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.

Peer-review under responsibility of the Conference Program Chairs.

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
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