Design and Implementation of an Intrusion Prevention System

Yousef Farhaoui
(Corresponding author: Yousef Farhaoui)
ASIA Team, Department of Computer Science, Faculty of Sciences and Technique, Moulay Ismail University
B.P 509, Boutalamine, Errachidia, Morocco
(Email: youseffarhaoui@gmail.com)
(Received June. 03, 2016; revised and accepted Aug. 21 & Sept. 5, 2016)

Abstract

In view of the recent advances of communication and information technology along with the growing need for online networking, computer security has become a challenge to almost all the studies that have been carried out in this research axis. So far, various tools and mechanisms have been developed in order to guarantee a safety level up to the requirements of modern life. Among these, intrusion detection and prevention systems (IDPS) tend to locate activities or abnormal behaviors suspect to be detrimental to the correct operation of the system. In this respect, this work targets the design and the realization of an IDPS inspired from natural immune systems. The immune systems have aroused 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: Artificial Immune System; Intrusion Detection System; Intrusion Prevention System; Security Systems

1 Introduction

Since their appearance, computer attacks have been a real threat. With their great diversity and specificity to systems, these can have catastrophic consequences. Various measures to prevent these attacks or reduce their severity exist but there is no complete solution.

The IPS is one of these current most effective measures. Their role is to recognize intrusions or intrusion attempts by abnormal users' behaviors, or recognize attacks from the network data stream. Different methods and approaches have been adopted for the design of IPS, most significantly,the methods inspired by nature, especially the immune system [12, 13, 15], which has properties and great similarity to IPS. The study of the immune system is a promising new area of research (artificial intelligence), namely, artificial immune systems (AIS) [4, 28]. These are actually modelling implementation and adaptation of concepts and methods of the biological immune systems to solve problems. Our goal is to develop an artificial immune system for our intrusion prevention system, implementing the main immune theories. To evaluate performance, we will conduct a series of tests to analyze the results in order to measure the contribution of the immune systems in the intrusion prevention [9, 22].

2 Natural Immune Systems (NIS)

2.1 NIS Properties

The NIS is a source of inspiration for new branches of IT. With very important properties, it has become a valuable reference. Several research works have been developed on this basis. 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 [2, 9, 22]. In each contact with a new kind of antigens, the NIS categorizes it and keeps it in mind, thanks to a cell division mechanism followed by a selection process to refine and improve the response of NIS in the next contact with the same antigen. This allows the NIS to increase efficiency to the recognition of antigens; this process is called affinity maturation [3]. The different actors of NIS need to exchange messages under the form of signals. This occurs by means of two types of dialogues:the one-way dialogues by the immunological components and the continuous dialogues through an exchange of molecular signals [26].

2.2 Immune Theories

The behavior and reactions of the NIS are primarily governed by immune theories. This theory manages the pro-

cess of creating cells. In particular, it manages the creative process at the level of the discrimination between self and non-self cells. 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 that, a very important test is introduced [1, 7]. The recognition of an antigen by B cells, which produce specific antibodies. The antibody associated 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 [6]. A second process will select among those new cells with a high affinity to make memory cells [19].

3 Artificial Immune Systems

Artificial Immune Systems (AIS) is a new branch of artificial intelligence. Inspired from remarkable properties and concepts of biological immune system [4], AIS are designed to solve various problems. Theyare a mathematical or computer implementation of the operation of the natural immune system.

3.1 Modelling AIS

The common model known as the Framework of AIS defines the rules to be complied by AIS and the process to develop new approaches. The necessary conditions are [5]: The representation of the system components. Adapting procedures to monitor the evolution of the system. The two conditions mentioned above are imperative for the development of a framework to define AIS [3]. Then, the form of an antibody consists of a set of l parameters. These parameters may be represented by a point in a space of l dimensions. A first notes that in this plan, those antibodies are close to each other. Population or repertoire of N individuals is modelled as a space forms a finite volume V containing N points. An antigen is represented by the point $Ag =< Ag_1, Ag_2, ..., Ag_l >$, an antibody is also represented by a point $Ab =< Ab_1, Ab_2, ..., Ab_l >$. To measure the degree of completeness between the antigen and the antibodies, several techniques can be used. Most often the distances are used [17]:

Euclidean distance

$$D = \sqrt{\sum_{i=1}^{l} (Ab_i - Ag_i)^2}$$

Manhattan distance

$$D = \sum_{i=1}^{l} \|Ab_i - Ag_i\|$$

Hamming distance

$$D = \sum_{i=1}^{l} \delta_i \; with \left\{ \begin{array}{ll} 1 & \text{if } Ab_i \neq Ag_i \\ \delta_i = 0 & \text{if } not \end{array} \right\}$$

if D $\uparrow \Rightarrow$ Affinity $\downarrow$.

So, we notice that the antigen-antibody affinity is relative to the distance in the space between them.Once the antigens and antibodies are represented, the quantitative function of the defined Completeness degree between them, it remains only to implement the immune theories.

3.2 Immune Algorithms

The Algorithm 1 Show how immune theory work. 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 processes:

- 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 unstimulated antibodies.
- The maturation of their affinity [3].

Algorithm 1 Clonal selection algorithm

```
Begin
P = set of shapes to be recognized
M = Population random individuals
while Aminimal form is not recognized do
    for i = 1 to size of(P) do
        aff = affinite(Pi, Mi).
    end for
    Select n1 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.
    Add mutated individuals in the population M.
    Choose n2 of these mutated elements(optimized) as memory.
end while
End
```

This concept is very interesting, especially for systems monitoring applications and detection and prevention of abnormal or unusual uses [5]. 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 the systems to the process of adverse selection which takes place in the thymus [25].

The algorithm 2 illustrates a summary of the negative selection algorithm.

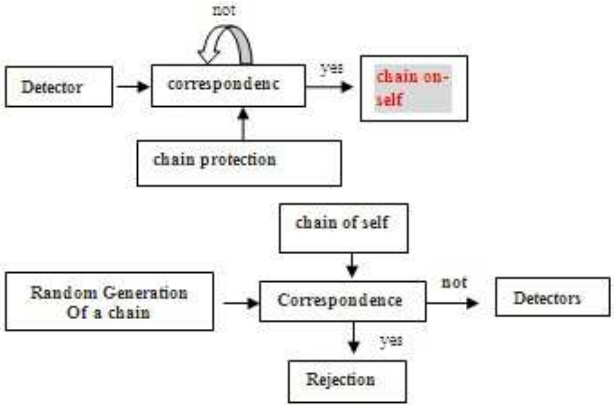

Figure 1: The method of negative selection

Algorithm 2 Negative selection algorithm

1: Begin
2: S = set of elements of the self.
3: D = a detector array.
4: SeuilAff = affinity threshold.
5: **while** i < nb Detectors **do**
6: Generating a d_i detector so that it has no affinity with a member S.
7: **if** affinity(d_i , S_i) > SeuilAff **then**
8: classified S_i as non-self.
9: **else**
10: classified S_i as self.
11: **end if**
12: **end while**
13: return a set of detectors D
14: End

3.3 Immune Systems Intrusion Detection and Prevention Systems (IDPS)

It is important to recall the functions or the fundamental properties that must satisfy an IDPS as listed in [13, 15]. We will, eventually, try to see what is offered in the parallel artificial immune systems and make the analogy between all IDPS [10, 12, 14]:

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 elementary monitored 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 the analysis of different signals and alarms from different hosts [24]. 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.

Table 1: Comparing immune systems and immune algorithms

Immune Systems	Immune algorithms
Antigen	Problem to besolved
Antibody	Vector better solutions
Recognition of antigens	Identifying the Problem
Production of antibodies from memory cells	Loading previously best solutions found
Removal of T cells	Elimination of surplus solutions potential
Proliferation of antibodies	Use of aprocessfor creating exact copies of the solution

The immune system is capable of protecting the human body surface from bacteria, viruses or any kind of antigens. This fundamental role is mainly based on the discrimination between self and non-self. The three most important properties of an IDPS are found in the immune systems. The immune systems are [16, 30]. This article talks about the negative selection algorithm. As illustrated in the Figure 1 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 can be a comparison of the number of common bits [18, 25, 29]. 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. As illustrated in the Table 1 a comparison between 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.

By following this process, we can develop the 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 2 shows a very adapted comparison.

Table 2: . Comparing immune systems and IDPS

Immune Systems	IDPS
Thymus and bone marrow	Primary IDPS(supervisor)
Lymphnode	Lymphnode Local Host
Antibody	Detector
Antigen	Intrusion
SelfSelf	Normal activity
Noself	Noself Abnormal activity (suspicious)

Based on this comparison,AIS for detection and intrusion prevention are proposed. These AIS consist of a primary IDPS which acts as a supervisor and a plurality of second IDPS will be installed on each host in the network. Thefunctioning of this IDPS model is as follows: These two points are crucial in creating a detector. Once the elements constituting the detector are listed with the type of each of them, the last step will be to define the values of each detector element as follows. If the item is a continuous type, it will be represented by an interval defined by two terminals.Once the elements and their respective values have been listed, the detector will be represented by a data structure containing these elements [11, 20, 21, 23, 27]. The choice of the clonal selection theory for scenario approach has been made because in this process, this theory is used to generate and refine antibody for the detection of known antigens. We could compare The clonal selection theory, antibodies and antigens detectors known to attack signatures. To conclude, this is the most frequent use of immune theories for the design of intrusion detection systems: NIDPS with detection by scenario,theory of clonal selection HIDPS with behavioral detection and theory of negative selection.

4 Solution Description and Global Architecture of the IDPS Results

We opted for the design of a hybrid IDPS composed of an NIDPS based on the approach of analysis by scenario, implementing the theory of clonal selection and using a signature database and a HIDPS 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 then composed of:

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

HIDPS: Based on profiles of normal user's 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 and start learning control. The components of our solution to be deployed are illustrated in the Figure 2 and are described as following: The NIDPS will be installed on the machine that is the network proxy to analyze all network packets. While, HIDPS will be deployed on all machines that constitute the LAN. Here is the overall architecture of our solution.

5 Databases Used

A large amount of information is analyzed and generated by the various components of our IDPS : the user's profiles, the alerts by the various detectors or the list of attack signatures. The use of databases is very important in the architecture of our IDPS. We opted for the use of three databases.

5.1 The Database "profiles"

This database contains all information about user profiles. The data contained in the database are generated by the HIDPS during the learning phase. For security reasons, user profiles must pass through the HIDPS supervisor to ensure compliance and consistency of the data in the profile.

5.2 The Database "signatures"

This data source is very important; it is the basis of NIDPS. It includes all the known attacks using a certain format. The format of the signature is important insofar as all detectors adopt this format. Unfortunately, there is no standard model for the codification of signatures. The signature must represent a reliable, unambiguous and accurate attributes that can recognize the attack. We must remember that the signatures will be used to analyze the network traffic. It is necessary to define the set of attributes to be used from the set of existing attributes [8, 18]. We propose in this paper a particular model of signatures. Our signature model is designed to meet the requirements by an attack signature. The attack signature must unambiguously represent the attack and should only contain information that allows recognizing the attack. In our case, the signatures are coded so as to be modifiable and can model the new attacks, with new analytical methods... etc. The analysis and synthesis of various network attacks has allowed to classify these into three classes:

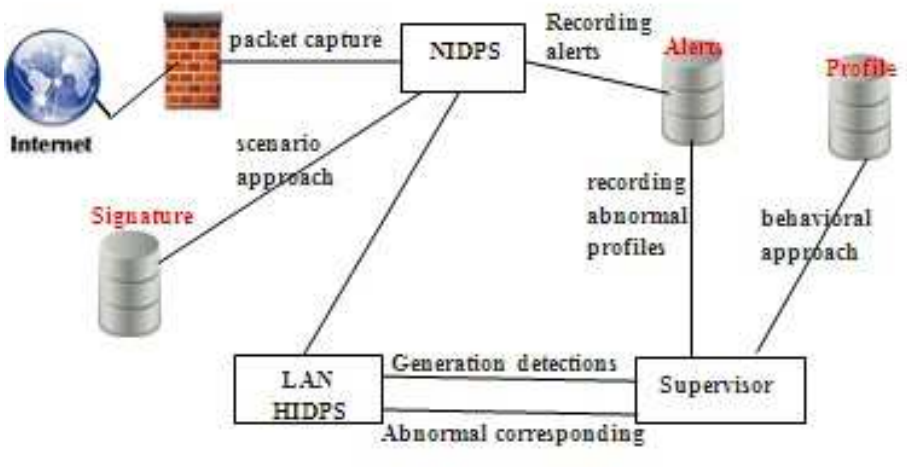

Figure 2: Global solution diagram

Attacks 'data': These are all recognized attacks by analyzing the data portion of the packet, such as SQL Injection attacks. These will be recognized if the following channels (" -, or 1 = 1) is found in the packet.

Attacks 'Headers': These are all recognized attacks by analyzing packet headers, such as DOS attacks with spoofing headers.

Attacks 'Requests/queries': The requests generally include several packages. Some attacks will be recognized by analyzing the set of packets that make up the request, such as attacks of input validation or buffer overflow attacks, which cannot be recognized, that the length or the number of parameters which constitute the request.

In the modelling of different classes of existing attacks, our Signature contains the following fields:

Id	type	Action	Data	Val	Flag

- Id: unique identifier of the signature.
- Type: header, data, queries/Request.
- Action: The Action Analysis (e.g., find a sub string, count the number of attributes, length of a query requested service... etc.)
- Data: In the case of attributes kind of strings: the desired string.
- Val: In the case of attributes to numeric values: the value of the attribute.
- Flag: Additional information.

The identifier serves as an index in the signatures database while the type allows to find the table that contains the signature. The action defines the processing to be used. This is the most important field for a signature. It contains a keyword that shows which method known for analyzing data.

5.3 The Database "Alerts"

This database will list all the alerts generated by the detectors of the two components of IDPS (NIDPS and HIDPS). Each alert should inform the administrator about suspicious event, providing enough information: time, date, sensor, signature or abnormal behavior, the attacker, the victim. This database will be accessed by the administrator to identify traces of attacks or anomalous behavior.

6 HIDPS with Behavioral Approach

The first stage of deployment HIDPS is undoubtedly the learning step, during which it traces back to normal user's behavior by creating a profile for each. User profiles are a source of data that can tell us about the behavior of the users. We chose to use the following information to model a user profile:

- Name of the user;
- Root directory;
- Average consumption CPU and RAM;
- Opening time/closing sessions.

Other information could be used, such as the average consumption of bandwidth, most visited websites, the response speed to the operating system messages.

6.1 Architecture HIDPS

Our HIDPS will consist of a HIDPS supervisor and a plurality of HIDPS slaves to be deployed throughout the network components machinery. The theory of negative selection is the HIDPS core. This theory runs in two phases: the generation of detectors and attack prevention and behavior analysis. The first phase runs on the HIDPS supervisor, which sends alarms generated at HIDPS slaves to execute the second phase of the theory. This consists of analyzing the actual behavior of the user on the basis of sensors.

6.2 HIDPS Supervisor

HIDPS the supervisor's role is to:

- Extract the users of the database profiles.
- Generate detectors and send them to HIDPS slaves by running the first phase of the theory of negative selection those generating sensors that gather all the necessary information for the analysis of user behavior in the future.
- Analyze the HIDPS of reports slaves and list alerts in a database.
- Send commands to start the learning phases, analysis, launch and stopping HIDPS slaves.

6.3 HIDPS Slaves

The main role of HIDPS slaves role is to:

- Generate user profiles during the learning phase.
- Run the second phase of the theory of negative selection, which involves using sensors generated by the first phase in order to analyze the behavior of the user.

6.4 Theory of the Negative Selection

Our HIDPS is based on this theory; it can generate alarms from the user profile and set up at the end to recognize suspicious behaviors. As we have previously seen,this theory runs in two phases:

Phase I: Generation of detectors.
This stage runs on the HIDPS supervisor. During this phase, we extract the user profiles from the database. Each profile will be considered the self system and will be used for the random generation of detectors. Then, a test is set up to purge all alarms generated by keeping only those who do not recognize the self-chain. This phase is shown in Figure 3.

Phase II: Analysis.
This phase runs on HIDPS slaves. During this phase, we operate the detectors generated by the proceeding phase to conduct the analysis of the current behavior of the user. The HIDPS slave must have sensors to inform it about the current behavior of the user. A function will measure the degree of resemblance between that conduct and the detectors previously generated,then an alert is generated if it reaches a certain percentage. This phase is shown in Figure 4.

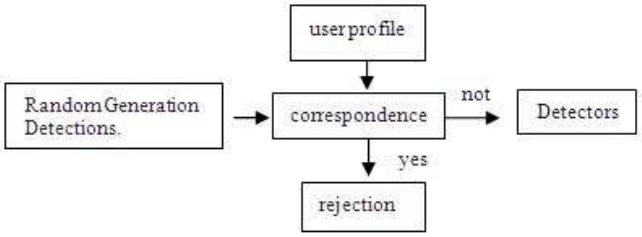

Figure 3: Phase I of negative selection (generation of detections)

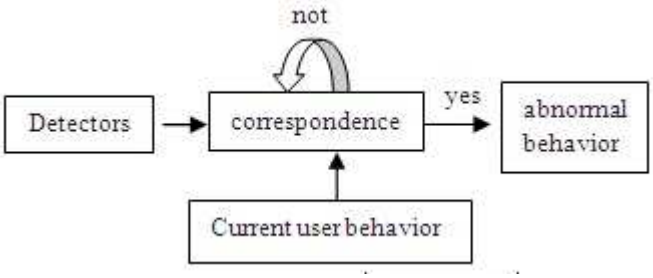

Figure 4: Phase II of negative selection

6.5 Operation HIDPS

As it is clear in the Figure 5, the HIDPS are deploying and starting in two phases:

Learning phase: The HIDPS supervisor sends the command from the beginning of the learning phase for different HIDS slaves. During the learning phase, the HIDPS slave periodically retrieves the user's behavior information.

Monitoring Phase: During this phase, the supervisor HIDPS extracts the profiles of each user, applies the first phase of the negative selection theory to generate detectors. Detectors will be sent to each slave HIDPS with the start command of the monitoring phase.

7 NIDPS with Scenario Approach

The second important component is the NIDPS using analysis with scenario approach. This approach requires a database of known attack signatures on the basis of these signatures, the core of NIDPS generates detectors, can

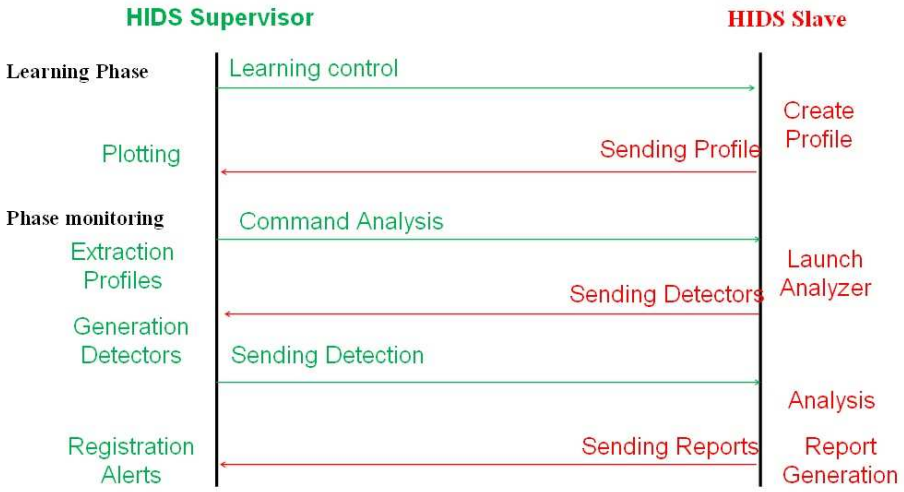

Figure 5: Mode of operation HIDPS

recognize the original signature, but also the signatures derive from the latter. The NIDPS core contains mainly the analysis function; it is based on the theory of clonal selection. The function analysis of our NIDPS contains both detectors generating process and their introduction to the packet-flow analysis.

7.1 Architecture NIDPS

7.1.1 Manager

This is the manager of the solution. The manager is responsible for:

- Starting the different components.
- Assigning different analysis tasks.
- Extracting attack signatures and generating detectors, performing clonal selection algorithm.
- Receive reports and list alerts.

7.1.2 Sensor

The sensor is responsible for capturing the network packets. Different 'sensors' can be deployed in our solution to make this task lighter. If one opts for the deployment of several 'sensors', he must define for each the subset of network traffic that will capture (eg TCP, UDP, ... etc.).

7.1.3 Analyzer

The analyzer is actually comparable to an antibody which is tasked to monitor and recognize certain types of antigens. In our case, the antigen in question is the attack signature to recognize. So the analyzer receives the signatures of the 'Manager' and puts in place to recognize a type of attack.We opt for the joint use of 'Analyzers Sensors'. This use guarantees alighter and autonomous solution.

7.2 Operation NIDPS

As illustrated in the Figure 6, our analysis uses NIDPS with the scenario approach based on the theory of clonal selection. It is used as a source of data network packets. Here are the steps for its implementation:

Packet capture: The first step of the analysis is capturing the packets through the 'sensors' that capture and transmit the network packets to 'analyzers' to conduct the analysis. At this level, one can also save the captured packets in data structures to analyze them later if the administrator opts for deferred analysis.

Extraction and formatting attributes: This step allows you to extract a high level of attribute vector from the captured packets to be analyzed later. This step is very important. It helps to prepare the packages for the analysis phase by making some changes on them.

Attribute analysis: Once the 'Manager' has generated a set of detectors by applying the theory of clonal selection, the analysis function performed by the Analyzer 'compares to the type of signature, a set of detectors with the attributes of packets. Based on this comparison,many reports are generated.

8 Conclusions

The objective of this work was to design and implement an IDPS inspired for immune systems. The IDPS is a very important brick in any security system. Several research studies using different methods and approaches have been devoted to these. Among these, the 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

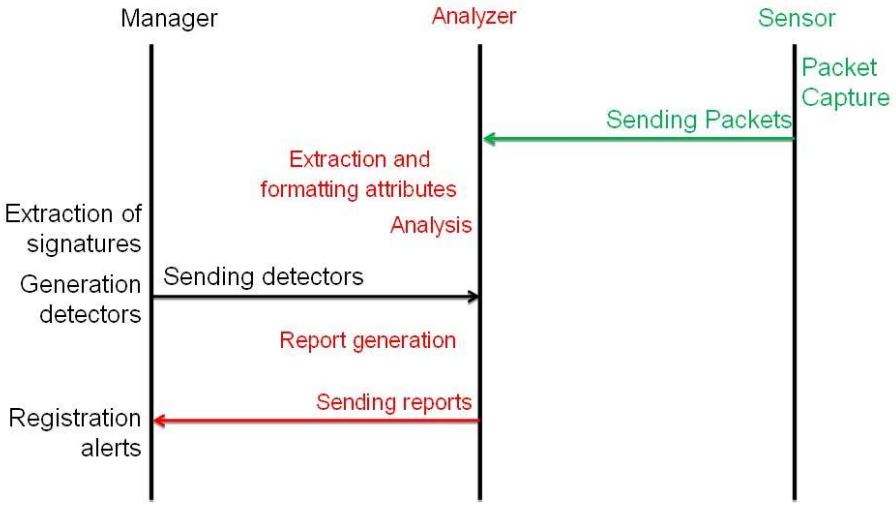

Figure 6: Mode of operation NIDS

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. The study of these two immune theories, in the case of intrusion detection,shows that the theory of clonal selection is more appropriate for the scenario analysis, while the theory of negative selection is more appropriate for behavioral analysis. The choice of implementing an IDPS is very important, especially if one considers that the IDPS will be deployed on a network with multiple machines with different hardware and software configurations. As a matter of fact, the IDPS is designed hierarchically and can be distributed across multiple machines,so it requires the analysis of data from different sources. Accordingly, we have designed a hybrid IDPS (NIDPS + HIDPS), analyzing the two sources of information and using both immune theories.

References

[1] M. Aljabr, "Using classification algorithms in building models for network intrusion detection," *International Journal on Numerical and Analytical Methods in Engineering*, vol. 3, no. 3, pp. 57–62, 2015.

[2] K. Boukhdir, A. Boualam, S. Tallaland H. Medromi, and S. Benhadou, "Conception, design and implementation of secured uav combining multi-agent systems and ubiquitous lightweight idps (intrusion detection and prevention system)," *International Journal on Engineering Applications*, vol. 3, no. 1, pp. 1–5, 2015.

[3] J. Brownlee, "Clonal selection theory & clonalg selection classification algorithm," *Master of Information Technology, Swinburne, University of Technology*, 2004.

[4] L. N. De Castro, "An introduction to the artificial immune systems," in *Handbook of Natural Computing*, pp. 1575–1597, 2012.

[5] L. N. De Castro and J. I. Timmis, "Artificial immune systems as a novel soft computing paradigm," *Soft Computing*, vol. 7, no. 8, pp. 526–544, 2003.

[6] L. N. De Castro and F. J. Von Zuben, "Learning and optimization using the clonal selection principle," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 3, pp. 239–251, 2002.

[7] L. N. De Castro, F. J. Von Zuben, and G. A. de Deus, "The construction of a boolean competitive neural network using ideas from immunology," *Neurocomputing*, vol. 50, pp. 51–85, 2003.

[8] K. D. D. Cup, *Data/the UCI KDD Archive, Information and Computer Science*, University of California, Irvine, 1999.

[9] L. N. de Castro and J. Timmis, "Artificial immune systems: A novel paradigm to pattern recognition," *Artificial Neural networks in Pattern Recognition*, vol. 1, pp. 67–84, 2002.

[10] F. S. de Paula, L. N. de Castro, and P. L. de Geus, "An intrusion detection system using ideas from the immune system," in *IEEE Congress on Evolutionary Computation (CEC'04)*, vol. 1, pp. 1059–1066, 2004.

[11] M. Enshaei, Z. M. Hanapi, and M. Othman, "A review: Mobile ad hoc networks challenges, attacks, security, vulnerability and routing protocols," *International Journal on Communications Antenna and Propagation*, vol. 4, no. 5, pp. 168–179, 2014.

[12] Y. Farhaoui and A. Asimi, "Performance assessment of the intrusion detection and prevention systems: According to their features: the method of analysis, reliability,reactivity, facility, adaptability and performance," in *The 6th IEEE International Conference on Sciences of Electronics Technologies Information and Telecommunication (SETIT'12)*, 2006.

[13] Y. Farhaoui and A. Asimi, "Performance method of assessment of the intrusion detection and prevention systems," *International Journal of Engineering Science and Technology*, vol. 3, no. 7, 2011.

[14] Y. Farhaoui and A. Asimi, "Model of an effective intrusion detection system on the LAN," *International Journal of Computer Applications*, vol. 41, no. 11, pp. 26–29, 2012.

[15] Y. Farhaoui and A. Asimi, "Performance assessment of tools of the intrusion detection/prevention systems," *International Journal of Computer Science and Information Security*, vol. 10, no. 1, pp. 7, 2012.

[16] Y. Farhaoui and A. Asimi, "Performance assessment of tools of the intrusion detection and prevention systems," in *The 3rd IEEE International Conference on MultimediaComputing and Systems (ICMCS'12)*, pp. 1–6, Morocco, Aug. 2012.

[17] M. Gharbi, "Systèmes immunitaires artificiels et optimisation," *Centre Européen de Réalité Virtuelle*, 2006.

[18] A. P Gopi, E. S. Babu, and C. N. Rajuand S. A. Kumar, "Designing an adversarial model against reactive and proactive routing protocols in manets: A comparative performance study," *International Journal of Electrical and Computer Engineering*, vol. 5, no. 5, 2015.

[19] S. A. Hofineyr and S. Forrest, "Immunity by design: An artificial immune system," in *Proceedings of Genetic and Evolutionary Computation Conference*, pp. 1289–1296, 1999.

[20] L. Jie, W. Ying, and W. F. Chen, "An improved privacy protection security protocol based on NFC," *International Journal of Network Security*, vol. 19, no. 1, pp. 39–46, Jan. 2017.

[21] G. R. Kavitha and T. S. Indumathi, "Novel roadm modelling with wss and obs to improve routing performance in optical network," *International Journal of Electrical and Computer Engineering*, vol. 6, no. 2, pp. 700, 2016.

[22] H. Khelil, A. Benyettou, and A. Belaïd, "Application du systme immunitaire artificiel pour la reconnaissance des chiffres," in *Maghrebian Conference on Software Engineering and Artificial Intelligence (MCSEAI'08)*, 2008.

[23] J. Kim and P. J. Bentley, "An evaluation of negative selection in an artificial immune system for network intrusion detection," in *Proceedings of the 3rd Annual Conference on Genetic and Evolutionary Computation*, pp. 1330–1337, 2001.

[24] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune system approaches to intrusion detection–a review," *Natural Computing*, vol. 6, no. 4, pp. 413–466, 2007.

[25] F. J. Von Zuben L. N. De Castro, "Artificial immune systems: Part i–basic theory and applications," *Universidade Estadual de Campinas, Dezembro de, Tech. Rep*, vol. 210, no. 1, 1999.

[26] M. M. Mantha, *The Truth about your Immune System: what you Need to Know*, Harvard College, États-Unis, 2004.

[27] B. Meng, C. T. Huang, Y. Yang, L. Niu, and D. Wang, "Automatic generation of security protocol implementations written in java from abstract specifications proved in the computational model," *International Journal of Network Security*, vol. 19, no. 1, pp. 138–153, 2017.

[28] T. M. Mubarak, M. Sajitha, G. A. Rao, and S. A. Sattar, "Secure and energy efficient intrusion detection in 3d wsn," *International Journal on Information Technology*, vol. 2, no. 2, pp. 48–55, 2014.

[29] Y. Qiao, *An Intrusion Detection System Based on Immune Mechanisms*, SPIE Newsroom, 2007.

[30] M. Zielinski and L. Venter, "Applying similarities between immune systems and mobile agent systems in intrusion detection," in *ISSA*, pp. 1–12. Citeseer, 2004. (`http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/016.pdf`)

Biography

Yousef Farhaoui is an professor, Department of Computer Science in Faculty of sciences and Techniques, Moulay Ismail University, Morocco. Received his PhD degree in computer security from the University Ibn Zohr. His research interest includes computer security, Data Mining, Data Warehousing, Data Fusion etc..