IJIAM
International Journal of Informatics
and Applied Mathematics

International Journal of Informatics and Applied Mathematics
e-ISSN:2667-6990 Vol. 2, No. 2, 45-60

Intrusion Detection System with Grey Wolf Optimizer (GWO)

Chaima KOUIDRI, Mebarka YAHLALI, Mohammed Amine BOUDIA,
Abdelmalek AMINE, Reda Mohamed HAMOU, and Siham KOUIDRI

GeCode Laboratory,Department of Computer Science,Tahar Moulay University of
Saida, Algeria.
ckouidri2014@gmail.com

Abstract. Intrusion detection system (IDS) has started becoming a part of every system with a presence of the growing security breaches in the world. Therefore, intrusion-detection systems have the task of monitoring the usage of such systems to detect apparition of insecure states. One of the main challenges has been to build Secure application. Researchers have developed Intrusion Detection Systems (IDS) capable of detecting attacks in several available environments. In this paper, we present a Grey wolf optimizer (GWO) approach with an improved of the intrusion detection system, this approach used for classifying data and to efficiently detect various of intrusions.

Keywords: IDS · HIDS · NIDS · Attack · Behavior · Scenario.

1 Introduction

Intrusion detection systems have emerged in the computer security area because of the difficulty to ensuring that an information system will be free of security flaws [2]. Threats to networks are numerous and potentially devastating. In the other hand intrusions in an information system are the activities that violate the security policy of the system, and intrusion detection is the process used to identify intrusions. Up to the moment, researchers have developed Intrusion Detection Systems (IDS) capable of detecting attacks in several available environments [1].

In this paper, we will study the different approaches that are being followed in future work to detect network intrusions. The rest of this paper is organized as follows: Section 2 presents the basic concepts of the intrusion detection system. In section 3, we define two main methods of intrusion detection. Section 4 provides an overview of the intrusion detection system. Section 5 presents the proposed approach. Sections 6 and 7 present the results and conclusion of the experiment.

2 Intrusion Detection

The Intrusion Detection concept was created by Anderson J. in 1980. Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. The IDSs may be classified into [4]:

2.1 Network Based Intrusion Detection System (NIDS)

NIDS passively or actively listens to the network transmissions, captures and examines packets that are being transmitted. NIDS can analyze an entire packet, payload within the packet, IP addresses or ports.

2.2 Host Based Intrusion Detection System (HIDS)

HIDS is concerned with the events on the host that they are serving. They are capable of (but not limited to) detecting the following intrusions: changes to critical system files on the host, repeated failure access attempts to the host, unusual process memory allocations, unusual CPU activity or I/O activity. HIDS achieves this by either monitoring the real-time system usage of the host or by examining log files on the host.

2.3 Hybrid Intrusion Detection System

It is composed of both NIDS and HIDS components in an efficient manner by the usage of the mobile agents. Mobile agents travel to each host and perform system log file checks while a central agent checks the overall network traffic for the existence of anomalies [5].

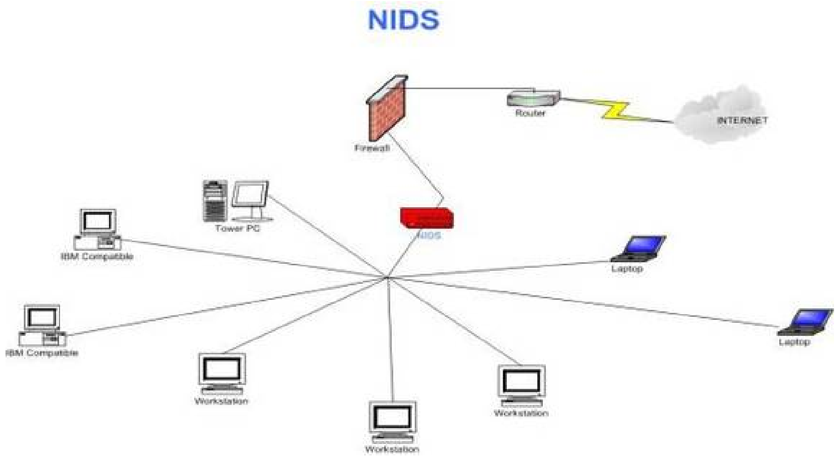


Fig. 1. Network based Intrusion Detection Systems .

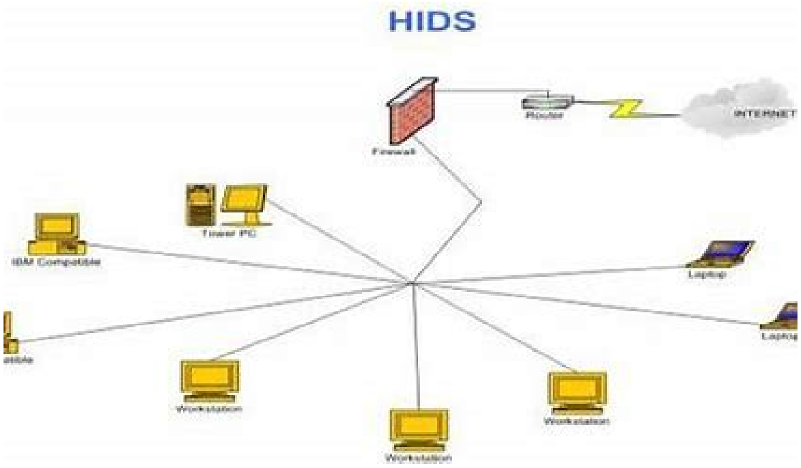


Fig. 2. Host based Intrusion Detection Systems .

3 Intrusion Detection Methods

To date two detection methods are proposed, the first is called the behavioral approach (anomaly detection) which consists of creating a model based on the normal behavior of the system and any deviation from it is considered suspect. The second is called the misuse detection (knowledge-based detection) approach, which consists of using accumulated knowledge about the attacks, then we draw scenarios of attacks and we look in the traces of audit their eventual occurrence.

3.1 The Behavior Approach

This approach was proposed by Anderson then developed by Denning and is based on the assumption that the exploitation of a system flaw requires abnormal use of the system, and therefore unusual behavior of the user. It is based on the observation of the system and any deviation from the expected normal behavior of the system is considered as intrusion. This approach consists, in a first phase, of defining a model of system behavior, users of applications, etc. which will be considered ”normal”. In a second phase, the current activity of the system is confronted with the model established in phase one by the IDS. In case a deviation is detected, an alert will be triggered. In addition, this approach considers as an intrusion, any behavior that is not previously recorded. Therefore, accuracy remains his greatest concern [6] [7].

3.2 The Scenario Approach

It aims to detect signs of known attacks according to a BDD of known attacks (knowledge accumulated on specific attacks and vulnerabilities of the system). The intrusion detection system contains information about vulnerabilities and looks for any attempt to exploit them. IDS confronts the observed behavior of the system with the database of known attacks, if this behavior matches one of the signatures in the database, an alert is triggered. In other words, any action that is not explicitly recognized as an attack is considered acceptable. Therefore, the accuracy of the intrusion detection systems based on the scenario approach is good. However, this accuracy still depends on updating knowledge about attacks that must be regular [8], [9], [10].

4 Related Work

In this section we provide the necessary background to understand the problem of intrusion detection system. We describe the methods which are being used for Intrusion Detection.

The authors in this reference [3], proposes three techniques for intrusion detection that are based on anomaly detection. The primary goal in this work is to detect novel attacks against systems, i.e., attacks that have not been seen before by the existing intrusion detection system. Their secondary goal is to reduce the false positive rate, i.e., the rate at which the system classifies normal behavior as intrusions. The proposed approach is to learn the normal behavior of programs (using different techniques) and then flag significant cant departures from normal behavior as possible intrusions. The techniques start from a simple equality matching algorithm for determining anomalous behavior, and evolve to a feed-forward back propagation neural network for learning program behavior, and finally to an Elman network for recognizing recurrent features in program execution traces.

The purpose of this survey papers [13][14] is to describe the methods/ techniques which are being used for Intrusion Detection based on Data mining concepts. The objective of this article is to study the Data Mining approaches which are being followed to detect intrusion in a network.

This paper [15] applies artificial bee colony for anomaly-based intrusion detection systems by harnessing the advantages and properties of bee's environment. It uses two feature selection techniques to reduce the amount of data used for detection and classification.

An intrusion detection model based on Deep Belief Networks is proposed to apply in intrusion recognition domain. In the first, an intrusion detection model based on the greedy multilayer DBN is presented and proved to be a feasibility of information extraction model in a large supply of unlabeled data. Then, this paper also discusses principles of DBN. Finely, the efficiency of DBN is evaluated on KDD CUP 1999 dataset [11].

The objective in this work [16] is first to take advantage of data mining techniques such as the feature selection method to eliminate data redundancy and irrelevant features in order to analyze the huge data namely the NSL-KDD. The second objective is the use of a new model of GFS which was not used in the intrusion detection area in order to solve the problem of classification and therefore to obtain a reliable IDS. The proposed model is the Genetic Programming Fuzzy Inference System for Classification (GFIS-CLASS).

The paper in [12] proposes a multiple-level hybrid classifier, a novel intrusion detection system, which combines the supervised tree classifiers and unsupervised Bayesian clustering to detect intrusions. The objective is to reduce the false alarm rate to an industrially acceptable level while maintaining the low false-negative rate. The Performance of this approach is measured using the KDDCUP99 dataset.

The Authors in [18] propose the new approach to analyze the behavior of Android applications, providing a framework to distinguish between applications that, having the same name and version, behave differently. The aim is to detect anomalously behaving applications, thus detecting malware in the form of trojan horses.

The objectif of [19] provides a comprehensive view of the human factors affecting information security in organizations were identified and classified.
describe anomaly-based intrusion detection as a specialized case of the more general behavior detection problem, By analyzing and leveraging concepts from the field of ethology and introduced a simple algorithm to build a Markov-based model of multiple classes of behavior [20].

This paper [21] describe an approach for identifying an intruder by his/her behavior on GUI based system. this system introduces logger to collect user log and BIDS detector. BIDS detector is program who create an initial user profile as well as update it if needed. BIDS program also use a t-test for identifying the user behavior deviation.

In the following table we have studied the different approaches proposed in this area. the parameters used in our studies are: algorithm used, dataset and types IDS treated, method adopted and platform.

Table 1. A comparative study of intrusion detection approaches

Ref	Authors	Paper Title	Dataset	Used Algorithms	Methods
[3]	K.Ghosh, Aaron Schwartzbard and Michael Schatz	Learning Program Behavior Profiles for Intrusion Detection	DARPA	Neural Network	Behavior approach
[11]	Ni GAO, Ling GAO, Quanli Gao,Hai Wang	An Intrusion Detection Model Based on Deep Belief Networks	KDD CUP 1999	Deep Belief Networks	scenario approach
[12]	Cheng Xiang ,Png Chin Yong, Lim Swee Meng	Design of multiple level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees	KDD CUP 1999	Bayesian clustering and decision trees	scenario approach
[13]	R. Venkatesan, R. Ganesan and A. Arul Lawrene Selvakumar	A Survey on Intrusion Detection using Data Mining Techniques	KDD 1999	Association Rule	scenario approach
[14]	Atmaja Sahasrabuddhe. Sonali Naikade, and al.	Survey on Intrusion Detection System using Data Mining Techniques	fichier XML	Nave Bayes	scenario approach

Ref	Authors	Paper Title	Dataset	Used Algorithms	Methods
[15]	Monther Aldwairi, Yaser Khamayseh and Mohammad AlMasri	Application of artificial bee colony for intrusion detection systems	KDD Cup 99	artificial bee colony	scenario approach
[16]	Mariem Belhor, Farah Jemili	Intrusion Detection Based on Genetic Fuzzy Classification System	NSL KDD	Genetic Fuzzy System	scenario approach
[17]	Surat Srinoy	Intrusion Detection Model Based On Particle Swarm Optimization and Support Vector Machine	Not defined	Particle Swarm Optimization, Support Vector Machine	Behavior approach
[18]	Iker Burguera and Urko Zurutuza, Simin Nadjm Tehrani	Crowdroid: Behavior-Based Malware Detection System for Android	Application crowdsourcing	K-means	Behavior approach
[19]	Murat OGUZ, Ihsan mr BUCAK	A Behavior Based Intrusion Detection System Using Machine Learning Algorithms	KDD	machine learning	Behavior approach
[20]	Stefano Zanero	Behavioral Intrusion Detection	Not defined	An algorithm for building Markovian models	Behavior approach

4.1 Advantages and Disavantages Comparative

Table 2. Advantages and Disavantages Comparative

Ref	Description	Advantage	Disavantage
[3]	The proposed approach is to learn the normal behavior of programs (using different techniques) and then flag significant cant departures from normal behavior as possible intrusions	The first goal in this work is to detect novel attacks against system. and reduce the false positive rate.	In the event of a profound change in the environment of the target system, triggering an uninterrupted flow of alarms (false positives)
[13,14]	this article is to study the Data Mining approaches which are being followed to detect intrusion in a network.	This paper discusses the different types of SQL injection attacks and also data mining algorithms that are used in detecting the intrusions.	the Naive Bayes Classifier algorithm assumes the independence of the variables: This is a strong assumption and is violated in the majority of real cases.
[15]	This paper applies artificial bee colony for anomaly-based intrusion detection systems.	reduce the amount of data used for detection and classification.	Experimental results show that artificial bee colony achieves average accuracy rate.
[16]	The proposed model is the Genetic Programming Fuzzy Inference System for Classification (GFIS-CLASS).	eliminate data redundancy and irrelevant features in order to analyze the huge data.	do not solve the classification problem in the intrusion detection zone.
[12]	proposes a multiple-level hybrid classifier, which combines the supervised tree classifiers and unsupervised Bayesian clustering to detect intrusions.	reduce the false alarm rate to an industrially acceptable level while maintaining the low false-negative rate.	this scheme can not be applied to other types of pattern recognition issues.
[18]	analyze the behavior of Android applications, providing a framework to distinguish between applications that, having the same name and version, behave differently.	The aim is to detect anomalously behaving applications, thus detecting malware in the form of trojan horses.	Do not handle the perceived loss of privacy when we provide behavior information to the research community.

Ref	Description	Advantage	Desavantage
[19]	provides a comprehensive view of the human factors affecting information security in organizations were identified and classified.	it study is to identify, describe and classify the human factors affecting Information Security and reduce the risk of insider misuse and assess the use and performance of the best-suited artificial intelligence techniques in detection of misuse.	It used the default settings for most of the algorithms that we tested.
[20]	describe anomaly-based intrusion detection as a specialized case of the more general behavior detection problem.	analyzing and leveraging concepts from the ?eld of ethology and introduced a simple algorithm to build a Markov-based model of multiple classes of behavior.	One problem that threatens the creation of the strong profile is the lack of sufficient training data to truly develop a strong representation of the user's behavior, this may somewhat be solved by using back propagation algorithm.
[21]	describe an approach for identifying an intruder by his/her behavior on GUI based system.	this system introduces logger to collect user log and BIDS detector.	One problem that threatens the creation of the strong profile is the lack of sufficient training data to truly develop a strong representation of the user's behavior, this may some what be solved by using back propagation algorithm.

4.2 Grey Wolf Optimizer (GWO)

Grey wolf (Canis lupus) belongs to Canidae family, is an innovative algorithm based on population that stimulates mechanism of grey wolves hunting in nature. Mirjalili et al. developed metaheuristic algorithm called Grey Wolf Optimizer (GWO).

Grey Wolves prefer to leave in groups. Their group sizes are often 5 to 12, Wolves live in four hierarchical societies: alpha, beta, delta and omega. [22]

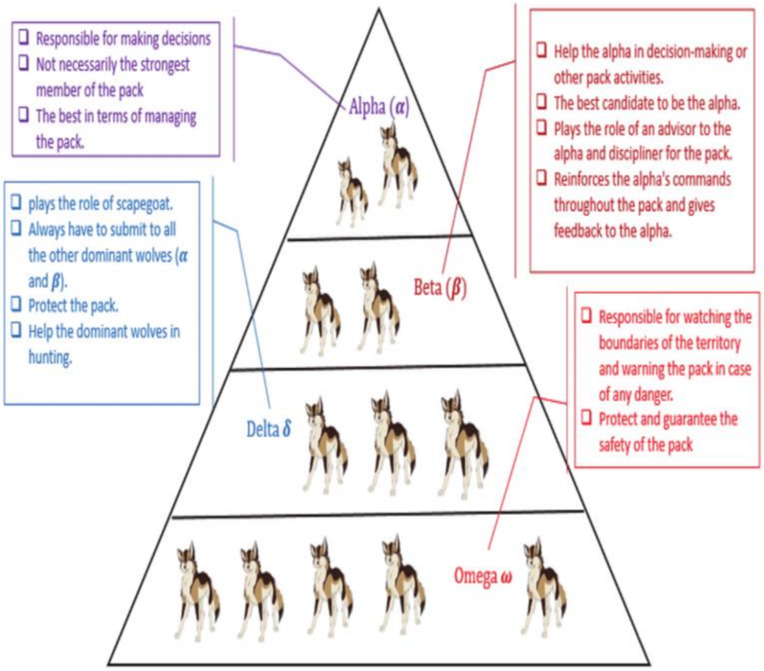

❑ Responsible for making decisions
❑ Not necessarily the strongest member of the pack
❑ The best in terms of managing the pack.
Alpha (α)
❑ Help the alpha in decision-making or other pack activities.
❑ The best candidate to be the alpha.
❑ Plays the role of an advisor to the alpha and discipliner for the pack.
❑ Reinforces the alpha's commands throughout the pack and gives feedback to the alpha.
❑ plays the role of scapegoat.
❑ Always have to submit to all the other dominant wolves (α and β).
❑ Protect the pack.
❑ Help the dominant wolves in hunting.
Beta (β)
❑ Responsible for watching the boundaries of the territory and warning the pack in case of any danger.
❑ Protect and guarantee the safety of the pack
Delta δ
Omega ω

Fig. 3. Social Hierarchy of grey wolves.

Alpha has higher dominance in pack and they are decision maker. They may be male or female. Alpha has higher dominance in pack and they are decision maker for hunting, Wakeup time, Place of sleep and so on. Other wolves are follower of alpha wolve.it is not mandatory to alpha are strongest member of pack but it has ability to manage pack properly. The dominance power decreased sequentially. . The second level in the hierarchy of grey wolves is beta. The betas are wolves that help the alpha in decision-making or other pack activities. The beta wolf can be either male or female, and he/she is probably the best candidate to be the alpha in case one of the alpha wolves passes away or becomes very old. It plays the role of an advisor to the alpha and discipliner for the pack. The beta reinforces the alphas commands throughout the pack and gives feedback to the alpha.

The omega plays the role of scapegoat. Omega wolves always have to submit to all the other dominant wolves. They are the last wolves that are allowed to eat. It may seem the omega is not an important individual in the pack. Delta wolves have to submit to alphas and betas, but they dominate the omega. Scouts, sentinels, elders, hunters, and caretakers belong to this category. Scouts are responsible for watching the boundaries of the territory and warning the pack in case of any danger. Sentinels protect and guarantee the safety of the pack.

Encircling the Prey The mathematical model of the encircling behavior is presented by the following equations:

$$\overrightarrow{X} = |\overrightarrow{A}.\overrightarrow{P}(t) - \overrightarrow{W}(t)| \tag{1}$$

$$\overrightarrow{W}(t+1) = \overrightarrow{P}(t) - \overrightarrow{B}.\overrightarrow{X}(t) \tag{2}$$

- $\overrightarrow{A}, \overrightarrow{B}$: cœfficient vectors
- $\overrightarrow{P}, \overrightarrow{W}$: position vectors of prey and wolves.

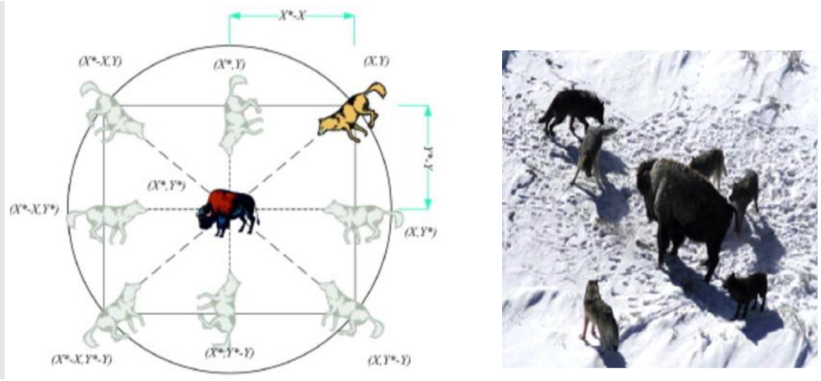


Fig. 4. position vectors and their possible next locations.

Hunting The position of alpha, beta and delta for best search is given by the following equations:

$$\overrightarrow{X}_{\alpha} = |A_1.\overrightarrow{P}_{\alpha} - \overrightarrow{W}|, \overrightarrow{X}_{\beta} = |A_2.\overrightarrow{P}_{\beta} - \overrightarrow{W}|, \overrightarrow{X}_{\delta} = |A_3.\overrightarrow{P}_{\delta} - \overrightarrow{W}| \tag{3}$$

The hunting is suggested by the alpha and beta and delta are participating in this occasion. [22]

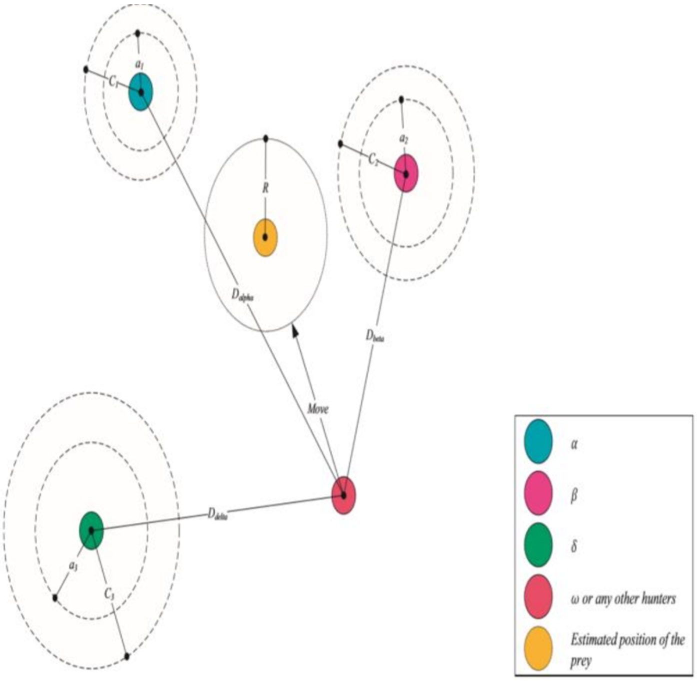


Fig. 5. position updating in GWO.[23]

Attacking Prey Hunting the prey by wolves is finished when they attack. To reach the prey in this algorithm

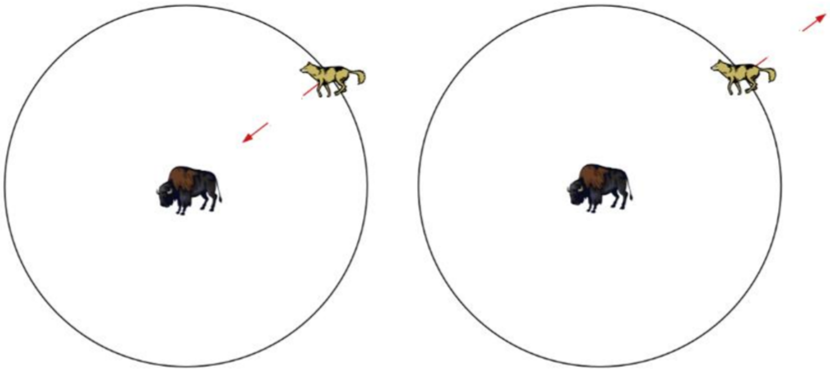


Fig. 6. Attacking prey versus searching for prey.

5 Proposed Approach

We have started the intrusion detection problem which is an NP-complet problem that has been solved with several methods among these methods they proposed meta-heuristics to save this problem. There are solutions that has been proposed by researchers such as the method of intrusion detection with bees colony and with genetic algorithms. and also techniques that allow to detect intrusions based on data maining concepts. In this paper we have proposed a solution to solve the problem of intrusion detection with gray wolves. The Gray Wolves is a new approach that was developed by researcher Seyedali Mirjalili in 2014 to solve the problems NP -complete, gray wolves based on the group concept is also inspired by the society of wolves. We have based on the data maining algorithms so the gray wolves contains a special hierarchy in each level contains a category of wolves (alpha, betta, delta, omega). each level we have placed a data maining algorithm, so the omega level we chose the KNN algorithm with distance Euclidienne that allows to carry out a classification either the user is an intruder or not intruder or suspect, and also for the delta level we go to use the KNN algorithm with a distance manhaten is realized a classification, also for betta with the algorithm KNN and the distance cheby chev, the objective of this hierarchy is to protect the alpha level and we used data set NSL KDD.

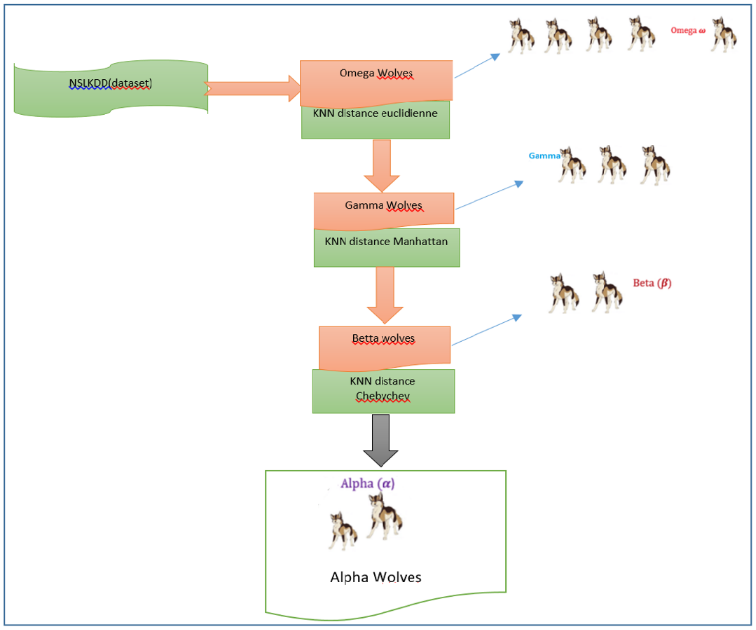
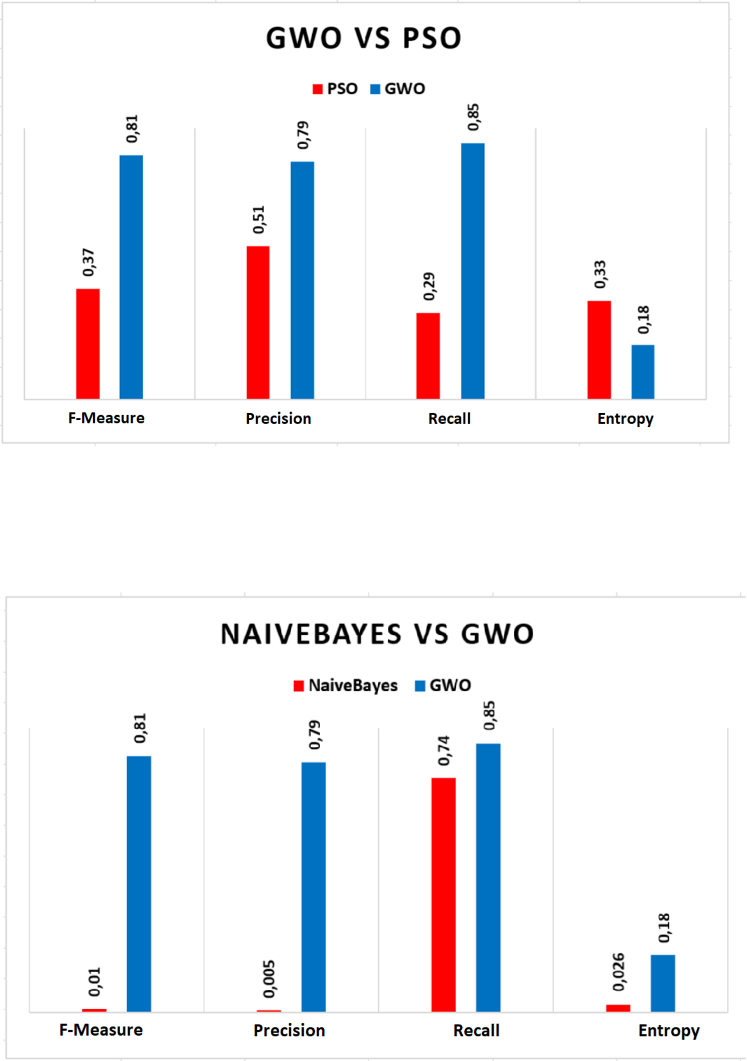


Fig. 7. Representation of the architecture of our proposition.

6 Experimentation

the goal of this experiment is to compare our solution with different approaches the result shows that our strategy is better in terms of **F-Measure**, **Precision**, **Recall**, **Entropy**

Fig. 8. Comparison of Our Results with Different Approach



7 Conclusion

The opening to the outside world makes the computer system more vulnerable to attack. It is essential to protect it, for this reason the research gate propose a solution of intrusion detection system problem.

In This paper we quoted a survey states the methods and techniques which can effectively detect a potential attack in network. We have proposed algorithm grey wolves optimizer for the problem of intrusion detection system and we noticed that our strategy gives better results.

In the future work, we plan to propose an approach based trace which takes into account the behavior of user.

References

1. Sabahi, F., & Movaghar, A.: Intrusion Detection: A Survey . The Third International Conference on Systems and Networks Communications,IEEE computer society,(2008).
2. Herv, D., Marc, D., & Andreas, W.: A revised taxonomy for intrusion detection systems. IBM Research Devision, Zurich Research Laboraty.ANN telecomunication,(2000).
3. Ghosh, K., Aaron, S., & Michael, S.: Learning Program Behavior Profiles for Intrusion Detection. Proceedings of the Workshop on Intrusion Detection and Network Monitoring,(1999).
4. Venkatesan, R., Ganesan, R. & Arul Lawrence Selvakumar, A.: A Survey on Intrusion Detection using Data Mining Techniques .International Journal of Computers and Distributed SystemsVol. No.2, Issue 1,(2012).
5. Ismail,B., Morgera, D., & Ravi, S. : A Survey of Intrusion Detection Systems in Wireless Sensor Networks. IEEE communications surveys & tutorials, vol. 16, no. 1, first quarter,(2014).
6. James P ANDERSON.: Computer security threat monitoring and surveillance. Rapp. tech. Fort Washington, Pennsylvania,(1980).
7. Dorothy,E.: An intrusion-detection mode. In :IEEE Transactions on software engineering2, 222-232,(1987).
8. Ludovic, M., & Cdric,M.: La dtection d'intrusions: bref aperu et derniers dveloppements. In: Mars (1999).
9. Herv, D., Marc, D., & Andreas, W.: A revised taxonomy for intrusion detection systems. IBM Research Devision, Zurich Research Laboraty.ANN telecomunication,(2000).
10. Jacob, Z., & Ludovic, M.: Les systmes de dtection d'intrusions: principes algorithmiques,(2002).
11. Ni, G., Ling, G., Quanli, G., & Hai, W.: An Intrusion Detection Model Based on Deep Belief Networks. Second International Conference on Advanced Cloud and Big Data,(2014).
12. Cheng, X. , Png Chin,Y. , & Lim Swee, M.: Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees , Pattern Recognition Letters 29 , 918-924,(2008).
13. Venkatesan, R. , Ganesan, R. ,& Arul Lawrene Selvakumar, A.: A Survey on Intrusion Detection using Data Mining Techniques. International Journal of Computers and Distributed Systems Vol. No.2, Issue 1, December (2012).

14. Atmaja, S., Sonali, N., Akshaya, R., & Burhan,S. ,Pravin, F.: Survey on Intrusion Detection System using Data Mining Techniques . International Research Journal of Engineering and Technology (IRJET),(2017).
15. Monther, A., Yaser, K., & Mohammad ,A.: Application of artificial bee colony for intrusion detection systems. Wiley Online Library (wileyonlinelibrary.com),(2012).
16. Mariem, B., Farah, J.: Intrusion Detection Based on Genetic Fuzzy Classification System . IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA),(2016).
17. Surat, S.: Intrusion Detection Model Based On Particle Swarm Optimization and Support Vector Machine. Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications,(2007).
18. Burguera, I., Zurutuza, U., & Nadjm, S.: Crowdroid: Behavior-Based Malware Detection System for Android. Chicago, Illinois, USA,(2011).
19. Oguz, M., Buckak, I.: A Behavior Based Intrusion Detection System Using Machine Learning Algorithms. International Journal of Artificial Intelligence and Expert Systems (IJAE), Volume (7) : Issue (2),(2016).
20. Zanero, S.: Behavioral Intrusion Detection. Via Ponzio 34/5, 20133 Milano, Italy,(2005).
21. Malek, Z., Trivedi, B.: GUI-Based User Behavior Intrusion Detection. IEEE International Conference on Power, Control, Signals and Instrumentation Engineering,(2017).
22. Vosooghifard, M;,& Ebrahimpour, H.: Applying Grey Wolf Optimizerbased decision tree c1assifer for cancer classification on gene expression data. International Conference on Computer and Knowledge Engineering (ICCKE) 2015.
23. Mirjalili, S;, & all.: GREY Wolf Optimizer. Advances in Engineering Software 69 (2014) 4661