hefei (China), 15-18 October 2006. Springer, Lecture Notes in Computer Science, Volume 4247, Simulated Evolution and Learning, pages 104-111, 2006.

[17] U. Aickelin and D. Dasgupta. Artificial Immune Systems. A book chapter in Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques, Ed. E.K. Burke and G. Kendall, Springer, Chapter 13, pages 375-399, 2005.

[18] V. Rodin, A. Benzinou, A. Guillaud, P. Ballet, F. Harrouet, J. Tisseau and J. Le Bihan. An immune oriented multi-agent system for biological image processing. Pattern Recognition, Elsevier, Volume 37, Issue 4, pages 631-645, April 2004.