A Novel Immune Anomaly Detection Technique Based on Negative Selection

F. Niño, D. Gómez, and R. Vejar

Department of Computer Science
National University of Colombia
Bogotá, Colombia
lfnino@ing.unal.edu.co, {djgomezb, ravejaru}@unal.edu.co

1 Introduction

In this paper, a novel immune based anomaly detection technique is proposed. Specifically an Artificial Immune System (AIS), based on negative selection, is used to detect some particular kind of computer attacks (Denial of Service attacks) on a typical LAN environment.

2 AIS Architecture

In this work, the general model of an AIS consists of the following phases: data collection, data pre-processing, learning (training), post-processing of the detectors and the detection phase. The learning and detection phases are described next.

2.1 Learning Phase

Here, a representation of the environment, the antigens (negative samples) and the detectors (antibodies) is chosen. Besides, a matching rule between detectors and antigens is specified; an antigen matches a detector if the distance between them is less than a threshold value. The goal of the training process of the AIS is to find an optimum covering of the self space with a suitable set of antibodies (hyper-spheres), which are generated based on the set of sample antigens. In intrusion detection, such set of antigens will correspond to DoS attacks.

- ***Generation of Antibodies***. The goal is to produce a new population of antibodies in the self space from the current population. The radius of a new antibody depends on the distance from its center to its nearest antigen. The generation of new antibodies is determined by its overlapping with existing detectors. The overlapping between two antibodies is a measure of the intersection between their corresponding hyper-spheres. Hence, the goal is to make such overlapping measure as small as possible.
- ***Selection of Antibodies.*** The best antibodies are selected according to the following criteria: the fittest antibodies are determined according to their radii

E. Cantú-Paz et al. (Eds.): GECCO 2003, LNCS 2723, pp. 243–245, 2003.

and their overlapping with other antibodies. Detectors with larger radius are more likely to be selected. Besides, if its overlapping measure is greater than a specified threshold, then such antibody will be discarded. Otherwise, it will become part of the next generation.

- ***Cloning Antibodies.*** A new set of antibodies is generated from the existing antibodies. A clone of an antibody is generated by making a copy of such antibody and moving its center at random; its radius is adjusted based on its distance to the nearest antigen.
- ***Post-processing Antibodies***. The goal is to cover small regions of the self space that may remain uncovered after the learning process, and that may produce false negatives. The radius of a new antibody is adjusted using the distance to the nearest antibody.

2.2 Detection Phase

A set of unseen patterns is presented to the AIS to be classified as either corresponding to normal traffic or to DoS attacks. The degree of abnormality of a pattern is proportional to the distance between the input pattern and the set of detectors. If the distance from a detector to an input pattern is smaller than a threshold then such pattern belongs to the self set. Otherwise, it will be considered as abnormal traffic. Four fields of the header information were used as input to the AIS, namely, *source and target port, packet size and protocol ID*. This data was used to completely characterize the information that would allow distinguishing packets belonging to DoS attacks and normal traffic.

3 Experimental Results

Network traffic was collected and used during the AIS learning process. The captured data was divided into two sets: the training set, which consisted of DoS attacks, and the test set that consisted of both, normal traffic data and DoS attacks. An input pattern consisted of a sequence of several consecutive packets. The AIS was able to detect all the attacks in the training set (it consisted of 4516 patterns), 99% of the attacks were detected in the test set, and the AIS performed well in classifying normal traffic. However, some patterns corresponding to normal traffic were misclassified as possible attacks. In the best experimental results, the AIS correctly classified 88% of normal traffic.

4 Conclusions

In this paper, a novel general anomaly detection technique based on immunology was developed. One main advantage of the AIS is that it starts with a small number of detectors and a new set of antibodies is generated through an iterative process that improves the covering of the self space. The number of detectors generated during the training process was smaller than the size of the input data set because the learning process allows the detectors to have variable radius and it is possible to cover the self

space with a small number of detectors. The post-processing of the antibodies improves the performance of the AIS. In future work, the immune technique may be applied to detect other types of intrusions in computer systems, or to solve any other anomaly detection problem.

References

1. R. Bolaños and C. Cadena. Intrusion detection in Linux using neural networks (in spanish). Computer Science Thesis. National University of Colombia. Bogotá, Colombia 2002.
2. D. Dasgupta (Editor), Artificial Immune Systems and Their Applications, Publisher: Springer-Verlag, Inc. Berlin, January 1999.
3. D. Dasgupta and F. Nino. Comparison of Negative and Positive Selection Algorithms in Novel Pattern Detection, In the Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC), Nashville, 2000.
4. IBM. Denial of service attacks: Understanding network Vulnerabilities in www.ibm.com. 2002.