An Application of Negative Selection Process to Building An Intruder Detection System

Jung W. Kim

Dept. of Computer Science, University College of London, J.Kim@cs.ucl.ac.kr

Jong Uk Choi

Dept. of Software, Sangmyung University, Korea, juchoi@markany.com

ABSTRACT

This research aims to unravel the significant features of the human immune system, which would be successfully employed for a novel network intrusion detection model. Several salient features of the human immune system, which detects intruding pathogens, are carefully studied and the possibility and the advantages of adopting these features for network intrusion detection are reviewed and assessed.

1. Human Immune Systems and Network Intrusion Detection

This research focuses on presenting the analogy between human immune systems and network-based IDSs. Somayaji *et al.*(1997) present more general principles and suggest various possibilities for a computer immune system. In contrast, this work concentrates on the design of competent *network-based IDSs*, and analyses the several outstanding features of the human immune system with this specific problem in mind.

Since the human immune system is distributed, self-organizing and lightweight, it clearly fulfills the design goals for network-based intrusion detection systems. Perhaps most importantly, the mechanisms used by human immune systems satisfy the three goals in an elegant and highly optimized way and this motivates future research harnessing such processes. Because of this study, it is thought that the application of computer immune systems to network-based intrusion detection is likely to provide significant benefits over other approaches.

2. An Artificial Immune Model for Network Intrusion Detection

Even though various approaches have been developed and proposed, no network-based IDS has satisfied all its requirements (Kim and Bentley, 1999a). This chapter roposes a novel approach to building a network-based IDS, which is inspired by a human immune system. (Kim and Bentley, 1999a) carefully studied the several salient features of human immune systems and showed the possibility and advantages of adopting these features for network intrusion detection.

Kim and Bentley (Kim and Bentley, 1999a) identified three main goals for designing an effective network-based IDS's: being distributed, self-organising and lightweight. Furthermore, they showed that the several sophisticated mechanisms of the human immune system allow it to satisfy these three goals. For the proposed artificial immune system, these mechanisms are embedded in three evolutionary stages: gene library evolution, negative selection and clonal

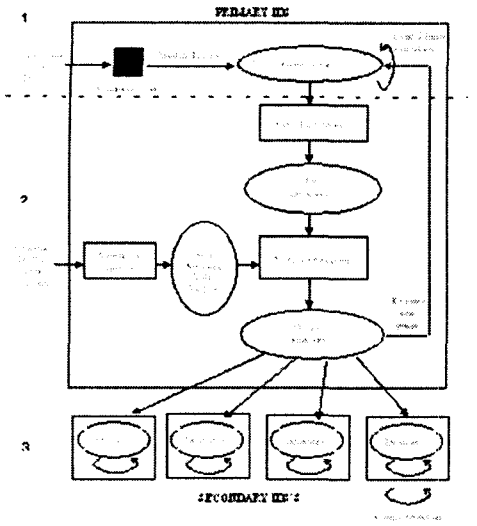

Figure 1.Conceptual Architecture of the Artificial Immune Model

selection. While the currently existing computer immune models focus on the use of a single significant stage according to their perceived purpose (Dasgupta and Attocj-Okine, 1997), (Forrest et al., 1997), (Mykerjee et al, 1994), the new artificial immune model proposed in this paper combines these three significant evolutionary stages into a single methodology. The overall conceptual architecture of the proposed artificial immune model is shown in Figure 1. In Figure 1, stage one indicates gene library evolution, stage two presents negative selection and stage three shows clonal selection.

3. Negative Selection of an Artificial Immune System

3.1) Negative Selection of the Human Immune System

An important feature of the human immune systems is its ability to maintain diversity and generality. It is able to detect a vast number of antigens with a smaller number of antibodies. In order to make this possible, it is equipped with several useful functions (Kim and Bentley, 1999a). One such function is the development of mature antibodies through the gene expression process. The human immune system makes use of gene libraries in two types of organs calledthe thymus and the bone marrow. When a new antibody is generated, the gene segments of different gene libraries are randomly selected and concatenated in a random order, see figure 2. The main idea of this gene expression mechanism is that a vast number of new antibodies can be generated from new combinations of gene segments in the gene libraries.

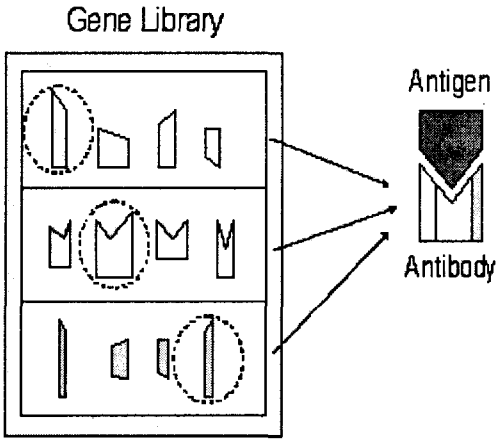

Figure 2. Gene Expression Process

However, this mechanism introduces a critical problem. The new antibody can bind not only to harmful antigens but also to essential self cells. To prevent such serious damage, the human immune system employs negative selection. This process eliminates immature antibodies, which bind to self cells passing by the thymus and the bone marrow. From newly generated antibodies, only those which do not bind to any self cell are released from the thymus and the bone marrow and distribute throughout the whole human body to monitor other living cells. Therefore, the negative selection stage of the human immune system is important to assure that the generated antibodies do not to attack self cells.

3.2) Negative Selection Algorithm

Even though the clear role of negative selection in a human immune system is to eliminate harmful antibodies, it shows some other important features, which can help us to devise

a more effective anomaly detection algorithm. Conventional anomaly detection algorithms generally establish the normal behaviour of a monitoredsystem and spot significant deviations from the established normal characteristics. The antigen detection mechanism by antibodies follows this conventional anomaly detection algorithm in a way, but it shows some other strengths over this conventional algorithm.

Forrest et al (1994), (Forrest, Hofmeyr, and Somayaji, 1997) proposed and used a negative selection algorithm for various anomaly detection problems. This algorithm consisted of three phases: defining self, generating detectors and monitoring the occurrence of anomalies. In the first phase, it defines self in the same way that other anomaly detection approaches establish the normal behaviour patterns of a monitored system. In other words, it regards the profiled normal patterns as self patterns. Inthe second phase, it generates a number of random patterns that are compared to each self pattern defined in the first phase. If any randomly generated pattern matches a self pattern, this pattern fails to become a detector and thus it is removed. Otherwise, it becomes a detector pattern and monitors subsequent profiled patterns of the monitored system. During the monitoring stage, if a detector pattern matches any newly profiled pattern, it is then considered that new anomaly must have occurred in the monitored system.

To apply the negative selection algorithm, firstly, we need to generate pre-detectors and this requires the creation of a gene library containing various genes. For the human immune system, the immature antibodies are generated via the gene expression process, in which the gene segments of different gene libraries are randomly selected and rearranged in a random order. From this process, the genes of the gene libraries contain the genetic information that determines the specific structure of antibody binding area, which will be the complementary structure of existing antigen binding area. These genes are usually inherited from ancestors genes. To be more precise, the genes of the gene library of the human immune system initially have some knowledge about the antigens that had attempted to attack ancestors body. Returning to our problem, the genes of the initial gene library of the artificial immune system, which will be the genes of pre-detectors, can be the selected fields of profiles to describe anomalous network traffic patterns. The initial genes might be set by the values of these fields that are observed when a previously known network intrusion is simulated. However, the simulation of network intrusion can be a difficult task if network administrators and users of the monitored network are not co-operative. For this reason, we employ Forrest et als negative selection algorithm (Forrest et al, 1994) to generate pre-detectors, which does not initially require any network intrusion simulation.

3.3) Network Traffic Data for Negative Selection

Data Gathering

The data chosen for this research is available at http://iris.cs.uml.edu:8080/network. html. This is a set of *tcpdump*data and was collected for a part of an Information Exploration Shootout, which is a project providing several datasets publicly available for exploration and discovery and collecting the results of participants. The network packet capturing tool, *tcpdump*, was executed on the single gateway that connects an intra-LAN to external networks. It captured TCP packet headers that passed between the intra-LAN and external networks as well as within the intra-LAN. Five different data sets were generated. The TCP packet headers of the first set were collected when no intrusion occurs and the other four sets were collected when four different intrusions were simulated. These intrusions are: *IP spoofing attack, guessing rlogin* or *ftp passwords, scanning attack* and *network hopping attack.* The details of attack signatures and attack points of the four different attacks are not available. This data originally had the fields of *tcpdump* format such as time stamp, source IP address, source port, destination IP address, destination port and etc.

Data Profiling

Since *tcpdump* is not designed for security purpose, its primitive fields are not enough to build a meaningful profile. Consequently, the first stage of our data profiling program is to extract more meaningful fields, which can distinguish normal and abnormal. Many researchers have identified the security holes of TCP protocols (Porras and Valdes, 1998) and so the fields used by our profiles are selected based on the extensive study of this research. They are usually defined to describe the activities of each single connection.

The automated profile program was developed to extract the connection level information from TCP raw packets. The TCP packet headers in the original file were collected according to chronological order. These original data were dumped into MS SQL-Server DBMS and the automated profile program was implemented in JAVA using JDBC accessing SQL-Server.

4. Experiments: the Feasibility of Independent Negative Selection

Experiment Design

The problems of the negative selection algorithm are exemplified through a seriesof experiments that apply it on the first data set. The negative selection algorithm used in these experiments mainly followed the implementation details which are used in (Forrest etal., 1994). However, there are several things that are different from Forrests implementation details and those are explained in the previous section 3.4 Implementation. Some implementation details have been kept the same as Forrests (Forrest et al., 1994). For example, the same matching function, the r-continuous matching function for measuring the similarity is used. Its matching threshold is defined as 9. In order to define this number, the formula to approximate the appropriate number of detectors when a false negative error is fixed (Dhaeseleer et al., 1997) , (Forrest et al, 1994) is used.

It was shown that the longer matching threshold drives the creation of more general detectors, but it also causes a larger number of random detector generation trials, which need to avoid the matching a self profile (Dhaeseleer et al.,1997), (Forrest et al, 1994). Thus, we can derive an approximate appropriate matching threshold number by varying the expected false negative error and random detector generation trial number. Even though this formula is clearly useful to predict the appropriate number of detectors and its generation number, its predicted number showed how infeasible this approach is for applying it on a more complicated search space. For instance, when the expected false negative error rate is fixed as 20%, its predicted the detector generation trial number is 51 and the appropriate number of generated detectors is 21935 for the matching threshold is 3. Similarly, when we define the matching threshold is 4, it predicted 535 for the former and 955 for the latter. None of these cases seem to provide any feasible test case in terms of computing time. In addition, it was observed that when we fixed the matching threshold number as four and ran the system, the system could not manage to generate any single valid detector after one day. Thus, we generated valid detectors by setting the matching threshold number that allowed a system to generate a valid detector in a reasonable time.

Experiment Result

It was observed that the average time of successful detector generation took about 70sec CPU time and the average number of trails to generate a valid detector was 2.6 when a matching threshold was nine. Even though this number gave reasonable computing time to generate a valid detector set, very poor detection accuracy by generated detectors was shown. The maximum 1000 valid detectors were generated and the detection accuracy was measured per every 100 detectors. The observed detection accuracy was less than 20% for four different intrusion data sets and one artificially generated random test set. This result was gained as the average of five runs.

In contrast to the promising results shown in Hofmeyrs negative selection algorithm for network intrusion detection (Hofmeyr, 1999) , the experiment result of this research raises doubt whether this algorithm should be used for network intrusion detection. These contradictory findings can be explained by the fact that Hofmeyrs encouraging result originated from the adoption of limited profile features which a negative selection algorithm can handle, while the experiment of this research used the more complicated but more realistic profile features that a negative selection algorithm struggles to solve. More importantly, Forrest (Forrest et al, 1994), (Somayaji et al., 1997) and Hofmeyer(1999) view that the network intrusion detection of artificial immune system is achieved mainly by the sole function of negative selection stage than the co-ordination of three different evolutionary stages However, Hofmeyer(1999) attempted to adopt the notion of clonal selection for his network-based IDS, but his system did not employ the full functionality of that stage such as clonning detectors when they detect intrusions. This is somewhat different from our view.

Consequently, the initial results of ourexperiments motivated us to re-define the real role of negative selection stage within an overall network-based IDS and design a more applicable negative selection algorithm, which following a newly defined role. As much of the other immunology literature addressed (Tizard, 1995), the antigen detection powers of human antibodies rise from the evolution of antibodies via a clonal selection stage. While Forrest et als negative selection algorithm allows it to be an invaluable anomaly detector, its infeasibility is also caused from allocating a rather overambitious task to it. To be more precise, the real job of a negative selection stage should be restricted to tackle a modest task but reflecting the closer role of negative selection of human immune system. That is simply filtering the harmful antibodies rather than generating competent ones.

Reference

[1] (Dasgupta and Attocj-Okine, 1997) Dasgupta, D.; Attoch-Okine, N., "Immunity-Based Systems: A Survey", *Proceeding of the IEEE International Conference on Systems, Man and Cybernetics*, Orlando, October, 1997.
Available at http://www .msci. memphis. edu:80/ ~dasgupta/publications.html

[2] (Dhaeseleer et al., 1997) Dhaeseleer, P. et al, "A Distributed Approach to Anomaly Detection", *ACM Transactions on Information System Security.*, 1997.
Available at http://www.cs.unm.edu/~patrik

[3] (Forrest et al., 1997) Forrest, S.; Hofmeyr, S; Somayaji, A, "Computer Immunology", *Communications of the ACM*, Vol.40, No.10, pp.88-96, 1997.

[4] (Forrest et al., 1994) Forrest, S. et al, "Self-Nonself Discrimination in a Computer", *Proceeding of 1994 IEEE Symposium on Research in Security and Privacy*, Los Alamos, CA: IEEE Computer Society Press, 1994.

[5] (Hofmeyr, 1999) Hofmeyr, S., *An Immunological Model of Distributed Detection and Its Application to Computer Security*, Phd Thesis, Dept of Computer Science, University of New Mexico, 1999.

[6] (Kim and Bentley, 1999a) Kim, J. and Bentley, P., "The Human Immune System and Network Intrusion Detection", *7th European Congress on Intelligent Techniques and Soft Computing (EUFIT '99), Aachen, Germany, September 13- 19, 1999.*
(Kim and Bentley, 1999b) Kim, J. and Bentley, P., "The Artificial Immune Model for Network Intrusion Detection", *7th European Conference on Intelligent Techniques and Soft Computing (EUFIT99), Aachen, German, September 13- 19, 1999.*

[7] (Mykerjee et al, 1994) Mykerjee, B.; Heberlein, L. T.; Levitt, K. N., "Network Intrusion Detection", *IEEE Network,* Vol.8, No.3, pp.26-41, 1994.
(Noel 1982), Noel, C., "Credit Scoring Systems: A Critical Analysis", *Journal of Marketing*, Vol.48, Spring, pp.82-91, 1982.

[8] (Porras and Valdes, 1998) Porras, P. A.; Valdes, A., "Live Traffic Analysis of TCP/IP Gateways", *Proceeding of ISOC Symposium of Network and Distributed System security, 1998.*
Available at http://www2. csl.sri.com/ emerald /downloads.html

[9] (Somayaji et al., 1997) Somayaji, A.; Hofmeyr, S.; Forrest, S., 1997, "Principles of a Computer Immune System", *Proceeding of New Security Paradigms Workshop, Langdale, Cumbria,* pp.75-82, 1997.

[10] (Tizard, 1995) Tizard, I. R., *Immunology: Introduction*, 4th Ed, Saunders College Publishing, 1995.