Artificial Immune System for Intrusion Detection

Meriem Zekri – Labiba Souici-Meslati

Département d'Informatique
Université Badji Mokhtar – Annaba
BP 12, 23000 Annaba
ALGERIE

zekri@labged.net, labiba.souici@univ-annaba.org

RÉSUMÉ. L'un des défis centraux en sécurité informatique est de pouvoir déterminer la différence entre un comportement normal et un comportement potentiellement dangereux d'un système. Pendant des décennies, les développeurs ont protégé leurs systèmes en utilisant des méthodes classiques. Cependant, la croissance et la complexité des systèmes informatiques ou de réseaux à protéger nécessitent le développement d'outils de défense automatisés et adaptatifs. Des solutions prometteuses voient le jour avec l'informatique inspirée de la biologie, et en particulier, les systèmes immunitaires artificiels. Dans cet article, nous proposons deux systèmes immunitaires artificiels pour la détection d'intrusion en utilisant la base de données *KDD Cup'99*. Le premier est basé sur la théorie du danger en utilisant l'algorithme des cellules dendritiques et le second est basé sur la sélection négative. Les résultats obtenus sont prometteurs.

ABSTRACT. One of the central challenges with computer security is determining the difference between normal and potentially harmful activity. For decades, developers have protected their systems using classical methods. However, the growth and complexity of computer systems or networks to protect require the development of automated and adaptive defensives tools. Promising solutions are emerging with biological inspired computing, and in particular, artificial immune systems. In this paper, we propose two artificial immune systems for intrusion detection using the *KDD Cup'99* database. The first one is based on the danger theory using the dendritic cells algorithm and the second is based on negative selection. The obtained results are promising.

MOTS-CLÉS : Systèmes immunitaires artificiels, Détection d'intrusion, Détection d'anomalies, Théorie du danger, Algorithme des cellules dendritiques, Algorithme de la sélection négative..

KEYWORDS: Artificial immune system, Intrusion detection, Anomaly detection, Danger theory, Dentritic cell algorithm, Negative selection algorithm.

1. Introduction

The network security of computer systems is very important and motivates many researches to find solutions. Intrusion detection is one of those solutions that detect intrusion of unwanted users. The challenge is to create a system able to differentiate between normal, non offensive to the system, and harmful use. An intrusion detection system uses anomaly detection or misuse detection, our study focuses on the anomaly detection which involves discrimination between normal and abnormal data, based on normal data knowledge. In recent years, a recent bio-inspired paradigm started to prove its ability in many areas, such as pattern recognition and data mining. This paradigm corresponds to artificial immune systems (AIS) inspired by the natural immune systems [1]. There are several models based on theoretical models of the immune system. We are particularly interested by the danger theory (DT). The danger theory [2] involves two basic algorithms that are the dendritic cell algorithm (DCA) and Tolk-like Receptor (TLR). The DCA algorithm was developed to detect anomalies; therefore, it seems most appropriate for our work, besides the fact that it is an algorithm of the danger theory which greatly interested us since the beginning of our work on artificial immune systems because this theory corresponds to a relatively new concept in natural immunology [1, 3]. The aim of our work is to design two systems for intrusion classification; the first is based on the dentritic cell algorithm (DCA) while the second is based on the negative selection algorithm (NSA). We compare the performance of these two immune approaches to determine which is most appropriate for the given problem, using the KDD cup'99 dataset.

Our paper is organized as follows. In the second section we present the artificial immune systems, followed by intrusion detection systems in the third section. In the fourth and fifth section, we present the chosen artificial immune algorithms followed by a description of the dataset, experiments and results. At the end of this article, we give our conclusion and prospects for future extensions.

2. Artificial Immune Systems

Artificial immune systems represent a class of algorithms inspired by the principles and functioning of the innate immune system. These algorithms typically exploit the characteristics of the biological immune systems in terms of learning and memory as means of solving complex problems [4]. Some models mimic the abstract mechanisms of biological immune system to better understand its natural processes and simulate its dynamic behavior in the presence of antigens or pathogens while others focus on the design of algorithms, using simplification techniques (sometimes outdated) of various

immunological processes [1]. The central principle of immunology is that the immune system responds to the presence of foreign entities (called non-Self) and not responding to the host (called the Self). The study of the danger theory considers two aspects of the hazard model. The immunologists examine potential danger signals and how to are affected cells of the immune system. In collaboration with immunologists, computer scientists have sought ways to model the formation of the danger that could be used in the improvement of AIS. This is done to improve the anomalies detection systems for computers on networks. There are two developed algorithms inspired by the danger theory, the Tolk-like Receptor algorithm (Twycross 2007) and the dendritic cells algorithm (Greensmith 2006) [5].

3. Intrusion Detection Systems

In computer security, intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. A system that performs automated intrusion detection system is known as intrusion detection system (IDS). The detection method, the behavior of the detection, location of the source audit and frequency of use represent the characteristics of IDS. The detection method describes the characteristics of the analyzer, when the IDS uses information about the normal behavior of the system, it is called "behavior based" and when the IDS uses information on the attacks, it is called "knowledge based". The location of the source audit distinguishes between the IDS based on the type of input information they analyze [6]. This input information can be the audit paths, system logs or network packets. The frequency of use is an orthogonal concept, some IDS capabilities have continuous monitoring in real time, while others must be performed periodically. The first three characteristics are grouped into the functional category, because they concern the internal operation of the intrusion detection engine, namely its input information, the reasoning mechanism and its interaction with the information system. The fourth characteristic distinguishes the RTID (Real-Time Intrusion Detection) from scanners used for security evaluation.

4. The Dentritic Cell Algorithm (DCA)

The dendritic cell algorithm (DCA) is a correlation algorithm that can perform anomaly detection on classified data sets. The merger process of the signal is inspired by the interaction between dendritic cells (DCs) and their environment. The DCA has the ability to combine multiple signals to assess the current context of the environment. The correlation between the context and the antigen is used as the basis of anomaly detection in this algorithm [1]. The antigens are required; they represent the data to be

classified, but the relative proportions of the three categories of input signals which are: "PAMP", "danger" and "safe" [7]. ***PAMP*** indicates the presence of definite anomaly. ***Danger Signal (DS)*** may or may not indicate the presence of anomaly. ***Safe Signal (SS)*** indicates the presence of absolute normal. The output signals of the DCA process associated with predefined weights to produce three output signals. The three output signals are the co-stimulatory signal (CSM), the semi-mature signal (Semi) and mature signal (Mat).

Algorithm 1. Pseudo code of DCA.

Inputs: S= input signals pre-categorized + antigens. / **Outputs:** E=antigens + MCAV.

- Create an initial population of dendritic cells (DCs), D
- Randomly select 10 DCs from DC population;

For *each selected DC* **Do**
- Get the antigen;
- Store the antigen;
- Get the signals;
- Calculate interim output signals;
- Update the cumulative output signals;

If *cumulative Csm > migration threshold* **Then**
- Remove the DC population;
- Assign the cell-context to DC;

If *cumulative Semi<=cumulative Mat* **Then**
Cell context=1;
Else
Cell context=0;
End
- All DCs who collected the antigen and have a cell-context out foranalysis;
- Terminate this DC and add a naive DC to the population;

Else
- DC back to population;

End

For each incoming data **Do**
- Calculate the number of mature DC and semi-mature DC;

If *nb semi-mature DC > nb* mature *DC* **Then**
Antigen = normal;
MCAV = 0
Else
Antigen = abnormal;
MCAV = 1;
End

End

The individual sums the DC output signals resulting in cumulative Csm, cumulative Semi and cumulative Mat. This process continues until the cell reaches the end of its useful life, that is, the cumulative Csm exceeds the migration threshold; the DC ceases to sample signals and antigens. At this point, the other two cumulative signals are assessed. If the cumulative Semi is greater than the cumulative Mat value, the cell differentiates towards semi-mature state and is assigned a 'context value' of 0, and vice versa [7]. To assess the potentially anomalous nature of an antigen, a coefficient is derived from the total values of the population, called MCAV (Mature Context Antigen Value) of this antigen.

5. Negative Selection Algorithm (NSA)

The negative selection algorithm is the first artificial immune algorithm that has been proposed for intrusion detection. NSA is considered an intrusion detection process consists of three main phases; (1) the definition of self, (2) generation of detectors and (3) monitoring of occurrence of anomalies. There are two ways to implement the algorithm of negative selection: with V-detectors (variable number of detectors) and with C-detectors (constant number of detectors) [4], which have been chosen in our work.

Algorithm2. Pseudo code of NSA

Input: labeled data "normal", *l*, *r* where *l*: string length and *r* matching threshold ;

Output: detectors set ;

Begin

- Generate a set (*D*) of detectors (such that each fails to match any element in *S*);
- Monitor new sample (by continually checking the detectors in *D* against ;

If any detectors matches **Then**

-Classify as normal;

Else

-Classify as abnormal;

End

6. The dataset and the standard process

The dataset of KDD cup'99 is derived from the DARPA 98, the data set of Lincoln Laboratory for the application of data mining techniques in the field of intrusion

detection. *KDD cup'99* summarizes the two sources of data connections (data instances), each connection has 41 attributes. *KDD Cup'99* is one of the few available labeled data sets in the field of intrusion detection. Instances of data connections are labeled as normal or attacks types [8]. As intrusion detection systems by artificial immune assumes the existence of two classes, the labels of each instance of data in the original data set are replaced by either "normal" for normal connections or "abnormal" for attacks. Because of the abundance of attributes, it is necessary to reduce the size of the data set by removing the irrelevant attributes. For this, the information gain is calculated for each attribute and attributes with lowest information gain are removed from the data set [9]. After that, it appears that there are only 10 attributes whose earnings information are the highest that have been grouped into three categories of input signals. There is other input data, in addition to pre-categorized signals DCA needs, which is antigens; they are created by combining the three nominal attributes. For the NSA algorithm, only these 10 attributes are used [9].

7. Experiments and Results

Our experiments consist in the implementation of two algorithms for artificial immune systems, which are the dendritic cell algorithm (DCA) and the negative selection algorithm (NSA) with C-detectors. Both algorithms were implemented in Java in NetBeans IDE. ROC analysis (receiver operating characteristic) is performed to evaluate the performance of the classification of the DCA and the NSA. The rate of true positives (TP), false negative (FN), false positive (FP) and true negative (TN) of each experiment are calculated in addition to the detection rate (DR) and the rate of false alarms rate (FAR). We applied some variations in the implementation of two algorithms, they are described as follows:

- **Experiment 1:** DCA with a continuous data loading.
- **Experiment 2:** DCA with a random data loading.
- **Experiment 3:** NSA with a random loading of 1000 detectors with different values of *r* (2, 3, 4, 5, 6).
- **Experiment 4:** NSA with a random loading of a single detector.

We wanted to test if the order of the data could affect the proper working of the DCA. The results of the first two experiments indicate a slight decrease in detection rate when the data are randomly selected. DCA appears to have provided good performance in terms of false alarm rate, which is 0; this means that one of the objectives of the anomaly detection has been achieved because it is important that there are the least possible false alarms. We also noted that when the data set is small (1000 records for

example), the classification of the DCA is excellent and the true positive rate is relatively high (0.99 or 1.00). For the NSA algorithm, we also made a random loading of 1000 detectors and single detector, with which the correspondence took place with all of our examples. The use of more than a randomly selected detector provides better results than the use of one. Another variant of the NSA algorithm is the change in the value of r (r contiguous bits matching rule), which has greatly affected the classification.

Category		**TP**	**TN**	**FP**	**FN**	**DR**	**FAR**
Experiment 1		0.7154	1.00	0.00	0.2846	0.7154	0.00
Experiment 2		0.6521	1.00	0.00	0.3179	0.6821	0.00
Experiment 3	*r = 2*	0.9211	0.4294	0.3705	0.0799	0.9211	0.4631
	r = 3	0.7548	0.5183	0.2361	0.2452	0.7548	0.3129
	r = 4	0.3455	0.6324	0.2005	0.6545	0.3455	0.2407
	r = 5	0.2845	0.7128	0.0085	0.7155	0.2845	0.0102
	r = 6	0.0814	0.1985	0.0007	0.9186	0.0814	0.0035
Experiment 4		0.7121	0.4987	0.2147	0.2879	0.1210	0.3009

Table3. The ROC results of experiments

8. Conclusion and future work

We used two algorithms for the immune detection of anomalies in our experiments with the *KDD cup'99* data set. The results for the dendritic cell algorithm (DCA) are quite encouraging and show that we can further improve the implementation of this algorithm to obtain better results. In contrast, the negative selection algorithm (NSA), did not provide conclusive results, it emits a large number of false alarms in contrast to the DCA algorithm whose false alarm rate is around zero. We also note that NSA has difficulty in managing a large data set, which is a serious drawback, given the current size of database computer systems.

Future researches that can be applied to the DCA algorithm are to find a way to make it more adaptive and flexible. We can also try to test with different data sets and make rigorous performance comparisons with other artificial immune methods.

9. Bibliography and biography

9.1 Bibliography

[1] Aickelin U., Bentley P., Cayzer S, Kim J., McLeod J. Danger Theory: The Link between AIS and IDS?, *2nd International Conference on Artificial Immune Systems*, Edinburgh, U.K. September, 2003

[2] Aickelin U. and Greensmith J., Sensing Danger: Innate Immunology for Intrusion Detection, *Elsevier Information Security Technical Reports*, Vol. 12, No. 4, pp. 218-227, 2007.

[3] Dasgupta D., Nino L. F., *Immunological Computation, theory and application*, Auerbach, 2009

[4] Greensmith J. The Dendritic Cell Algorithm, PhD Thesis, University of Nottingham, 2007

[5] Greensmith, J., Aickelin U., DCA for SYN Scan Detection, *Genetic and Evolutionary Computation Conference (GECCO)*, pp. 49–56, 2007

[6] Greensmith J., Feyereisl J., Aickelin U. *The DCA:* SOMe Comparison A comparative study between two biologically-inspired algorithms, *Evolutionary Intelligence*, pp. 85-112, 2008

[7] Matzinger P., Tolerance, danger and the extended family, *Annual Reviews in Immunology*, Vol. 12, pp. 991–1045, 1994.

[8] Stibor T. On the Appropriateness of Negative Selection for Anomaly Detection and Network Intrusion Detection, PhD Thesis, Germany, 2006

[9] Simon M. Garrett, How do we evaluate artificial immune systems, *Evolutionary Computation*, Vol. 13, No. 2, pp. 145-178, 2005.

9.2 Biography

Meriem Zekri is currently a PhD student in the Computer Science department of Badji Mokhtar University, Annaba, Algeria. She received her Master degree in 2010 and is affiliated to LabGED laboratory. Her research interests include bio-inspired systems, data mining and bioinformatics.

Labiba Souici-Meslati is full professor in the Computer Science department of Badji Mokhtar University, Annaba, Algeria. She is affiliated to LRI laboratory. She has published several papers in international conferences and journals. Her research interests include machine learning, computational intelligence, bio-inspired systems, pattern recognition, data mining and bioinformatics.