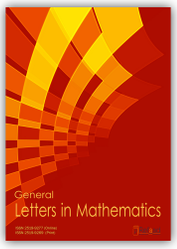
General Letters in Mathematics Vol. 2, No. 2, April 2017, pp.57-66
e-ISSN 2519-9277, p-ISSN 2519-9269
Available online at http:// www.refaad.com



A Lightweight Neural Classifier for Intrusion Detection

Azidine GUEZZAZ * [1], **Ahmed ASIMI**[2], **Younes ASIMI**[3], **Zakariae TBATOU**[4] **and Yassine SADQI**[5]

[1 2 3 4]LabSiv Laboratory. SCCAM Team. Departement of Mathematics and Computer Sciences Faculty of Sciences, Ibn Zohr University, B.P 8106, City Dakhla, Agadir, Morocco
[5]Departement of Mathmatics et Computer science Polydisciplinry Faculty, University of Sultan Moulay Slimane Mghila B.P. 592, Bni Mellal, Morocco.
[1]a.guzzaz@gmail.com, [2]asimiahmed2008@gmail.com, [3]asimi.younes@gmail.com, [4]tbatou.zakariae@gmail.com,[5] yassine.sadqi@gmail.com

Abstract. Intrusion detection and prevention is a set of techniques that try to detect attacks as they occur or after the attacks took place. There are two recent and useful approaches to detect intrusions: misuse and anomaly. They collect network traffic activities from some points on the network or computer system and then use them to secure the network using one or both of the available detection methods. The IDPS suffer major vulnerabilities with large generation of false positives and negatives. The anomaly detection aims to specify behavior detection problems that require modeling of profile preliminary. This paper describes a new approach of intrusion detection based on specified profile built from training basis using a database that contains normal activities collected within monitored network. The modeling of profile represents a real challenge for network administrators and computer security researchers. Our main goal is in the first hand, to present an application of multilayer perceptron to make a monitored system, in the second hand, to build a classifier for traffic events. A supervised algorithm is suggested and used in training. The recognition phase aims to validate the new classifier. Our classifier is able to distinct between normal activity and intrusion. We describe in details our novel detection approach and we validate the proposed solutions. We demonstrated that this novel approach is robust, flexible and gives useful performances using multilayer perceptron.

Keywords: *Security, Intrusion, false negatives, Classification, Multilayer Perceptron.*

1 Introduction and Notations

Intrusion detection products become widely available in recent years and are beginning to gain acceptance in improvement on security. The IDPS are used to take important events occurring in computer systems and analyze them to detect possible attacks. There are software and hardware tools that used to monitor and analyze events automatically [1, 6, 7, 8]. A false positive is any normal or expected behavior that is identified as malicious. It creates the problem that there are missed attacks that will not be detected. A false positive is a normal activity mistakenly identified as an attack. The performances assessment of IDPS is useful to examine their efficiency and accuracy [3, 6]. This paper presents a background of detection methods, their types and certain actual architectures. We cite an analysis of neural network, especially multilayer perceptron describing the backpropagation algorithm used in training phase. We show how these techniques can be used in the identification of attacks against a network. A

*Corresponding author.Azidine GUEZZAZ [1]a.guzzaz@gmail.com

new classifier is modeled and used to distinguish between normal activities and intrusions. In the rest of this paper, we cite various approaches of intrusion detection and describe the new model. The second section gives a state of art of automatic detection and describes the main components of classical detection system. It analyzes the back-propagation algorithm of multilayer perceptron. Our work is presented in third section; we realize the performances assessment on some actual IDPS more used in practice. We validate the proposed solutions of new approach. For the fourth section, the performances and limitations of the model are discussed. The article is achieved by a conclusion. In this paper, we use the following notations (see Table 1):

Table 1: Notations

f	: Activation Function.
$X_{i=1}^{n} = (x_{i,j})_{j=1..m}$	: The presented occurrence to input.
$W_{i=1}^{n} = (w_{i,j})_{j=1..m}$	: The model weight initialized randomly and associated to input X_i.
$w_{0,i}$	: Initialized Bias to 1 and associated to input X_i.
a_i	: Weighted sum associated to input X_i.
$y(a_i) = f(a_i)$	: Calculated output associated to input X_i.
ϵ_i	: Calculated error associated to an entry X_i.
$W_i^{op} = (w_{i,j}^{(op)})_{j=1..m}$	: Optimal system solution (Training Algorithm) for X_i.
$W_{0,i}^{op}$	: Optimal System Bias (Training Algorithm) for X_i.
IDS	: Intrusion Detection System.
IPS	: Intrusion Prevention System.
IDPS	: Intrusion Detection and Prevention System.
HIDPS	: Host Intrusion Detection and Prevention System.
NIDPS	: Network Intrusion Detection and Prevention System.

2 Background

2.1 Intrusion Detection

Current intrusion detection systems go beyond the detection of attacks and provide reaction mechanisms to cope with detected attacks or at least reduce their effect. The system of information represents an essential element of the company which is important to be protected. So, the computer security consists to assure that the material or software resources of an organization are used effectively. The computer security is generally based on following main objectives [6]:

- *Authentication:* consists in assuring that only authorized people can have access to the resources.
- *Confidentiality:* assures that only authorized people can have access to exchanged resources.
- *Integrity:* aims at ensuring that the data cannot be affected or changed.
- *Availability:* permits to maintain the good working of the system of information.

To assure the confidentiality, the integrity, the availability and the authenticity of the system, we have to follow a set of security measures: remove the not used programs, use some firewalls, use controls of access, configure the programs correctly, use the antivirus and some IDS, etc. The automatic detection is one of the good solutions for improving network security by integrating many kinds of security techniques. It can enforce security of the network, but there are also drawbacks existing in themselves. Intrusion prevention is a technique combining the techniques of the firewall and those of the IDS. Intrusion is a set of actions that try to violate one of security objectives. An IDPS monitors informations and detects malicious activities which try to violate security politic. The IPSs are developed

to take necessary measures to anticipate with precision a detected intrusion. They are usually considered a second generation of IDS or active IDS. There are two general methods of intrusion detection [6, 7, 8]:

- *Misuse approach* where the detection aims to identify an intrusion based on known configuration to malicious activities or signature.
- *Anomaly approach* where the detection aims to identify malice based on deviation of normal profile. It involves the comparison of a profile and others activities using a threshold. It is proposed by J.P Anderson (1980) and extended by D.E Denning (1987). It is based mainly on behavior analysis of users, services or applications.

Therefore, the task of intrusion detection systems is to monitor the usage of such systems and to detect the apparition of insecure states. They detect attempts and active misuse by legitimate users of the information systems or external parts to abuse their privileges or exploit security vulnerabilities. The very used IDPS are [2, 6]:

- *NIDPS or network IDPS* that monitor traffic within network.
- *HIDPS or Host IDPS* is implemented to control the concerned host.
- *Hybrid IDPS are the IDPS* that offer basic functions of NIDPS HIDPS.

In general, IDPS architecture is composed by the following parts (see Fig.1) [1, 2, 6]:

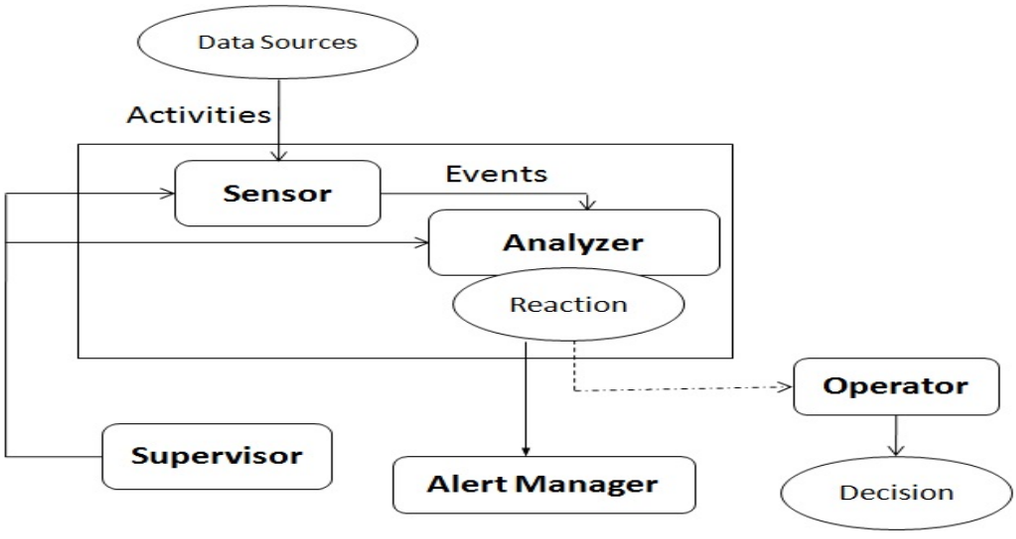


Fig. 1: General IDPS Architecture

- *Data sources* contain:
  - Data that reflect accurately what is happening on the hosts.
  - Traffic networks (a network monitor could intercept packets).
- *Activities:* are collected within data sources by a sensor and stored in database.
- *Sensor:* is a sensor that observes the system activity through data sources and provides a sequence of events that inform evolution of the system state.
- *Events:* represent the preprocessed activities presented to analyzer.
- *Analyzer:* his role is to determine if the events contain malicious activity.
- *Reaction:* is guaranteed by activating the countermeasures to end the detected attack.
- *Supervisor:* is responsible to analyze alerts and has a global vision toward system.

- *Alert Manager:* used to generate alerts after detection.
- *Operator:* it is a part of IDPS that make a final decision and reaction.

The majority of IDPS are based on signatures basis to against attacks. They compare the contents of this basis with collected activity within networks. The system can detect attacks and generate an alert. A signature is a code or serial of characters that identify malice. Each attack has a known signature. A lot of scenario detectors use scan techniques to monitor systems. The scan is lunched after demands and can be provoked regularly; it allows analyzing of many activities and verifies the presence of intrusion. During the scan technique, the detector researches attack traces. Each discovered intrusion is stored. To protect systems in realtime, the detectors use sniffing tools to monitor networks continuously in permanent activities [1, 2].

2.2 Multilayer Perceptron

The artificial neural networks have been applied to an increasing number of real world problems [9]. Their greatest advantage is in solving problems that are too complex for conventional technologies. These problems include pattern recognition and forecasting. Other advantages of neural networks is an ability to learn to do tasks based on the data given for training and self organization, they can create its own organization during learning time and realtime operation. The artificial neural networks are flexible and can perform any complex function with desired accuracy. They are typically composed of several layers of many computing elements called nodes. Each node receives an input signal from other nodes or external inputs and after processing the signals locally through a transfer function, it displays a transformed signal to other nodes or final result. Multilayer perceptron (Rosenblatt 1957) is a neural network that composed of successive feedforward layers connecting neurons by weighted links. In MLP, all nodes and layers are arranged in a feedforward structure. The first layer is called the input layer where external information is received. The last layer is called the output layer where the network produces the model solution. One or more hidden layers which are critical to artificial neural networks to identify the complex patterns in the data are appended [4, 5, 9]. An example of an MLP with one hidden layer and one output node is shown in Fig.2.

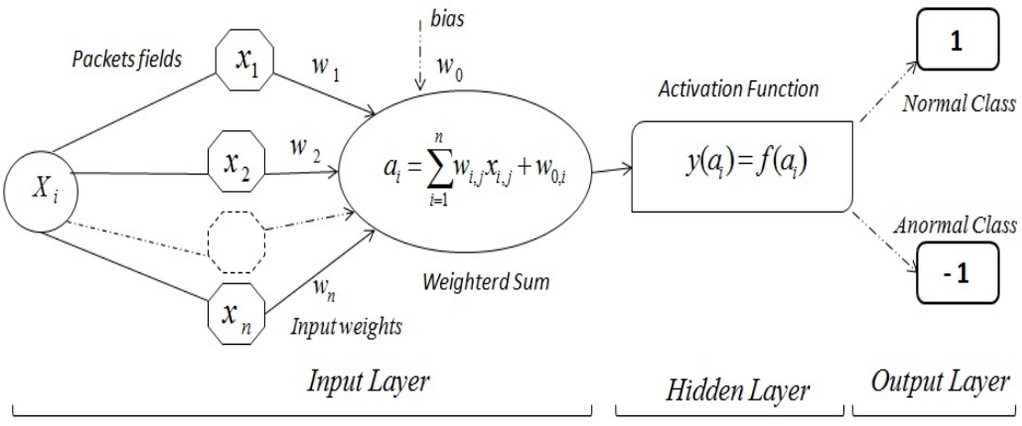


Fig. 2: Neural Multi Layer Perceptron Structure

The input layer represents a vector of values. Those values are distributed to each of the neurons in the hidden layer. In addition, there is a constant input called the bias which is multiplied by a weight and added to the sum going into the neuron. At the hidden layer, the value from each input neuron is multiplied by a weight, and the resulting weighted values are added together producing a combined value. The output corresponds to weighted sum of inputs is:

$$a_i = \sum_{i=1}^{n} w_{i,j} x_{i,j} + w_{0,i};$$

A transfer function is applied on weighted sum. The outputs from the hidden layer are distributed to the output layer. On arrival at the output layer, the value from each hidden layer neuron is multiplied by a weight, and the resulting weighted values are added together producing a combined value. The training is a developmental phase in which behavior changes until a desired behavior is achieved by adjusting weights by presenting the examples to establish new connections or modifying existing ones and comparing the calculated result with the expected output response.

Algorithm 1: Back Propagation Training

1. DBA : Training Base.
   $X_{i=1}^{n} = (x_{i,j})_{j=1\ldots m}$: Integer Inputs.
   $C_i = (c_{i,j})_{j=1\ldots m}$: Desired Results for $i = 1 \ldots n$.
   $W_{i=1}^{n} = (w_{i,j})_{j=1\ldots m}$:Weights.
   θ_i: Calculated Results for $i = 1 \ldots n$.
   λ_i:Training rate for $i = 1 \ldots n$.

2. BEGIN : Initialize the weights randomly

   For i from 1 to n do
   Calculate W_i for the input X_i
   Optimization of weigts:
   For j from 1 to $(m-1)$ do
   $w_{i,j+1} = w_{i,j} + \lambda_i(c_{i,j} - \theta_i)x_{i,j}$
   EndFor
   EndFor

3. END

The goal of the training algorithm is to find a set of weight values that will cause the output from the neural network to match the actual target values as closely as possible. There are several issues involved an multilayer perceptron such as selecting the number of hidden layers and how many neurons to use in each layer, converging to an optimal solution in a reasonable period and validating the network architecture.

3 Our work

In this section, we study some actual IDPS and evaluate their performances. Also, we describe different solutions for our new proposed model of an intrusion detection system using neural MLP.

3.1 Performances Assessments

To realize assessment performances and classify various intrusion systems, we use many parameters that are related to security objectives. The protection of data depends on the system to protect. This assessment adopts the method of the objectives of the security which is based on (see Table2):

- *Authentication:* ensures identity of a user.
- *Confidentiality :* encryption algorithm.
- *Integrity :* number of robust bits.
- *Availability :* Operation time.

Our final objective in this work is to propose an approach to improve the security level. So, we begin with testing the intrusion systems to test their availability and reliability. Related to study of computer security carried and described in [1, 3], we arrive to accomplish the classification bellow (see Table2):

This study Table2 leads to cite certain limits. The majority of IDPS suffer from a wide generation of positive false and no detection of some negative false, it influences negatively on operational functioning of these tools. Some

Table 2: Performances assessements of some IDS and IPS

	Snort	NetASQ	Suricata	Winpooch Intercept	MC Afee	Bro	Net Screen Intrusion	Cisco Net Ranger
Authenticity	High	Protocole IPSEC, Certificats X.509, PKI infrastructures, SSL	MAC algorithm	High	High	High	Medium	ACL Lists
Confidentiality	TowFish Algorithm	DES, 3DES, AES, BlowFish.	Cryptografic functions of TLS protocol	—-	—-	Include SSH functions	RC4 Algorithm	——
Integity	5MB/s, 10MB/s, 4GB/s	High speed MD5, SHA1, SHA2	Hush functions of TLS protocol	Includes scan of ClamWin antuvirus	——	high-level semantic analysis/ detect a large number of protocols	5MB/s, 100MB/s, 1GB/s	High reliability
Availability	Continuous frequency	Continuous frequency	Continuous frequency	High	Continuous frequency	Continuous frequency	Continuous frequency	Continuous frequency

packets are not treated and certain attacks are not detected during a monitoring of high traffic. A lot of modern IDPS dont integrate prevention intrusion functions and dont make ports monitoring. The IDPS cannot analyze encrypted or fragmented packets. In addition, the bad formed packets are not very treated. The IDPS are based on misuse require to put up signatures; they suffer some constraints because the development of signatures is a complex task. Also, the designers do usually errors on alert part. The signatures are developed to response new reports vulnerabilities. They must be unique to alert only in case of malicious traffic; the real constraint is that attack code can be easily changed. The IPS doesnt produce any alert when an intrusion is being really. The signature basis must to be updated at any detection. The IDPS problem is based on motif exists at level of defining and maintaining an exact state of reference to model a normal behavior which any deviation according to this state is detected like an intrusion. Another important aspect is how many data that system can analyze effectively and efficiently. It is impossible to have a perfect IDPS because of decision taken by these systems due to number of positive false that are produced when the system detects by error on anomaly and number of negative false when not wanted activity is not detected.

3.2 New Approach

Following the limits mentioned above, our research proposes a more efficient intrusion system prototype, able to overcome some of those limits. The various components of the proposed model are described in Fig.3:

3.2.1 Proposed Model

In intrusion detection approach, the final objective is to detect intrusions and then block them to prevent the attacker to achieve his or her objective. Our detection system is composed of (see Fig.3):

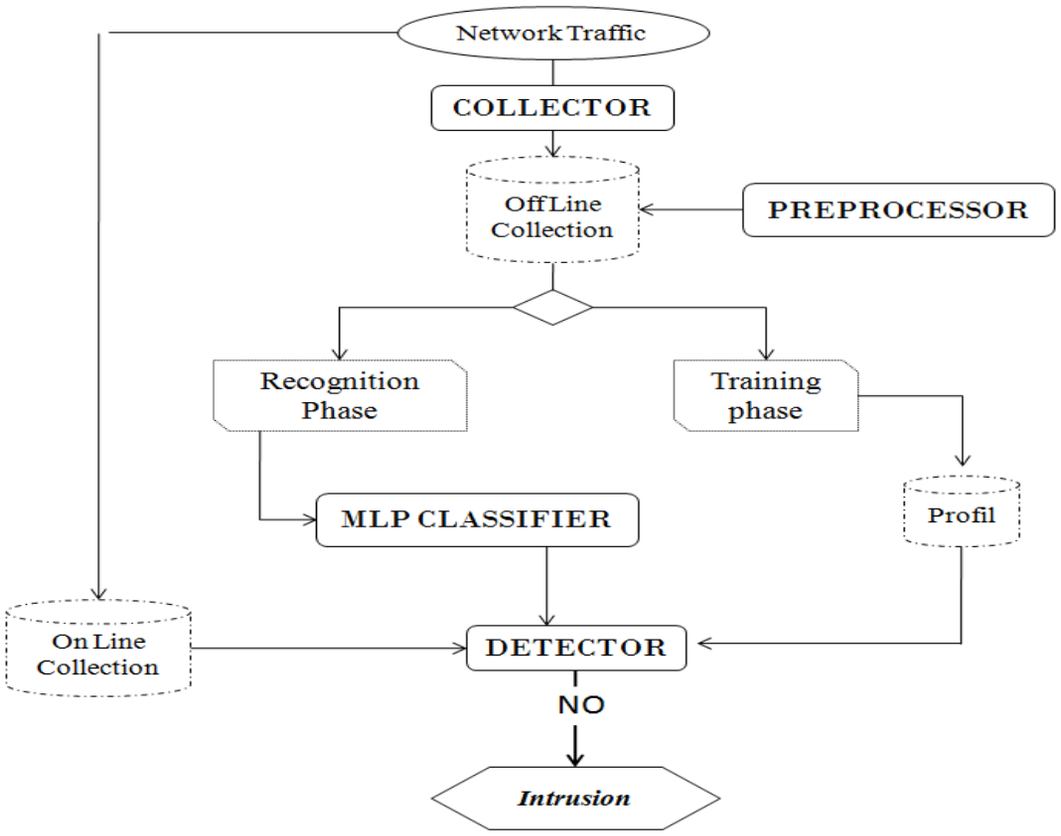


Fig. 3: Proposed Intrusion Approach Architecture

- Collector: the system has a traffic collector that collect data from a low and high network level for the both TCP and UDP connections. We developed specific software, called PcapSockS sniffer to satisfy this task [1].
- Preprocessor: a significant preprocessing of format is required before traffic analysis and classification.
- MLP Classifier: capable to categorize and classify collected events within the networks.
- Detector: used to take decision in real time.

3.2.2 Description and discussion of solutions

A particular coding for traffic is necessary to adapt activities to the model inputs which only accept integer, real or Boolean entries. The MLP has an experience by training the system to correctctly identify preselected examples of the problem. The principal advantage in using of a neural network in the intrusion detection is the flexibility that the network provides. Multilayer Perceptron is able to analyze data in real time, even if data are incomplete and no linear. The training routine requires very large amount of data to ensure that the results are statistically accurate. The new design defines a supervised method using three layer perceptron. The training basis is intercepted in a period when the monitored network is offline. A training algorithm is suggested:

Algorithm 2: Training Algorithm

For i from 1 to n do

1. Initialize weights $W_{i=1}^{n} = (w_{i,j})_{j=1\ldots m}$ randomly and $w_{0,i} = 1$ for $i = 1 \ldots n$.
2. Present the iutputs $X_i^n = (x_{i,j})_{j=1\ldots m}$.
3. Calculation of optimal W_i and ϵ_i :
   $\epsilon_i = \min\limits_{a_i}(1 - y(a_i))$

$$\left\{\begin{array}{l} a_i = \sum_{j=1}^{m} w_{i,j}x_{i,j} + w_{0,i}; \\ y(a_i) = f(a_i); \\ \text{For } j \text{ from 1 to } m \text{ do} \\ \quad w_{i,j} = w_{i,j} + [1 - y(a_i)]x_{i,j}; \\ \quad w_{0,i} = w_{0,i} + [1 - y(a_i)]; \\ \text{EndFor} \end{array}\right\}$$

4. EndFor

The optimized weights that obtained during the training phase are used in recognition phase to classify the new collected activities within monitored networks. This modeling leads us to develop a restricted database containing the occurrences (see Table3):

Table 3: Database Structure of our Scheme

$(W_i^{op})_{i=1}^{n}(w_{0,i}^{(op)})_{i=1}^{n}(\epsilon_i)_{i=1}^{n}$

Definition 3.1. *Let* $t = (t_j)_{j=1}^{m}$ *be an input occurrence and* $a_i = \sum_{j=1}^{m} w_{i,j}^{(op)} t_j + w_{0,i}^{(op)}$ *for all* $i \in \{1, \ldots, n\}$.

1. $t = (t_j)_{j=1}^{m}$ *is a normal occurrence if there exits* $i \in \{1, \ldots, n\}$ *we get* $1 - y(a_i) < \epsilon_i$.
2. $t = (t_j)_{j=1}^{m}$ *is an intrusion occurrence if for all* $i \in \{1, \ldots, n\}$ *such that* $1 - y(a_i) \geq \epsilon_i$.

To validate the new model, a recognition algorithm described below is applied:

Algorithm 3: Recognition Algorithm

1. New input $X = (x^{(j)})_{j=1..m}$, final output s .
2. Classification of activities

$$\left\{\begin{array}{l} \text{For } i \text{ from 1 to } n \text{ do} \\ a_i = \sum_{j=1}^{m} w_{i,j}^{(op)} t_j + w_{0,i}^{(op)}; \\ y(a_i) = f(a_i); \\ \quad \text{if } (1 - y(a_i) \geq \epsilon_i) \\ \quad\quad continue; \\ else \\ \quad\quad Break; \\ \quad\quad N = i; \\ \text{if}(N == n) \\ \quad\quad s = 1 // \text{ Normal activity} \\ \quad\quad else \\ \quad\quad s = -1 // \text{ Abnormal activity} \\ \quad \text{End if} \\ \quad \text{End if} \\ \text{EndFor} \end{array}\right\}$$

4 Conclusion

An IDPS monitors the activities of an environment and decides whether these activities are malicious or normal. As soon as a malicious or an intrusive event is detected, the IDPS produces an alert and sends it to the network administrator. The IPS blocks activities from the suspected malicious source. In this paper, we present a background on intrusion detection. Two major approachs are available, behavioral and misuse method. Each of those presents advantages and disadvantages. A detection system can use one of the methods or the both. We describe the importance of multilayer perceptron to solve real problems. Our work shows with performances assessment based on security objectives that more detection systems used actually suffer many limitations and vulnerabilities. So, we propose a new approach of network intrusion detection based on multilayer perceptron method aiming to minimize some limitations with bringing new solutions. We deduct that is difficult to find a perfect and standard detection system. Thus, the optimal security is obtained by combining several techniques. The future work aims to design a complete detection system by purposing an optimal architecture taking into account the control of host events to accomplish a global monitoring of networks and their systems.

References

[1] A.Guezzaz, A. Asimi, Y. Sadqi, Y. Asimi and Z.Tbatou. A New Hybrid Network Sniffer Model Based on Pcap Language and Sockets (Pcapsocks). International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016 (IJACSA).

[2] P. Asrodia and H. Patel, Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis, International Journal of Electrical, Electronics and Computer Engineering 1(1): 55-58(2012).

[3] Y. Farhaoui, A. Asimi Performance method of assessment of the intrusion detection and preventionsystems, International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462, Vol. 3 No. 7 July 2011.

[4] P. Comon, Classification supervise par rseaux multicouches, Supervised Classification by Multilayer Networks. THOMSON-SINTRA, Parc de Sophia Antipolis, BP 138, F-06561 albonne Cedex. Soumis la revue Traitement du Signal le 7/9/91 ; rvis le 17/3/92.

[5] W.Schiffmann, M.Joost, R.Werner, Optimization of the Backpropagation Algorithm for Training Multilayer Perceptrons, University of Koblenz Institute of Physics Rheinau 1 56075 Koblenz e-mail: evol@infko.uni-koblenz.de September 29, 1994 (First edition published in 1992).

[6] Y. Farhaoui, A. Asimi, Creating a Complete Model of an Intrusion Detection System effective on the LAN, International Journal of Advanced Computer Science and Applications, Vol. 3, No. 5, 2012 (IJACSA).

[7] P. Biondi, Architecture exprimentale pour la dtection dintrusions dans un systme informatique , philippe.biondi@webmotion.com, Avril-Septembre 2001.

[8] J. Balasubramaniyan, J. Garcia-Fernandez, D. Isacoff, E. Spafford, D. Zamboni, An Architecture for Intrusion Detection using Autonomous Agents, COAST Laboratory Purdue University West Lafayette, IN 47907-1398.

[9] N. Malik, Artificial neural networks and their applications, National Conference on Unearthing Technological Developments & their Transfer for Serving MassesGLA ITM, Mathura, India 17-18 April 2005. Department of Electronics and Instrumentation Engineering, Hindustan College of Science and Technology, Mathura, India.