The Application of Immune Clone Algorithm In Network Intrusion Detection

Nitu Kumari[1], Remya sivan[2], Pallavi N[3]
[1, 2, 3] Atria institute of technology

Abstract- *With computer network's fast penetration into our life, various types of malicious attacks and service abuses increase dramatically. Network security has become one of the big challenges in the modern networks. Intrusion Detection (ID) is one of the active branches in network security research field. Many technologies, such as neural networks, fuzzy logic and genetic algorithms have been applied in intrusion detection and the results are varied. In this thesis, an Artificial Immune System (AIS) based intrusion detection is explored. AIS is a bio-inspired computing paradigm that has been applied in many different areas including intrusion detection. The main objective of our research is to improve the AIS based Intrusion Detection System's (IDS) performance on detection while keeping its system computing complexity to a low level. This paper, the immune cloning algorithm is used to optimize the detection of the intrusion detection system, use MATLAB software to carry out simulation and obtain the result analysis, and compare with the performance difference of the detector before and after the improvement according to the simulation results.*

Keywords- intelligent detector; immune algorithm; network intrusion detection.

I. INTRODUCTION

Driven by the rapid growth of the computer network technologies, the security of the computer and network information is becoming increasingly important. The appearances of the new access technologies and the advanced devices have increased the possibilities of malicious attacks or service abuses by various hackers. Also, with the appearances of multimedia services (video, audio, image, text, etc.), a faster, short-delay anti-virus system is required. However, the traditional passive defence mechanisms like encryptions and firewalls cannot fully meet current security requirements. Therefore, a special attack and misuse detection system is needed. The intrusion detection system (IDS) is such a system, which is composed by a series of devices and software applications to monitor network activities in order to protect the system from malicious activities.

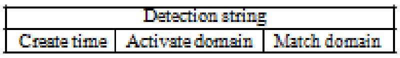
The IDS can detect unauthorized users or processes by comparing the user behaviour with a user profile. Two approaches, misuse detection and anomaly detection, are usually used in the intrusion detection process. The misuse detection is used to detect the intrusion when the behavior of the system matches with any of the intrusion signatures in the user profile. And the anomaly detection, which is also called as outlier detection , is used to detect the intrusion when the given data set does not match with the established normal behavior.

With the development of artificial intelligence, intelligent algorithm is applied to intrusion detection system, which has become a new research hotspot of intrusion detection system. Immune algorithm is one of the main trends of artificial intelligence algorithms in intrusion detection system. The core idea of the biological immune system is to identify and deal with "self" and "non-self", which is consistent with the goal of the intrusion detection system to achieve. The biological immune system has the characteristics of learning and cognitive ability, recognition ability, self-adaptability, self-organization, diversity and distribution. The distribution characteristic is that the immune system can be regarded as a distributed system, jointly realize more complex immune function through immune network's interconnection, which is currently consist with the real needs of constructing distributed intrusion detection system. So the constructed intrusion detection system based on immune system algorithm principle has a natural advantage. This paper analyzes the dynamic clone selection algorithm in immune algorithm, and proposed an improved dynamic clone selection algorithm as for its deficiency.

II. INTRUSTION DETECTION SYSTEM

Intrusion Detection System (IDS) can be defined as a system for recognizing and dealing with the malicious use of computers and network resources, including external intrusion of the system and unauthorized behavior of internal users. Designed and configured for the purpose of ensure the security of the computer system, IDS is a real-time discovery and processing of abnormal or unauthorized behavior technology and can detect of computer networks in violation of security policy behavior. Intrusion detection system, conducts real-time monitoring of network transmission, sound the alarm or take the initiative network security equipment to defend when discover suspicious transmission, is a proactive security technology. It first appeared in April 1980, the mid-1980s, IDS gradually developed into intrusion detection expert system (IDES). In 1990, IDS was divided into network-based IDS and host -based IDS, followed by distributed IDS. At present, IDS is developing rapidly, and many research scholars have carried out in-depth and fruitful research work in this field.

TABLE I. THE STRUCTURE OF THE DETECTOR



Detection string		
Create time	Activate domain	Match domain

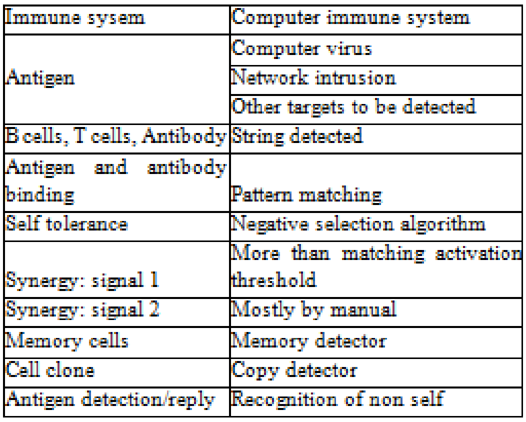
Intrusion detection system is generally composed of information collection module, data analysis module and response module, and the core of which is the data analysis module from which to determine whether the intrusion behavior occurred. In the immune-based intrusion detection system, as the core of the data analysis module, the efficiency of the detector generation algorithm and the matching algorithm of the detecting antigen directly affect the efficiency of the data analysis module. Therefore, the improvement of the algorithm plays an important role in improving the detection efficiency of the data analysis module and the entire intrusion detection system. The dynamic nature of the model is mainly reflected in the high frequency autologous filtering, the dynamic evolution of autologous, the dynamic tolerance of the immature detector and the dynamic immune memory and auto co-stimulus of the detector.

III. IMMUNE ALGORITHM

Computer immunology is an interdisciplinary subject based on bio-immunology, artificial immunology, and computer science. It mainly uses the latest computer science and technology to study the theory, rules, algorithms and models of artificial immunity, and apply these theories to specific application systems, to solve practical problems. In the system of intrusion detection, the principle of recognition of antigen and the process of antibody production and evolution in the biological immune system are used. The abnormal condition to be detected is set as antigen. The system produces the antibody according to the principle of immune algorithm and carries out the antigen Identify.

Immune algorithms mostly combine T cells, B cells, antibodies and other functions into one, unified abstract detector concept, the main simulation of biological immune system on the core of antigen treatment, including antibody production, autologous tolerance, clonal amplification, Immune memory, etc. [5]. When solving the specific problem with the immune algorithm, it is necessary to first correspond the relevant description of the problem with the related concepts and immune principles of the immune system, define the mathematical expression of the immune elements, and then design the corresponding immune algorithm.

TABLE II. THE COMPOSITION BETWEEN COMPUTER AND BIOLOGICAL IMMUNE SYSTEM



Immune sysem	Computer immune system
Antigen	Computer virus
	Network intrusion
	Other targets to be detected
B cells, T cells, Antibody	String detected
Antigen and antibody binding	Pattern matching
Self tolerance	Negative selection algorithm
Synergy: signal 1	More than matching activation threshold
Synergy: signal 2	Mostly by manual
Memory cells	Memory detector
Cell clone	Copy detector
Antigen detection/reply	Recognition of non self

Immune algorithm is an artificial intelligence algorithm based on biological immunology principle. In nature, immunity means that the body is resistant to infection without disease or infectious disease. The immune system is a complex system composed of immunologically active molecules, immune cells, immune tissue and Organ. It has a recognition mechanism, can be infected from the body of cells and external infection of micro-tissue infection caused by non-autologous tissue, pathogens or non-auto-element detection and elimination of viruses and other pathogens themselves and the function Bad, dysfunction, dysfunction and other symptoms caused by infection.

The immune system effect cells in the host body are responsible for identifying and removing the pathogens invading from the external environment and the toxins produced by them, and the tumor cells produced by the mutations in the inner environment, to realize the immune defense function and to protect the environment in the environment. The immune system can "remember" every source of infection, so when the same infection occurs again, the immune system reacts more quickly and more effectively . The most important feature of the biological immune system is immune memory, antibody self-identification and immune diversity, and from the information processing point of view, the immune system has tolerance, learning and cognition, distribution, robustness and adaptation, immune feedback, diversity and self-organization.

The immune cloning algorithm consists of the following steps:

- Define the antigen: abstract the problem needed to solve to the antigen form that the immune system can deal with, and antigen recognition corresponds to the problem of solving.
- Generate the initial antibody population: the antibody population is defined as the solution of the problem, the affinity between the antibody and the antigen corresponding to the solution assessment of problem, the higher the affinity, the better solution to the problem.
- Affinity calculation: Calculate the affinity between antibody and antigen.
- Clone selection: Antibodies with greater affinity for antigens are preferentially propagated and eliminated with less affinity antibodies. In order to obtain diversity, antibodies undergo mutations during cloning.
- Evaluate the new antibody community: If the termination condition is not met, the affinity is recalculated, and if the condition is satisfied, the current antibody community is the optimal solution for the problem.

In the immune dynamic cloning algorithm, the number of mature detectors is relatively small, and if you improve the diversity and effectiveness of mature detectors, you can generate more memory detectors, but also improve the detection rate. In view of this, the evolution of the mature detector is carried out on the basis of the immune dynamic cloning algorithm.

The evolutionary body is then tolerated by the negative selection, which is added to the mature detector set when it does not match the autobiographical set.

A niche genetic algorithm based on a shared function is used to generate a variety of antibody genes. The basic idea of the niche genetic algorithm based on the shared function is that in the solution space, some adjacent individuals form the niche, and by calculating the distance between the individuals in the population, the number of neighboring individuals around an individual is determined.

The fitness of all individuals in the habitat is reduced in a certain way according to the size of the niche, and the probability of small-scale niches being chosen will be increased to maintain the diversity of the population.

From the above analysis, we can see that the algorithm guides the evolution trend according to the interrelationship among the individuals within the population, and does not need the diversity of the antigens as the training set. The algorithm code is as follows:

```
CMatureDector CMatureDector::evolve(){ CColection *
subClt= new CClection [length]; for(int i=0;i<length;i++){

for(int j=0;j<length;j++){ Tj= array[j]^ array[j] dist = 0; //
dist While(tj){
if(tj==3){
dist+=2;
break;
}
if(tj==2||tj==1){
dist+=2;
break;
dist+=1;
break;
}
Tp==tj>>1;
if(tp%tj!=0)
dist++;
}
Tj=tp;
}
if(dist>=10){
subClt[i].add[arry[j];
subClt[j].add[arry[i];
}

}
```

The results of the evolutionary experiment of the mature detector are shown in the following figure. The model uses the niche technique to evolve the mature detector. It can be seen from the following figure that the niche technology can generate more effective mature detectors at the same time at the same time also greatly improves the diversity of the detector, and the number of mature detectors increases with the activation threshold, where p represents the probability of selection of the mature detector.

In order to verify the proposed model more flexible than the traditional immune -based intrusion detection model, the definition flexible, the detection dynamic and effective, the contrasting experiment is carried out. The contrast object is Dynamic _CS model, and the contrast experiment is carried out from three aspects Compare, TP values, FP values, and FN values, respectively. From the experimental results shown in the following figure, we can see that the dynamic model proposed in this paper has higher TP value than the traditional Dynamic_ CS algorithm model. The main reason is that the self-set of the improved model can be updated continuously. So that more efficient mature detectors can be produced by the tolerance process.

In order to simulate the real invasion, test the performance of this new model, each generation has joined 20 unknown "non-me" as a new invasion mode. They are tested with the known "non -me", and the performance of the system is described by true positive (TP) and false positive (FP), TP is the "non-me" detection rate, FP is the self-mistaken as "non-me" test rate, the goal to achieve is high TP, low FP.

V. CONCLUDING REMARKS

The research contents of this paper are mainly based on the network intrusion detection system model of immune cloning algorithm, and deeply study the running mechanism of biological immunity, compare the similarities and differences between biological immune system and intrusion detection system, and summarize the immune clone improvement algorithm which can be used for intrusion detection. The improved immune clonal selection algorithm proposed in this paper is mainly based on the introduction of niche technology on the basis of the original dynamic clonal selection algorithm. The evolutionary body is then tolerated by negative selection and those who not match with the font set are added into mature detector's collection. A new type of detector model is proposed based on the improvement of immune dynamic

REFERENCES

[1] U Aickelin, P Bentley, S Cayzer, J Kim, and J McLeod, “Danger theory:The link between AIS and IDS”[C], in Proc of the Second International Conference on Artificial Immune Systems (ICARIS-03), 2003.

[2] W. Jung, J. Kim, P.J. Bentley. Towards an artificial immune system for network intrusion detection: an investigation of colonel selection with a negative selection operator[C]. Proceedings of the 2001Congress on Evolutionary Computation, 2001, 2: 1244-1252.

[3] J. Kim and P.J. Bentley. Immune Memory in the dynamic clone selection algorithm[R]. Submit to the first international Conference on Artificial Immune System(ICARIS), 2002.

[4] D haeseleer, Forrest, Helman. An Immunological approach to change detection: Algorithms, analysis and implications[C]. In: Proc of the 1996 IEEE Computer Society Press,1996:110-119.

[5] J Kim, P Bentley. A Model of Gene Library Evolution in the Dynamic Clone Selection Algorithm. Proceedings of the First International Conference on Artificial Immune Systems(ICARIS) Canterbury[C], 2002. 9.