An immune system-based defence system of robot network security

Hua He¹, Zhiming Zhu*, Jie Zhang³
¹Department of mechanical engineering, Tsinghua University, Beijing, 100000, China
*Department of mechanical engineering, Tsinghua University, Beijing, 100000, China
³School of Electronics and Information Engineering, Liaoning Technical University, 125000, China
¹13910518989@139.com,³110566607@QQ.com
*Corresponding author’s e-mail:zzmdme@tsinghua.edu.cn

Abstract. After millions of years of evolution, as the representative of the biological world, human beings have adapted well to the earth's environment, including a wide variety of bacteria, chlamydia and viruses. Among them, the immune system plays a big role. But the immune system is also inadequate. For example, when dealing with old viruses, antibodies will gradually decrease or even disappear completely; what’s more, in the face of new viruses, the quantity of antibody production is not ideal, maybe even the virus engulfed immune cells. In view of this, this article draws on the human immune system and proposes an immune system-based defence system of robot network security taking advantage of machine learning.

1. Introduction
This paper proposes an immune system-based defence system of robot network security taking advantage of machine learning. Experimental results show that the system has many advantages such as fast virus interception, high accuracy, and long immune time.

The human immune system is a very complex and sophisticated system, but it comes down to three parts in short: B/T immune cells detecting intrusion; phagocytes detecting and killing invading viruses; immune active substances enter the bloodstream and maintaining long-term immune effects. In response to this immune process, this system has designed an efficient robot immune defense system. Experiments show that this system can detect a variety of external intrusions, with fast detection speed, and high accuracy and recall rates. In addition, this system also supports collaborative immunity between various parts of the robot. After one part is invaded, other parts will be notified to defend in time. After the defense is over, the immune capacity will be updated to the antibody library, and they will share the antibody library, which can achieve the purpose of all coordinated defense. The system has self-learning ability and can also play a defensive role against the invasion of new viruses.

2. Related work and research status
The biological immune system is a highly distributed and adaptive learning system with a perfect mechanism to resist the invasion of exotic pathogens and maintain the health and stability of the organism. It has the characteristics of good diversity, tolerance, immune memory, distributed parallel processing, self-organization, self-learning, self-adaptation and robustness. The biological immune
system is essentially similar to the network intrusion detection system. The biological system protects organisms from the invasion of pathogens in a complex environment. When pathogens invade the organism, the immune system can also detect the invaders in time and eliminate the invading pathogens using various mechanisms. After the pathogen is eliminated, the immune system has a memory function for the pathogen. When the pathogen invades again, the pathogen can be identified and eliminated more quickly.

Compared with the traditional intrusion detection technology, the network intrusion detection technology based on artificial immunity has the following advantages: first, it has good distribution and adaptability; second, it has the excellent ability to deal with variants of known and unknown attack behaviors; third, it can effectively improve the efficiency of intrusion detection system, increase detection rate, and reduce false alarm rate.

Hongwei Mo et al. introduced the current research status of artificial immune system in the field of computer security in [1], including abnormal diagnosis, network intrusion detection and virus detection. Licheng Jiao et al. summarized the general steps of immune algorithm in [2], and compared it with neural networks, evolutionary algorithms, and general deterministic optimization algorithms. In [3], Tao Li innovatively referred to the corresponding relationship between the antibody concentration and the body temperature, so that the grid body temperature could quantitatively describe the dangers currently threatening the network in real time. Haibo Li further proposed specific application scenarios of artificial immune system in [4]. Jinyin Chen et al. proposed a lightweight WSN intrusion detection method based on artificial immunity and mobile agent in [5]. Pearson proposed a novel robot design idea based on bionics in [6], which also provided inspiration for bionic immunity. Qishuai Yuan compared the similarities between artificial immune system and network intrusion in [7], and designed a network intrusion detection system which achieved improved results significantly. Tarapore D used bionic immunity in [8] to improve the fault tolerance of the robot system. Timmis J was inspired by the immune system in [9] and designed a system that allows the robot system to heal itself. In [10], Raj A was inspired by fish and elaborated on the key nodes in the robotics field from multiple angle of view, including the security field. In [11], Maria Akram constructed a safety system with high fault tolerance based on bionic immunity.

Currently, intrusion detection systems based on immune theory have the following main problems:

(1) Detector generation algorithm problem. After the negative selection algorithm is introduced into the artificial immune theory, almost all intrusion detection models based on the immune theory use the negative selection algorithm as a basic algorithm. However, due to the establishment of a complete autologous set for immune tolerance, the efficiency of detector generation will be very low. To reach the desired level, the time it takes is unbearable. Therefore, how to efficiently produce more qualified detectors has become a critical issue.

(2) The integrity of the autologous collection. In network intrusion detection, we are faced with a constantly changing network environment, and it is very difficult for us to build a complete autologous set that can describe the network environment. Since the network intrusion detection system based on artificial immunity is an anomaly detection system, only the accurate description of the autologous collection can effectively improve the detection efficiency of the system, and the incomplete autologous collection can easily lead to a relatively high false detection rate. Therefore, how to build a relatively complete autologous collection is a problem worthy of attention.

(3) The synergy of multiple immune mechanisms. Studies have shown that a single immune mechanism cannot achieve the desired detection effect. The human immune system is a complex system with multiple mechanisms synergistically. How to reflect this synergistic system into the network intrusion detection model is also an urgent problem to be solved.

3. Robot immune system

Imitating the human immune system, this system proposes a similar bionic immune system taking advantage of machine learning. It includes three parts: intrusion detection, intrusion recognition, cooperative immunity, and cold start.
3.1 intrusion detection
In the network intrusion detection system based on the immune system, the main function of the detector
is to detect illegal intrusion from outside. In terms of functional logic, the intrusion detection system
includes three basic modules: data acquisition module, data analysis module and user interface module.

The data collection module is mainly responsible for collecting data. The input data includes any
system data that may contain clues to intrusion behavior, such as network data, system call records, log
files, etc. The data acquisition module transmits the collected data to the data analysis module for
detailed analysis.

The data analysis module is the core module of the entire system. It receives data from one or more
acquisition modules, analyzes the collected data to determine whether an intrusion has occurred, and
finally outputs an indication signal that tells whether the intrusion has occurred. This signal can be a
simple alarm or contains relevant evidence of the intrusion and relevant response measures that can be
taken. Commonly used analysis techniques include pattern matching, statistical analysis and
completeness analysis. The first two techniques are used for real-time analysis, and the integrity analysis
is mainly used for post-mortem analysis.

The user interface module enables users to observe the output signal of the system and monitor the
operation of the system.

For the immune system, the first problem to solve is how to distinguish between autologous and non-
autologous activities.

3.1.1 Recognition of autologous and non-autologous activities
This paper adopts Bayesian method to distinguish autologous and non-autologous activities.

By measuring the values of A1, A2,..., An variables at any given moment, it is estimated whether the
system is being invaded. Among them, each Ai variable represents the information characteristics of
various aspects of the system: for example, cpu load, I/O times, network data packet size, and so on.
The Ai variable has two values, 0 means normal and 1 means abnormal. I means that the system is
currently under intrusion attacks. Then, P(Ai=1/I) and P(Ai=1/¬I) respectively represent the abnormal
reliability and sensitivity of each abnormal variable Ai.

\[
P (A_1, A_2, \ldots, A_n | I) = \frac{P (I | A_1, A_2, \ldots, A_n) \cdot P (I)}{P (A_1, A_2, \ldots, A_n)},
\]

Given the value of Ai, the reliability of I derived from Bayes' theorem is:

We need the joint probability distribution of I and ¬I. Assuming that each variable Ai is only related
to I and has nothing to do with other variables Aj (i≠j), then:

\[
P (A_1, A_2, \ldots, A_n | I) = \prod_{i=1}^{n} P (A_i | I),
\]

\[
P (A_1, A_2, \ldots, A_n | \neg I) = \prod_{i=1}^{n} P (A_i | \neg I).
\]
Then we have:

Through Bayes' theorem, we can detect and judge the probability of intrusion by using various measurement outliers and the prior probability of intrusion and the abnormal probability of each variable when the intrusion occurs. However, this kind of detection can only detect anomalies, and cannot tell what type of intrusion it is, therefore further classification taking advantage of machine learning models judgments are needed.

### 3.1.2 Intrusion recognition

In this paper, the clone selection algorithm is optimized. On the basis of the original algorithm, a machine learning algorithm is considered to complement each other.

The clonal selection algorithm (The Clonal Selection Algorithm, CSA) is mainly characterized in that immune cells generate clonal proliferation under antigen stimulation, and differentiate into diverse effector cells (such as antibody cells) and memory cells through genetic variation. In the process of clonal proliferation, only those B cells activated by the antigen can divide and proliferate, and the scale of proliferation is proportional to the affinity of the cell. Those cells with higher affinity to the antigen have a higher chance of clonal proliferation, and the mutation frequency during the clonal proliferation process is kept at a relatively low level. In this way, the original high-affinity characteristics can be retained on the basis of ensuring cell diversity. For those B cells with relatively low affinity, their chances of clonal proliferation are relatively small, but the frequency of mutation during the clonal proliferation is high. In this way, low-affinity cells have the opportunity to increase their affinity for antigens and maintain the diversity of cell populations. After clonal proliferation, the cells with degraded affinity will be killed. In this way, the affinity of the cell population is gradually improved and the entire system evolves toward the optimal solution.

The main steps are as follows:

1. Generating the initial population randomly, including the memory cell population and the remaining population;
2. Calculate the affinity and select top n best individuals;
3. Clone these n best individuals to produce a temporary clone population. The size of the clone depends on the size of the affinity. The larger the size of the clone with the higher individual affinity, vice versa.
4. The cloned individual undergoes mutation with a certain probability, and the probability of mutation is inversely proportional to the affinity. Then generate a mature antibody population.
5. In the mature antibody population, select some individuals with higher affinity to form a memory cell population, and then select some strong individuals to replace some individuals with low affinity in the population.
6. Regenerate new antibodies to replace antibodies with low affinity and maintain the diversity of the population. The core of the algorithm is to copy the multiplication operator and the mutation operator.

However, it needs very harsh conditions if the clone selection algorithm wants to achieve a more ideal effect. It requires the algorithm to be in a relatively static environment, which is obviously very different from the actual robot network environment.

In view of this, this paper considers machine learning based on the clone selection algorithm to make up for this shortcoming.
The field of machine learning has developed to this day, and there are already a variety of tools that can be used, such as: logistic regression, svm, decision tree, neural network and so on. Based on the robot scenario, considering the limited processing and storage capabilities of the robot, this paper adopts a simple and effective model of logistic regression to identify the type of intrusion.

The formula of logistic regression is shown in the formula above. Our goal is to train vector \( w \). To achieve this goal, we need to accumulate a certain sample size, which is, enough vector \( x \). Whenever a model \( m \) is trained, we put this model into the model library \( M \), which is our antibody library. Define the antibody library \( M=(m_1,m_2,\ldots,m_n) \).

The steps of intrusion identification are as follows:
1) Bayesian algorithm detects whether there is an intrusion event in real time.
2) If an invasion event \( x_i \) occurs, scan the antibody library \( M \), and calculate the affinity \( \text{sim}_i \) between \( x_i \) and antibody \( m_i \).
3) The final affinity of the invasion event \( x_i \) is: \( \text{sim}(x_i) = \max(\text{sim}_i) \).
4) Notify the corresponding antibody processing procedures to deal with the intrusion event \( x_i \).
5) If the antibody library is empty, store the intrusion event \( x_i \) in the sample library \( S \). When the sample volume of the sample library \( S \) reaches the number \( N \), a logistic regression model \( m_{\text{new}} \) is trained, that is, a new antibody is generated, and the model is placed in the antibody library \( M \).

It should be noted that the sample database \( S \) is classified according to the probability given by Bayesian algorithm. Different sample categories mean different intrusion type.

The flowchart of this process is as follows:

![Flowchart of intrusion identification process](image-url)
3.2 Synergistic immunity
The robot immune system designed in this paper can play a role of synergistic immunity. After each part detects an invasion, it can immediately notify other parts to enter the defense state. All parts share the antibody library. After the antibody library is updated, all parts have the latest and strongest immunity.

3.3 Cold start and transfer learning
This system can greatly alleviate the cold start problem through transfer learning. Network security is a long-standing problem. Although the attack methods on various platforms and carriers are not completely consistent, there are still many similarities in general. Therefore, this system collects samples of common attack behaviors on the network, then trains the samples in advance, and then fills the trained samples into the antibody library of the system, which perfectly alleviates the inefficiency of cold start. After the entire system is running, the system will automatically update the antibody library and evolve itself according to the actual situation.

4. Experiment
We build a robot immune system (RIS) in the simulation system using the above ideas, and test how the system performs under different attack types.

4.1 data processing
When detecting network intrusion, the original data may be affected by external noise, inconsistency, different data units, and redundancy in data attributes. These factors will ultimately have a decisive impact on the detection results. This paper deal with dirty data as follows: principal component analysis (PCA) to extract features, cleaning data noise, and normalization.

4.2 Experimental results

| Attack type        | accuracy/% | recall/% | Cost time/s |
|--------------------|------------|----------|-------------|
| DOS                | 95         | 92       | 0.31        |
| DDOS               | 93.6       | 91       | 0.4         |
| Trojan horse virus | 89         | 87       | 0.44        |
| CC                 | 97         | 96       | 0.52        |
| script attack      | 91         | 83       | 0.39        |

It can be seen from the experimental results that the robot defense system based on the immune system can achieve high recognition accuracy, and the false negative rate is also relatively low, that is to say the recall rate is high enough.

5. Conclusion and outlook
This paper designs a network intrusion detection system based on artificial immunity from the perspective of bionics. It is a complex system capable of parallel processing, self-learning, and self-adaptation. It not only improves the detection network speed and detection accuracy, but also effectively reduces the false negative rate of network intrusion. At the same time, the system can effectively identify existing attack patterns, and has the ability to discover new network attacks in a real-time changing network environment. The system has advantages of distributed parallel processing, self-organization, and self-learning.
However, the biological immune system also has shortcomings. For example: 1) If a virus is cunning and concealed, it is difficult to activate the immune system (for example, the new coronavirus is very concealed, and the previous immune system is helpless against the virus); 2) the immunity system may accidentally injure healthy cells; 3) The effective time of antibodies produced by the immune system is short, and it needs to be vaccinated from time to time to produce enough antibodies. In view of the above situation, on the one hand, the system can be improved to allow a quicker virus identification when the virus occurs. In addition, low-activity programs also need to be monitored just in case, which is also the direction of future research.

Acknowledgment

Upon the completion of this paper, I would like to first express my heartfelt thanks and sincerest respect to my teacher Mr. Zhu Zhiming. Mr. Zhu's tireless spirit of scientific research, profound academic knowledge, practical and realistic working attitude, magnanimous and modest character, the spirit of selfless dedication has always inspired me to pursue a higher realm of life and learn more knowledge. Words are endless, I sincerely thank all the people who care about me, thank them for giving me the power to overcome myself, surpass myself, and constantly pursue new heights, thank you.

References

[1] Hongwei M, Hongzhang J. (2003) Application of artificial immune system in computer security. Journal of Harbin Engineering University.
[2] Licheng J, Haifeng D. (2003) Progress and Prospect of artificial immune system. Acta electronica Sinica.
[3] Tao L. (2006) Network intrusion risk assessment method based on immunity. Invention patent CN200610020461.0.
[4] Haibo L. (2008) Research and application of computer system based on artificial immunity. Guangxi quality supervision guide.
[5] Jinyin C, Dongyong Y, Zhilin F. (2011) A lightweight intrusion detection method based on artificial immune and mobile agent for WSN. Invention patent CN201110434504.0.
[6] Pearson MJ, Mitchinson B, Sullivan JC, Pipe AG, Prescott TJ. (2011) Biomimetic vibrissal sensing for robots. Philosophical Transactions of the Royal Society B Biological Sciences.
[7] Qishuai Y, Yunpeng L. (2014) Application and research of network intrusion detection system based on Artificial Immune Principle.
[8] Tarapore D, Lima PU, Cameirao J, Christensen AL. (2015) To err is robotic, to tolerate immunological: fault detection in multirobot systems. Bioinspiration & biomimetics.
[9] Timmis J, Ismail AR, Bjerknes JD, Winfield AF. (2016) An immune-inspired swarm aggregation algorithm for self-healing swarm robotic systems. Biosystems.
[10] Raj A, Thakur A. (2016) Fish-inspired robots: design, sensing, actuation, and autonomy--a review of research. Bioinspiration & biomimetics.
[11] Maria Akram, Ali Raza. (2018) Towards the development of robot immune system: A combined approach involving innate immune cells and T-lymphocytes. Biosystems.