Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 110 (2017) 416–421

Procedia Computer Science

www.elsevier.com/locate/procedia

International Workshop on Big Data and Networks Technologies

(BDNT-2017)

Securing a Local Area Network by IDPS Open Source

Yousef FARHAOUI*

Moulay Ismail University, Faculty of sciences and Techniques,Department of Computer Science, M2I Laboratory, ASIA Team,Errachidia, Morocco.

Abstract

We present in this paper different architectures of IDPS. We will also discuss measures that define the effectiveness of IPS and finally the very recent work of standardization and homogenization of IPS. The purpose of this work is the design and the realization of an IDPS (intrusion detection and prevention system) inspired from natural immune systems. The study of biological systems to get inspired from them for the resolution of computer science problems is an axis of the artificial intelligence field which gave rise to robust and effective methods (ants colonies, genetic algorithms, neuron networks…) by their natural function, the immune system's the interest of researchers in the intrusion detection field, taking into account the similarities of NIS (Natural Immune System) and IDPS objectives.

Within the framework of this work, we conceived an IDPS inspired from natural immune system and implemented by using a directed approach. A platform was developed and tests were carried out in order to assess our system performances.

Keywords: Natural immune system; security systems; intrusion prevention system; intrusion detection system; artificial immune system; specifications.

1. Introduction

The IDPS (intrusion detection prevention system) is one of these currently most effective measures. Their role is to recognize intrusions or attempted intrusions by abnormal user behavior or recognition of attack from the network data stream. Different methods and approaches have been adopted for the design of IPS. Among these methods, one is inspired by nature, especially immune systems[1,3], which have properties and great similarity to IDPS.

* Corresponding author. Tel.: +212-67-237-7651.
E-mail address: youseffarhaoui@gmail.com

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.06.106

The study of the immune system is promising new area of research (artificial intelligence), namely, artificial immune systems (AIS)[13]. These are actually modeling, implementation and adaptation of concepts and methods of biological immune systems to solve problems. To evaluate performance, we will conduct a series of tests to analyze the results in order to measure the contribution of immune systems in the intrusion prevention [6,7].

Intrusion prevention systems and immune systems are characterized by their hierarchical architecture and their distributed operation on a set of subsystems. To better model these notions, we will adopt a method of designing an IPS.

2. Natural Immune Systems (NIS)

The most important property which is the basis of immune reactions is the ability of the NIS to distinguish between self cells and non-self cells and the ability to recognize the exact type of each foreign cell [6,7] .

This allows the NIS to increase efficiency for the recognition of antigens; this process is called affinity maturation[8,9]. This theory manages the process of creating cells. Specifically, this theory manages the creative process at the level of the discrimination between self and non-self. Lymphocytes have receptors on their surfaces lymphocytes from the bone marrow migrate to the thymus; at this stage they are called immature or naïve T cells. Their para-topes undergo a process of pseudo-random genetic rearrangement, after a very important test is introduced[10]. The recognition of an antigen by B cells, they produce specific antibodies. The antibody associate with the antigen using receptor then using cells such as T aide uses, B cells of stimulated and a proliferation process allows B cells to reproduce by creating clones themselves[11]. A second process will select among those new cells with high affinity to make memory cells[12].

3. Artificial Immune Systems (AIS)

The AIS is a new branch of artificial intelligence. Designed to solve various problems, inspired from remarkable properties and concepts of biological immune system[13]. AIS are a mathematical or computer implementation of the operation of natural immune system.

The common model known by the Framework of AIS, defines the rules to be complied by AIS and the process for developing new approaches. The necessary conditions are[14]:

Adapting procedures to monitor the evolution of the system. The three conditions mentioned above are imperative for the development of a framework to define AIS[8].

3.1. Clonal selection algorithm

This theory is based on the principle that only the cells having the antigen recognize the antigen proliferate and become memory cells. The clonal selection algorithm is based on the following:

- Holding a set of memory cells.
- Selection and cloning of the most stimulated antibodies.
- Re-selection clones proportionally to the affinity with the antigen.
- Removal of unstipulated antibodies.

The maturation of their affinity[8] (Figure 1).

```
Begin
    P = set of shapes to be recognized,  M = Population random individuals
    while (A minimal form is not recognized)
        for  i de 1 à  taille(P)
            aff = affinite($P_i$, $M_i$)
        end for
        Select  $n_1$ elements having the best affinity with the elements of M  Generate copies of these
        elements in proportion to their affinity with the antigen Mutate all copies proportionately
        with their affinity with the forms of the assembly P Add mutated individuals in the
        population M Choose $n_2$ of these mutated elements (optimized) as memory
    end while
End
```

Figure 1 . Clonal selection algorithm

3.2. Negative selection algorithm

This concept is very interesting, especially for systems monitoring applications and detection and prevention of abnormal or unusual uses[14]. The problem of protection of computer systems in the learning problem of distinguishing between self and non-self. Rather, they compare the loads detection problem within systems to the process of adverse selection takes place in the thymus[16] (Figure 2).

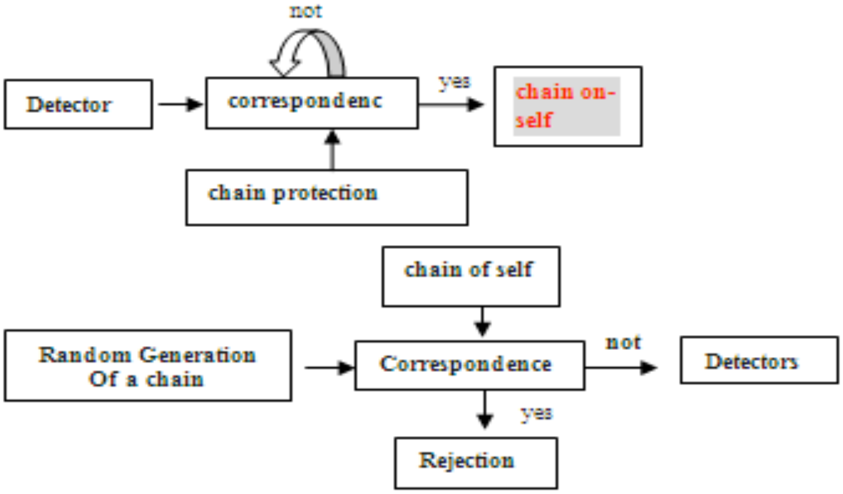

Figure 2 . The method of negative selection

Here is a summary of the negative selection algorithm (Figure 3).

```
Begin
        S = set of elements of the self.
        D = A detector array
        SeuilAff = affinity threshold
        while (i < nbDetecteurs)
            Generating a $d_i$ detector so that it has
            no affinity   with a member S
                if (affinity($d_i$ , $S_i$) > SeuilAff) Then
                       classified $S_i$ as non-self
                else if
                       classified $S_i$ as self
               end if
        end while
        return  A set of detectors D
end
```

Figure 3 . Negative selection algorithm

3.3. Immune systems intrusion detection and prevention systems (IDPS)

It is important to recall the functions or very important fundamental properties that must satisfy an IDPS and should be listed[1,2]. After that, we will try to see what is offered in parallel artificial immune systems and make the analogy between All IDPS[3,5,15:]

- Robust: The IDPS must have different points of detection and prevention, and should be highly resistant to attacks.
- Configurable: The IDPS must be easily configurable based on each machine on which it will be deployed. The degree of dependence on the operating system must be minimized.
- Expandable: Adding new hosts in all machines must be monitored elementary and the dependence on operating systems should not be an obstacle to this extension.
- Upgradable: It is necessary that the IDPS can face an unexpected increase in the flow of data to be monitored due to an extension of all the constituents' hosts the IDPS.
- Adaptable: The IDPS must dynamically adapt to changes (hardware or software) within the network in question.
- Effective: The IDPS should be simple and easy to be deployed in order to avoid affecting the hosts and network performance monitoring.
- Distributed: Special attacks can be detected and stopped after analysis of different signals and alarms from different hosts[19]. The IDPS should be able to recover various events from different stations on the network, analyze them and send responses to different stations.

In order to develop an effective IDPS we will try to find the properties mentioned above in an artificial immune system.

3.4. Properties of AIS for detection and intrusion prevention

The immune system is capable of protecting the human body surface to bacteria, viruses or any kind of antigens. This fundamental role is mainly based on discrimination between self and non-self. Whether or not known antigens, the natural immune system can be compared to an anomaly detector with a very small number of false positives and false negatives[4]. The three most important properties of an IDPS were found in the immune systems. The immune systems are[4,20].

This article talks about the negative selection algorithm. The algorithm proceeds in two phases. The first is to generate a set of sensors and the second is to use these detectors to monitor data by making a comparison. The comparison may be a comparison of the number of common bits[16,21].

3.5. Immune Systems and Immune Algorithms

Once we have found the necessary properties for our IDPS and the choice of using immune systems has been done. It is interesting to have a method for creating algorithms composed of AIS. A comparison of the components of the immune systems and their equivalents in immune algorithms, allows us to easily design the algorithms forming our artificial immune system components.

Table 1 . Comparing immune systems and immune algorithms

Immune Systems	***Immune algorithms***
Antigen	*Problem to besolved*
Antibody	*Vectorbetter solutions*
Recognitionof antigens	*Identifying the Problem*
Productionof antibodies frommemory cells	*Loadingpreviouslybestsolutions found*
Removal ofTcells	*Elimination ofsurplussolutions potential*
Proliferationof antibodies	*Use of aprocessfor creatingexact copiesof the solution*

By following this process we can develop immune algorithm. This comparison applies to the different problems, we will be interested only in the design of an IDPS inspired immune systems. The table shows a very adapted comparison:

Table 2. Comparing immune systems and IDPS

Immune Systems	***IDPS***
Thymus andbonemarrow	*PrimaryIDPS(supervisor)*
Lymphnode	*Local Host*
Antibody	*Detector*
Antigen	*Intrusion*
Self	*Normal activity*
Noself	*Abnormalactivity(suspicious)*

4. Solution Description and Global architecture of the IDPS results

We opted for the design of a hybrid IDPS composed of an NIDPS (Network Intrusion Detection and Prevention Systems) based on the approach of analysis by scenario, implementing the theory of clonal selection and using a signature database and a HIDPS (Hot Intrusion Detection and Prevention Systems) based on behavioral approach, implementing the theory of negative selection and using a user profile database. Using immune theories, the core of our IDPS generates some varied signatures of attacks and user profiles in a pseudorandom manner. This methodology allows us to develop the analyzer to possibly discover new attacks or variants of attacks.

Our IDPS is composed of:

- NIDPS: generating sensors on the basis of signatures. These detectors will be used to analyze network traffic.

- HIDPS: Based on profiles of normal user behavior in order to generate detectors able to recognize unusual behaviors of users.

- Administration Console: From this console, the administrator can configure the different parameters of the IDPS, see the different alerts, start learning control.

The components of our solution to be deployed in this way: The NIDPS will be installed on the machine that is the network proxy to analyze all network packets. While, HIDPS be deployed on all machines that constitute the LAN.

Here the overall architecture of our solution:

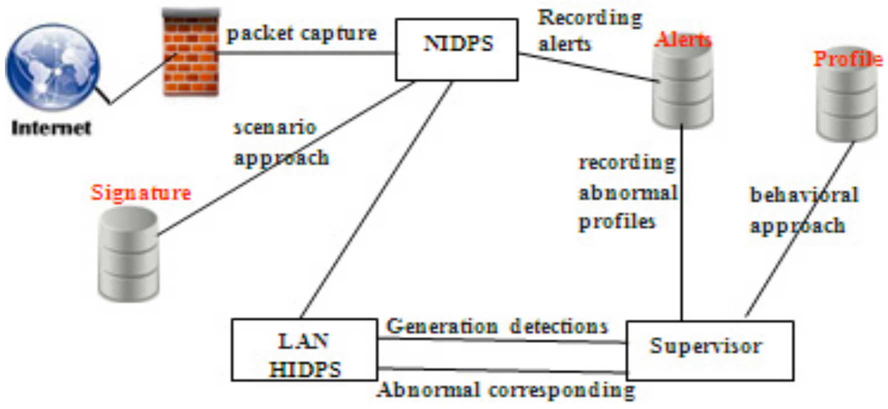

Figure 4 . Global Solution diagram

5. Conclusion

The objective of this work was to design and implement an IDPS inspired for immune systems. The IDPS is a very important brick in a security system, several research studies using different methods and approaches are devoted to them. Among them, artificial immune systems, inspired by the natural immune systems, can be very interesting for the field of intrusion detection, given the similarity of features and objectives of the latter. We focused on the two main theories that are the basis of the immune response, namely the theory of clonal selection and the theory of negative selection.

References

1. Y. Farhaoui, A. Asimi, “Performance method of assessment of the intrusion detectionand prevention systems,” IJEST , Vol. 3 No. 7 July 2011: 5916-5928.
2. Y. Farhaoui, A. Asimi, “Performance Assessment of tools of the intrusion Detectionand Prevention Systems,” IJCSIS , Vol. 10 No. 1 January 2012:7-13.
3. Y. Farhaoui, A. Asimi, «Performance Assessment of the intrusion Detection andPrevention Systems: According to their features: the method of analysis, reliability,reactivity, facility, adaptability and performance», The 6th IEEE international conferenceSciences of Electronics Technologies Information and Telecommunication (SETIT 2012),
4. Y. Farhaoui, A. Asimi, « Performance Assessment of Tools of the intrusionDetection/Prevention Systems », The 3rd IEEE International Conference on MultimediaComputing and Systems (ICMCS'12), Tangier, Morocco, 2012.
5. Y. Farhaoui, A. Asimi, “Model of an effective Intrusion Detection System on the LAN,” IJCA , Vol. 41 No. 11 March 2012:26-29
6. L. N. DE CASTRO, J. TIMMIS, In Artificial Neural Networks in Pattern Recognition Artificial Immune Systemes : A Novel Paradingm to Pattern Recognition, University of Paisley, UK, pp. 67-84, 2002.
7. Hiba KHELIL, Abdelkader BENYETTOU, Abdel BELAÏD : Application du système immunitaire artificiel pour la reconnaissance des chiffres, Maghrebian Conference on Software Engineering and Artificial Intelligence -MCSEAI'08, 2008.
8. Jason BROWNLEE,clonal Selection Theory & Clonalg selection classification algorithm, Master of Information Technology, Swinburne, University of Technology, 2004.
9. Marie-Michèle MANTHA, The truth about your immune system ; what you need to know, Harvard College, États-Unis, 2004.
10. Leandro Nunes DE CASTRO, Fernando José VON ZUBEN, the Construction of a boolean Competitive Neural Network Using Ideas From Immunology, Neurocomputing, 50C, pp. 51-85,2003.
11. Leandro Nunes DE CASTRO, Fernando José VON ZUBEN, Learning and Optimization Using the Clonal Selection Principle, Transactions on Evolutionary Computation/ Special Issue on Artificial Immune Systems, vol 6, n. 3, pp.239-251, 2002.
12. Steven A. HOFMEYR, Stephanie FORREST, Immunity by Desing ; An Artificial Immune System, Dept. of Computer Science University of New Mexico, 2004.
13. Leandro Nunes DE CASTRO, An Introduction to the Artificial Immune Systems, ICANNGA-Prague, 22-25th April, 2001.
14. L. N. DE CASTRO, J. TIMMIS,Artificial immune système as a novel soft computing paradingm, Computing laboratory, university of kent at canterbury, Soft Computing Jounal, Vol 7 July, 2003.
15. Mokhtar GHARBI, Systèmes Immunitaires Artificiels et Optimisation, Centre européen de réalité virtuelle, 2006.
16. Leandro Nunes DE CASTRO, Fernando José VON ZUBEN, Artificial immune system : Part II- A survey of applications, Technical Report, DCA-RT, feb 2000.
17. Jungwon Kim , Peter J. Bentley, An Evaluation of Negative Selection in an Artificial Immune System for Network Intrusion, Department of Computer Science University College London, 2002.
18. Leandro Nunes de Castro ,Fabricio Sérgio de Paula, Paulo Licio de Geus,An Intrusion Detection system Using Ideas from the Immune system, 2004.
19. Jungwon Kim , Peter J. Bentley, Uwe Aickelin, Julie Greensmith, Gianni Tedesco,Jamie Twyeross, Immune System Approaches to Intrusion Detection, Department of Computer Science University College London, 2002.
20. Marek ZIELINSKI, Lucas VENTER, Applying similarities between immune systems and mobile agent systemes in intrusion detection, School of Computing, University of South Africa, 2000.
21. Yan Qiao, An intrusion detection system based on immune mechanisms, SPIE Newsroom, 2007.
22. The UCI KDD Archive, Information and Computer Science, University of California, Irvine, 1999.