ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
December 2013,
Vol. 6, No. (4):
Pgs. 383-390

The Multi-Agents Immune System for Network Intrusions Detection (MAISID)

NORIA BENYETTOU[1], ABDELKADER BENYETTOU[1], VINCENT RODIN and SOUAD YAHIA BERROUIGUET

[1]Laboratoire SIMPA, Universitedes Sciences et Technologie d'Oram,
Mohammed Boudiaf, BP 1505, Oran, Algerie
[2]European University of Brittany, UBO, EA3883, LISyC, CS 93837,
29238 Brest Cedx3, France
[3]National Institute of Telecommunications and Information Technology
and Communication, INTTIC, Senia street, elm'naouar, Oran Algéria

(Received: December 10, 2013; Accepted: December 20, 2013)

ABSTRACT

Network intrusion detection Systems are designed to protect computer networks by observing frames and notifying the operators when a possible attack happened. But with the development of network and the information exchange, networks became increasingly vulnerable faced at the new forms of threats. It is necessary to improve the performance of an intrusion detection system. Inspired by immune biological system behavior and the performances of the multi-agent systems, we present in this article a new model (MAISID) of multi-agent system immune for intrusion detection. MAISID is a system that performs frames analyses by a group of immune agents' collaboration. These agents are distributed on the network to achieve simultaneous treatments, and are auto-adaptable to the evolution of the environment and have also the property of communication and coordination in order to ensure a good detection of intrusions in a distributed network. In this approach, the MAISID model is installed in each host of the network and sub-network for an extensive monitoring and a simultaneous analysis of the frames.

Key words: Intrusion Detection System, Artificial Immune System, Multi-Agents System, Network Security.

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], National Institute of Telecommunications and Information Technology and Communication INTTIC, Senia street, elm'naouar, Oran Algéria. 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 [9]] 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.

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 (MAISID). 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).

Related Works

The idea of using artificial immune systems for intrusion detection, in distributed networks, appears recently, the first work was develop by Hofmeyer and Forest in 1999[1].

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 network, by a set of agents that communicate and cooperate at different levels. One more interesting architecture is proposed by NianLiu in 2009, called Network Intrusion Detection Model Based on Immune Multi-Agent (NIDIMA)[14]. This model ensures security of distributed networks against intrusions. There are many other models, but we present those close to our architecture (SMAIDI). Let us recall that our aim is to increase immunity and to decrease the false alarm rate.

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]

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

Biological immune system

Biological immune cells (IB) have membrane receivers, who allow them to recognize specifically an epitope of an antigen. The immune system is mainly founded on three elements: gene database of genes, negative selection and the clonal selection. The gene database makes it possible to generate antibodies. The negative selection makes it possible to remove the inappropriate antibodies, and the clonal selection makes it possible to keep the best antibodies to make cells memories of them. These three processes are independent; they are subjected to no central body to manage them.

The recognition of an antigen by a cell (IB) is according to the affinity between antibodies and this antigen.

The IB cells differentiate between them via their competence. This immunocompetence depends on the synthesis of a membrane receiver. IB cells which recognize antigen will proliferate while being cloned, according to clonal selection principle[10].

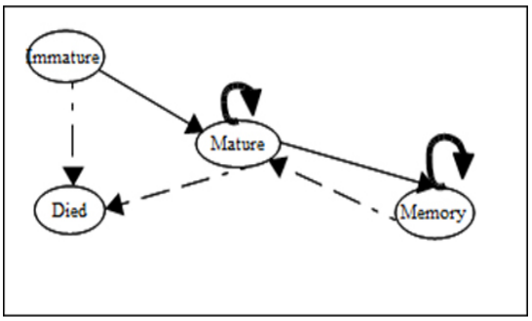

Fig. 1: immune system life cycle

Following this immunocompetence we distinguish two cases

1. IB Cells with a weak affinity will be transferred, or destroyed by negative selection.
2. IB Cells which have the capacity to recognize antigens become mature cells.

At the end of their maturation, (IB) Cells will undergo of the somatic mutations which will promote their genetic variation, then become memory cells.

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 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>Match /bU, t<¸, ag=Ø } and Match={<x,y>/x,yU, 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/ bU, ¸<t<¸', 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 }

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/bU,t>¸',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 x_i (i=1...L) the bit string of length L and y_i (i=1...L) another bit string of the same length L. x_i represents Antigen and y_i represents an Antibody. 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
and
DH(x,y)= withif x_i y_i, else

Artificial Multi-Agents Immune System

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.

Let us note, that the Detector agents (*D-agents*) are constantly in competition to defend their existence; they increase their life cycle and exchange state (immature, mature and memory) according to their intrusion detections.

MAISID Architecture

In this article, we employed a new model MAISID, 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. MAISID Architecture is illustrated in Figure2.

Table 1: IB and AI common points

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

The system is installed in each Host/ Server, and the system agents cooperate and communicate for best and more reliable intrusion detection.

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

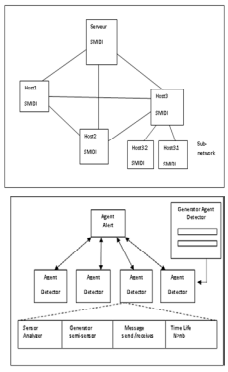

Fig. 2: MAISID Architecture

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 HD_{int} > 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 Figure3).

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.

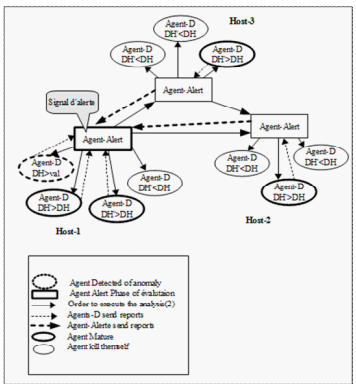

Fig. 3 : Immune Agents Cooperation

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'>HD_{int}), 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 Figure4).

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

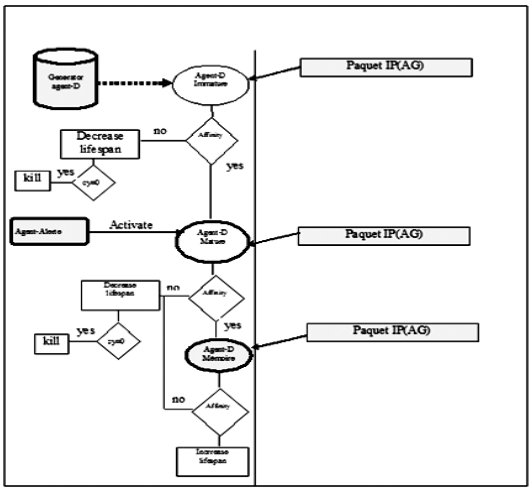

Fig. 4: Dynamic evolution of Agent-D

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* $_{(memory)}$

1. When an anomaly is detected the *D-agent* $_{(memory)}$ blocks the frame, and
2. 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,

1. *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 (see figure4).

Intrusion assessment allows *A-agent*

1. To ignore the warning message if this evaluation is insignificant or;
2. To Activate all *D-agents* $_{(mature)}$ to execute (semi-sensor) (see figure4)

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}),

1. Send their report to their A-agents
2. Block this ip-packet and increase their lifespan. When their life time reached (Tm=¸'), 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) (see Figure 4).

*A-agent*s exchange between them analysis results and they trigger the alert if the risk assessment is similar (see Figure5).

Case-2

if no anomaly is detected

1. 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,

1. if no anomaly is detected , IP packet is authorized to pass,
2. 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

1. Then IP-packet is authorized to pass
2. The *D-agent*s $_{(Immature)}$ concerned by this alert decrease their lifespan, when they arrived at a threshold they kill themselves (see figure 4 & 5).

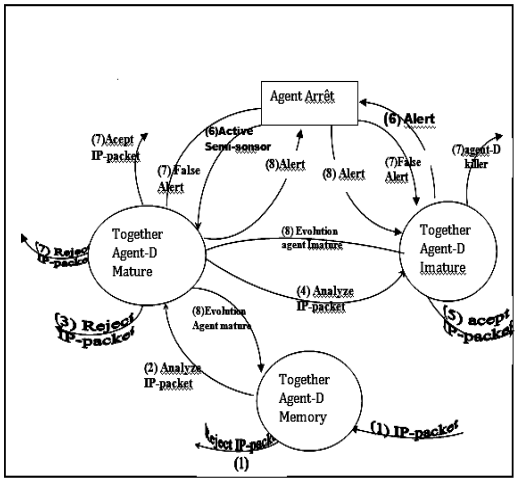

Fig. 5: IP-Packet analysis Process

Case 2.2

A-agent accepts this alert,

1. *D-agent*s $_{(mature)}$ state analysis is activated.
2. If the analyses by semi-sensors detect an anomaly,
3. *D-agent*s $_{(mature)}$ send alert to their *A-agents* and Block this IP-packet furthermore they increase their lifespan.
4. *A-agent* sends message to all *D-agent*s $_{(Immature)}$ concerned by this detection
5. *D-agent*s $_{(Immature)}$ increase their lifespan; When their time-life is (Tm= ¸'), they became *D-agent*s $_{(mature)}$ with Tl=Tm
6. The other *D-agent*s (immature, mature, memory) decrease their lifespan and when *D-agent*s $_{(Immature)}$ lifespan arrived at a threshold they kill themselves.
7. If the analyses by semi-sensor do not detect any anomaly
8. *D-agent*s $_{(mature)}$ conclude that it is a false alarm and send message to their *A-agents*
9. *D-agent*s $_{(mature)}$ authorize IP-packet to pass
10. *A-agent* sends message (false alert) to *D-agent*s $_{(Immature)}$
11. *D-agent*s $_{(Immature)}$ decrease their lifespan and when arrived at a threshold they kill themselves (see figure4).

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

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, (2001).
5. D.E. Denning and P.G. Neumann. Requirements and model for IDESla 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) (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, 54-61 (1990).
9. J.Hochberg& all: NADIR: An automated system for detecting network intrusions and misuse, Computers and Security 12(3): 253 - 248 (1993).
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, **2**: 1244-1252 (2001).
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, **22**(2): 115-119 (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), 407-418, Vienna, (Austria), (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), (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)*, **2**(6): 569-574, (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., 167 – 176 (1991).
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: 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, **37**(4): 631-645 (2004).