第32卷第5期 中国科学技术大学学报 Vol.32,No.5
2002年10月 JOURNAL OF CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY Oct. 2002

Article ID:0253-2778(2002)05-0530-12

NIDS Research Advance Based on Artificial Immunology

LUO Wen-jian, ZHANG Si-hai, LIANG Wen
CAO Xian-bin, WANG Xu-fa

(*Department of Computer Science and Technology, USTC, Hefei 230026, China*)

Abstract: Current network intrusion detection systems have a fatal deficiency of being unable to detect new intrusive behaviors of unknown signatures and low intelligence level. The protection mechanism of the natural immune system has brought us inspirations for designing a novel network intrusion detection system. By extracting the information processing mechanism of the natural immune system, network data transferring behaviors are divided into normal and abnormal behaviors, corresponding to the self behaviors and non-self behaviors of the network, and an initial network intrusion detection system is established based on artificial immunology. The main inspirations from natural immune system include non-self recognition mechanism, immune evolution mechanism, etc. This paper stresses on the construction and characteristics of the system, immune recognition algorithm and the testing experiments. The result of the experiments proves that the application of the protection mechanism of natural immune system to network intrusion detection system has an exciting future.

Key words: network intrusion detection; artificial immunology; unknown intrusion signature; immune evolution; immune recognition

CLC number: TP393.8 **Document code**: A

0 Introduction

Intrusion detection is an important component of network security systems. So far people have introduced statistical analysis, expert system, artificial neural network and other intelligent methods to design the IDS (intrusion detection system)[1]. These IDSs can be classified into two types: IDS based

Received date: 2001-05-11

Foundation item: This work is supported by National Natural Science Foundation of China(No. 69971022), and of Natural Science Foundation of Anhui Province.

Biography: Luo Wenjian, male, born in 1974, Ph.D. candidate. Research areas: artificial intelligence and network security. E-mail: wjluo@mail.ustc.edu.cn

on the host, and IDS based on network, namely network intrusion detection system (NIDS). This paper stresses on the latter. NIDS figures the abnormal behaviors by intercepting and analyzing the IP data packets. Some NIDS have been put forward[2]. But the current systems and their kernel technologies have obvious deficiencies. The main deficiencies are: (1) mere recognition and detection of the intrusions of known signatures and the impossibility to recognize new intrusion means; (2) low level intelligence and especially lack of the abilities of self-adaptability and self-learning. In fact, the intrusion detection systems based on the host also have the same problems. Therefore, in order to protect our network better in the vulnerable circumstances, some new ideas and methods must be employed to detect network intrusion behaviors, and then to construct the highintelligent network intrusion system.

The protection mechanism of the natural immune system is an excellent real paradigm for research on network intrusion detection, especially the mechanism of recognizing non-self pathogens (namely antigen) of the immune recognition, immune regulation mechanism and immune memory mechanism and others. All of them can be extracted and modeled to guide the construction of a novel NIDS. The relevant researches have just started, and Dasguptas has a good summarization in his paper[3]. The typical works are as follows: Forrest put forward the self/non-self distinguishing algorithm based on T-Cell immune response mechanism and applied it to the simple virus detection experiment in his paper[4]; Hofmeyr analyzed the algorithm offered by Forrest and make an experiment about SYN attack[5]; Kim analyzed the work of Forrest and others and provided a possible network intrusion detection model[6,7,8].

Based on the above works and deep exploration into the natural immune system, network intrusion means, network intrusion detection model and system based on artificial immunology, we design and establish a NIDS prototype[11]. In this paper, we use the information processing means in the natural immune system for reference, design and establish a prototype of network intrusion detection system based on artificial immunity, which can recognize intrusion behaviors of both known and unknown signatures and have better intelligent behavior. The prototype reflects the self-adaptive recognition ability of the natural immune mechanism for unknown antigen and makes use of the function of MHC (major histocompatibility complex) and the humoral immune response mechanism mediated by the B-Cell and immune evolution mechanism. This paper describes the modules of the system and their natural immune principles and analyzes the characteristics of the system and offers the result of the experiments.

The paper is organized as follows. Section 1 introduces components of the NIDS based on artificial immunology and the corresponding natural immune system principles, section 2 describes the immune recognition algorithm, section 3 is about the analysis and characteristics of the system, section 4 discusses the experiment and the experimental results, and the last section is conclusion and perspective.

1 The components of the NIDS based on artificial immunology

1.1 Introduction of natural immune mechanism

The basic function of natural immune system is to distinguish self and non-self, classify the non-self and then eliminate them. The natural immune system consists of immune organs, immune cells and

immune molecules. Immune organs are composed of central immune organs and peripheral immune organs. Central immune organs are composed of bone marrow and thymus, where lymphocytes and other immune cells generate, differentiate and mutate. Peripheral immune organs include lymphocytes, spleen, and catarrh tissues, where T-cell and B-cell settle and proliferate, and where immune system respondes to antigen's stimulation.

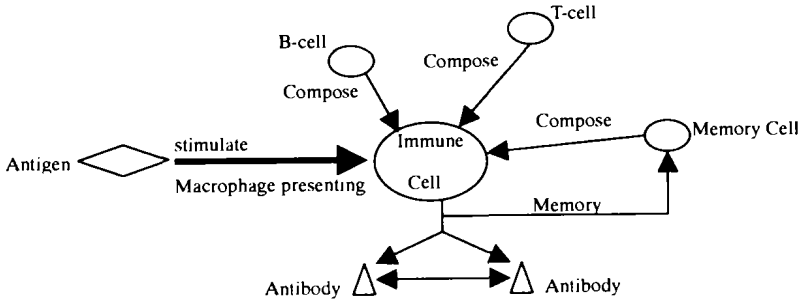

Fig.1 Immune abstract model based on clone selection

According to Burnet's clone selection theory[9], the natural immune system has a great deal of lymphocyte subsystems for all kinds of antigens. After the antigen intrudes into the body, the natural immune system selects a corresponding lymphocyte subsystem to combine with it, activates the lymphocyte subsystem, and makes it proliferate cells and generate the special antibody, thus inducing the immune response, and finally eliminating the antigen. Immune response can be classified into primary immune response and secondary immune response. When the immune system is confronted with an unknown pathogen (namely a new antigen), it can selectively generate many antibodies by bone marrow and thymus to recognize and analyze the antigen and memorize it after the antigen is recognized. This is the process of the primary immune response, which normally needs a long period of time. The secondary immune response, which normally needs a short period of time, means that the immune system can give out an immune response quickly when the same antigen intrudes again, activate the corresponding antibody, and eliminate the antigen by complex chemical responses[10]. Figure 1 is an abstract immune model based on clone selection theory.

1.2 The components of the NIDS based on artificial immunology

Relative definitions are listed below[7]:

Definition 1 Antigen and antibody:

The antigen refers to network intrusion behavior, namely the non-self signature; while the antibody is the detector of the NIDS.

Definition 2 PIDS and SIDS:

PIDS refers to the central immune organ and SIDS refers to peripheral immune organ.

Definition 3 Gene and gene library:

In the natural immune system the antibody consists of genes; in our NIDS, we regard every field of our detectors as a genotype, the value of a field as a gene unit. All possible values of each field make up of a gene library.

Definition 4 Gene representation:

Gene representation means the immature immune cell generated by gene recombination, a part of the immature detector set.

Definition 5 Immature detector:

Immature detector refers to the immature immune cells and molecules, which are generated by gene recombining and affinity mutating.

Definition 6 Mature detector:

Mature detector, namely the detector used to detect the intrusion behaviors, refers to the mature immune cell and molecule of the natural immune system.

As the following Figure 2 shows, this system is composed of PIDS (primary IDS) and SIDS(secondary IDS), whose structure is based on reference[6, 7, 8]. PIDS produces detector sets and send them to all secondary intrusion detection systems. SIDS detects the network data traffic where it locates, returns the detection results to PIDS, and drives PIDS to evolve. PIDS and SIDS cooperate with each other in our NIDS and form an NIDS with a high self-adaptive ability and can recognize both known and unknown signatures. Affinity mutation driven by the feedback from SIDS to PIDS is our best innovation, by which immature detectors have a good performance. Affinity mutation is the most important evolutional way to improve the self-adaptive ability in natural immune system and our NIDS based on artificial immunology.

In the following parts we introduce all the modules of our system, their functions and their respective design principles derived from the natural immune system.

(1) Primary IDS (PIDS)

The function of PIDS is the same as bone marrow and thymus of natural immune system, which is to adaptively generate detector sets that can be used to recognize the intrusion behaviors of known and unknown intrusion signatures. The process of PIDS's producing the antibody is divided into two stages.

The first stage is to generate immature detectors. In order to maintain the diversity of our detector, we introduce gene library evolution and affinity mutation. By analyzing the TCP/IP protocols and all kinds of attacks, from network data traffic we extract the features that can exactly reflect current network behaviors, such as the total counts of packets, the total counts of bytes and the total counts of SYN packets. According these extracted features, we define the self-pattern and the non-self pattern corresponding to the structure of the protein. Then from sufficient network traffic data that certainly do not contain attacks, we extract the packets' features and learn the normal network behaviors set by induction (regarded as the self signature set of network traffic); after gaining a self set that is large enough, the system produces short genes (regarded as the peptides of a protein), and each gene matches a unit of network traffic pattern. Then through diversity operation, primarily mutation, the system maintains the population distribution and diversity of gene library. The system repeatedly selects some genes from the gene library to recombine a gene representation, so we get an immature detector set (namely immature antibody set). The pattern of the immature detector is the same as the self-pattern of

network data traffic.

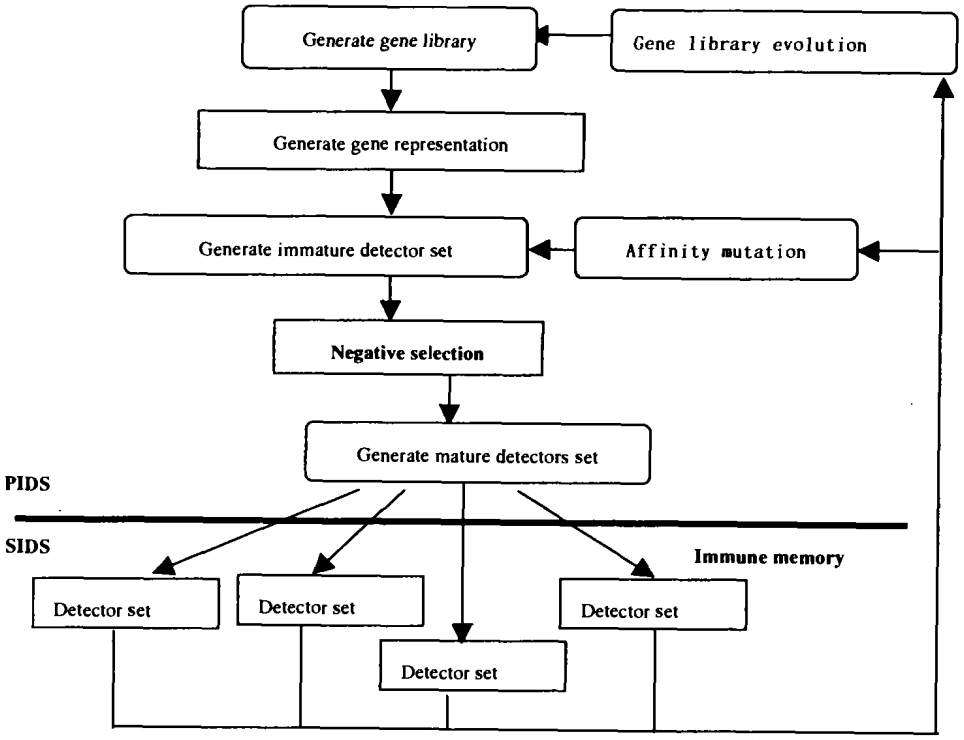

Fig.2 Structure of NIDS based on artificial immunology

The second stage is to generate mature detector through the negative selection module. Because the immature detector set includes both normal (self) and abnormal behaviors (non-self), the negative selection module processes a partial matching between the self patterns obtained by self-obtaining-module and elements in the premature detector set. If the matching is successful, corresponding detector will be erased from the premature detector set. Thus, only non-self patterns are kept in the final mature detector set. Non-self patterns represent abnormal behaviors in the network and should not be matched with normal behavior in the network. So we put all non-self patterns into the current detectors set (mature antibodies set) which is used to monitor network traffic. Negative selection module is extracted from biological immune recognition mechanism. The key characteristic of the module is that it designs monitoring technology based on normal network behavior and can recognize unknown network intrusion patterns. It can also incorporate immune memory of IDS to recognize and process known and unknown network intrusion patterns. The details are described in section 3 below.

(2) Secondary IDS (SIDS)

The function of SIDS is the same as the recognition and clearing of foreign pathogens (namely antigen) by dissociated antibodies or antibodies in the peripheral immune organ. Lymph nodes are distributed at different parts of the body and can communicate with each other. Similarly there are multiple SIDSs in the NIDS based on artificial immunology. There is at least one SIDS in each local network

(here it means the network behind the gateway) to ensure that it can monitor both the network traffic of the host and that of other parts, even that of all parts of the LAN. The SIDS works as follows:

First it receives the detector set from PIDS and then monitors current network traffic to extract the patterns that can represent current network behaviors and have the same structure with detectors. Second, partial matching is performed, that is, match each pattern with each detector. If all matching fails, it means that the current network behavior is normal; otherwise the network behavior which has a successful match is abnormal, perhaps an intrusion. So warning information is given out and set this detector to be a good one at the same time. The final stage is immune memory, that is, storing good detectors for the future detection and sending them to other SIDSs through PIDS. So all SIDSs can detect successfully the intrusion of the same pattern very quickly in the future.

2 Recognition Algorithm based on Immune Recognition Mechanism

2.1 Introduction to biological immune recognition mechanism

2.1.1 Basic biological immune recognition mechanism

The most important function of the natural immune system, which is performed by immune cells is to recognize self and non-self pathogens. The recognition for antigens includes antigen ingestion, process, presenting and recognition, achieved separately by microphages, T-cells and B-cells. The basic procedure of natural immune recognition and reaction is: (1) the antigen intrudes the body; (2) immune cells recognize antigens. On the surface of immune cells, the paratope integrates with the epitope and recognize antigens by binding the paratope and the epitope; (3) the activation and differentiation of immune cells. Immune cells with high affinity are activated and many new cells are generated.

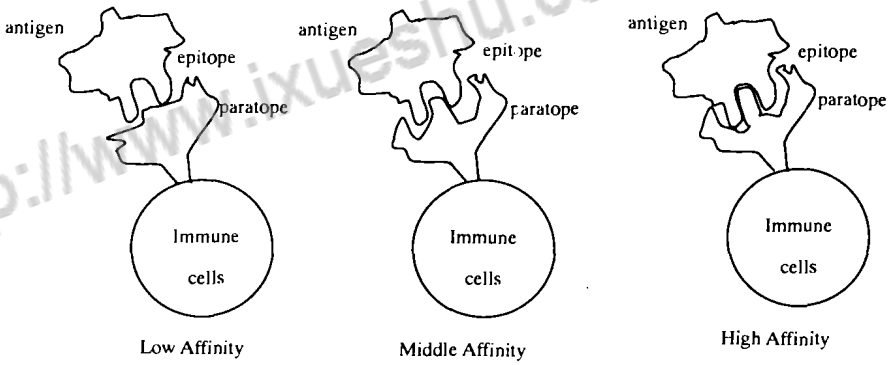

Fig.3 Recognition of patatope to epitope

Whether or not the immune cells are activated is determined by the degree of tightness of the coupling between the antigen's epitope and the paratope on the surface of an immune cell. The recognition of antigens is implemented through complementary matching between the epitope and the paratope. The binding intensity depends on the degree of tightness the complementary match. The tighter the binding, the more effective the recognition. As Figure 3 shows, the immune cell mainly refers to T-cells and B-cells and affinity means the binding intensity between the epitope and the paratope. The immune cells with low affinity will not be activated, those with middle affinity may be activated, while those with

high affinity can recognize the antigens well and be fully activated and abundantly generated.

2.1.2 MHC

In the natural immune system, MHC describes the features of individuals. There are proteins that can process antigens and protect themselves in MHC. If a cell has infected MHC different from the original MHC (not infected), individuals can recognize antigens through paratope on the immune cell's surface. That is, the function of MHC is to distinguish self and non-self. Thus, when MHC is used to design efficient NIDS, the first task is to properly define self and non-self patterns and the value range of self.

2.1.3 Humoral immunity mediated by B cells

The B cells and T cells are two main kinds of lymphocytes. The generation of them is similar, both needing negative selection to prevent autoimmunization. But the function mechanism differs greatly, which is usually seen as cell immunity mediated by T cells and humoural immunity mediated by B-cells. We think that the latter can reflect the self-adaptive recognition and elimination to foreign pathogens much better than the former. This section is to study the humoral immunity by B cells, extract the recognition mechanism and apply it to network intrusion detect.

The antibody paratope, sometimes called B cell paratope, is an immunoglobulin molecule on the cell surface. Activated B cells proliferate fast and generate a lot of antibodies (with the same paratopes as those of B-cells).

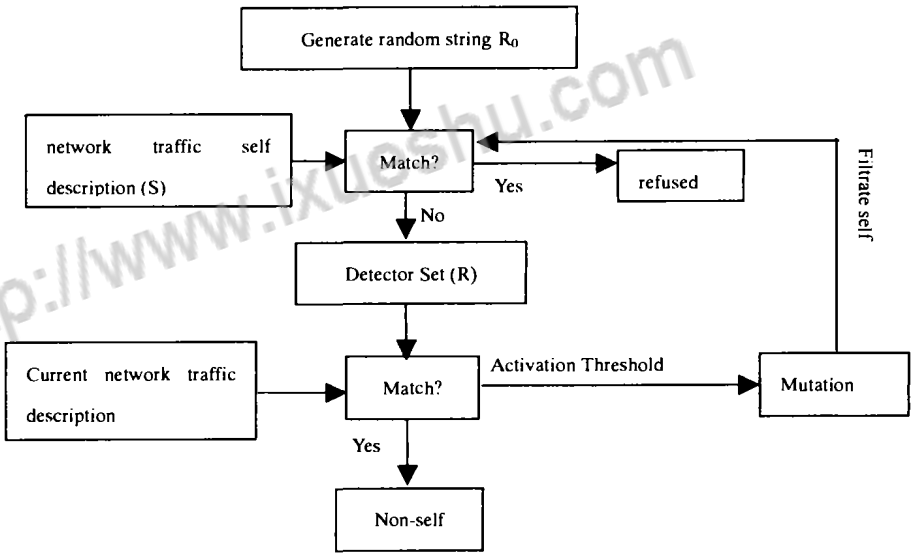

Fig.4 Immune recognition algorithm

2.2 Recognition algorithm based on immune recognition mechanism

Inspired by the humoral immunity mediated by B cells and the MHC, we propose a novel intrusion pattern recognition algorithm, as Figure 3 shows.

The algorithm has the following steps (as shown in Figure 4):

(0) According to the analysis of all kinds of network intrusion means, define the patterns of self

and non-self, which correspond to the compound structure of MHC that functions as self and non-self in the immune recognition.

(1) Define self and its value range by normal network traffic, which corresponds to all possible integration formats of MHC and the protein's peptides in the biological immune system.

(2) Generate the detector set. Each detector is a string that does not match the self-string (the data to be protected). This step corresponds to B cells' growth process.

(3) Protect data by comparing the current network traffic with detectors. This step corresponds to mature B cells' joining the lymphocyte re-circulation after leaving bone marrow and entering peripheral lymph organ.

(4) Detectors (immune cells) generate more efficient antibodies through high mutations after being activated by the current suspicious network behaviors (antigen). To avoid the autoimmunization, the new detectors generated by high mutation must be filtrated to erase the self-signatures.

The matching rule adopts partial matching rule. Because it is rather difficult to match two strings entirely when the length of the two strings is not very short, the partial matching of two strings means that if and only if at least r continuums fields in the two strings match each other. That is, to strings X, Y, when in both of them there are r identical characters in r continuums locations, match(X,Y) is true.

2.3 The characteristics of recognition algorithm based on the immune recognition mechanism

Here the calculation of the algorithm is mainly used for two types of the operation: one is the producing of random strings; the other is comparing two strings to judge whether they match each other.

The algorithm has the following characteristics:

(1) The detection probability increases with the number of the independent detection terminals. We can install several SIDS in an intranet to promote detection probability and robust performance.

(2) It needs a rather long time to produce the algorithm of detector. But since the normal network traffic has comparatively identical features, we do not need to reproduce our detector set regularly after we get enough detectors. What we must do is to update the detector set according to the evolution and the learning driven by SIDS.

(3) By mutation operation, this algorithm has the self-adaptive and self-learning abilities. So if we fix the detector set, the probability of detection changes is much better than the algorithm proposed by Forrest[4].

(4) This algorithm can be used to other optimization problems because of its good self-adaptive and self-learning abilities.

It's worth pointing out that this algorithm is invalid for the intrusive signatures formed by self-strings. This can be overcome by choosing different string lengths with enough features in different environments. So defining the patterns of self and non-self in step (0) is the key operation. In fact, there are similar tactics in the natural immune system. In the natural immune system, the protein is divided into many polypeptides. The polymorphic MHC molecules can combine with some polypeptides and present the mixture to T cells for recognition.

3 The analysis of characteristics of NIDS based on artificial immunology

The NIDS based on artificial immunology is designed by using information processing mechanism of the natural immune system for reference. The natural immune mechanisms employed in this system include immune recognition mechanism, immune memorizing mechanism, antibody variety mechanism and so on. It's a novel NIDS with capability of self-adapting and self-learning. According to the conclusion of J. Kim[8], NIDS should be distributive, self-adaptive and lightweight. The current NIDS hasn't reached the above requirements completely. But as a natural immune engineering model, the NIDS based on the artificial immunology can meet these requirements. Compared with the present NIDS, this system has some obvious advantages:

(1) The ability to recognize unknown intrusive signatures

The current NIDS can only recognize and process known intrusion, and are of no use to unknown intrusion, while following the recognition mechanism of natural immunology, the NIDS based on artificial immunology designs a novel negative selection algorithm by analyzing normal behaviors of the network and regarding them as itself. This algorithm is abstracted from the analysis and recognition process of B cells and MHC molecules to the unknown antigen in the natural immune system. The non-self model obtained from this algorithm can recognize and process the new intrusion means.

(2) Self-adaptability

This system displays a strong self-adaptive ability by continuous detection and learning. Firstly, the negative selection process guarantees that the normal signatures wouldn't be a mature detector; when an intrusion occurs, immune memory, gene library evolution and affinity mutation can guarantee the attainment of the most suitable detector subset by evolution and learning. Secondly, once a new intrusion is detected, the genes contained in the corresponding non-self signature will be added to gene library, which will have higher probability to be selected in the next evolving selection. Therefore similar non-self signatures are produced with high probability, and finally the system memorizes this intrusive signature. Thirdly, once a new intrusion is detected, the corresponding non-self signatures are sent to the primary IDS. The primary IDS will perform affinity mutation so that the similar intrusive means of this intrusion signature can be quickly dug out. In addition, the newly discovered intrusive signature will be memorized in the SIDS, and other SIDS will also remember it through the adjustment of PIDS so that they can detect the same kind of intrusion directly.

(3) Robustness

Robustness of this system is shown at two aspects: one is that each SIDS does not depend on each other. If one SIDS fails, it won't result in the collapse of the whole detecting system, and other SIDS still can perform the detection. The other aspect is described as follows. If a hacker successfully intrudes into some terminal machine and finds out the description of the abnormal behaviors of the SIDS in the terminal. Then he will try to intrude other terminals in disguise. The current NIDS does not have a good protection in this case, while our immune system can do better because in our system the inspector of every SIDS is particular, even if the invader steals the abnormal description of some SIDS, it's still difficult to enter the machines supervised by other SIDS.

(4) Distribution

In this system, detectors are produced in PIDS and used in SIDS. And the results of the detection will promote the evolution of the gene library and the variation of affinity, so that it produces better detectors. All SIDSs are distributed randomly. So this system is a distributed system. And this distributing characteristic makes the system easier to extend.

Please notice that this system is not designed by wholly simulating the biological immune system; the system is an engineering model. For instance, if it completely imitates the biological immune system, the affinity mutation should occur in SIDS after the detector is activated. But in our system it happens in PIDS, so as to perform negative selection process more easily and to reduce time complexity and space complexity of system operations. At the same time, the design of this system is not limited to biological immune mechanism. It also absorbs some techniques of the current non-immune intrusion detection.

4 Experiment

4.1 System description

Table 1 is our self/non-self pattern that we adopt in our prototype system now.

As a NIDS, our system can detect various attacks aiming at the leaks of TCP/IP, and can also detect attacks that have serious effects on network performance, including port scanning and most DoS attacks.

Tab.1 Self/Non-self definition

Index	Name	Meaning
3	RPN	Destination port
2	SPN	Source port
1	SS	The count of SYN packet
4	SDN	The count of data packet sent
5	RDN	The count of data packet received
6	SEQ	The value of SEQ in the IP data packet
…	…	…

4.2 Practical experiment

Figure 5 is a typical implementation of the NIDS based on artificial immunology. PIDS captures the network data traffic through our gateway. SIDS can be within and out of the internal local network.

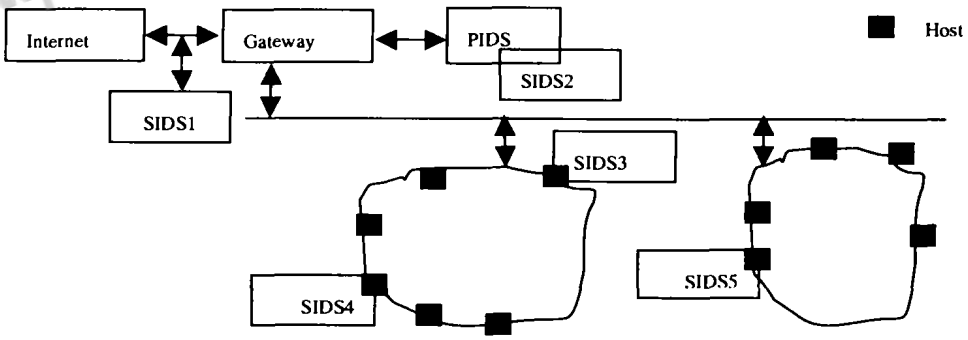

Fig.5 The implementation of NIDS based on artificial immunology

We build an actual environment to test the ability of our NIDS. In our experimental platform, PIDS and one SIDS(such as SIDS2 in Figure 5) are placed on the gateway; Other SIDS are placed in

a terminal of the internal network, such as SIDS3, SIDS4 and SIDS5 as shown in Figure 5.

After a lot of experiments, this NIDS based on artificial immunology shows good abilities, especially the ability of recognizing unknown intrusions. It is necessary to note that our IDS dosen't know initially any intrusive signatures, and that the system can learn to detect all attacks by self-signatures and non-self signatures learned before.

It must be noted that SIDS in a terminal can be configured to monitor not only the network behaviors of terminal itself, but also the behaviors of the subnet that it belongs to.

Tab.2 Shows some results of our experiment

Attack type	Attack tools(running system)	Our NIDS
		Can or can't
scanport	Portsacn(win)	Yes
	Haktak(win)	Yes
	Netfox(win)	Yes
	Scan.c(linux)	Yes
	Twwwscan.exe(win)	Yes
Tear Drop	Teardrop.c(linux)	Yes
SYN	Syn.c(linux)	Yes
Running 2 hours without attacks (heavy network traffic daytime)		There exists false alerts
Running 8 hours without attacks (light weight network traffic at night)		No false alerts

5 Conclusion

Nowadays, network security is an urgent problem. Current network intrusion detection systems cannot meet the practical requirements. The natural immune system is a real good example to design the defensive mechanism of our open and fragile network, especially IDS.

This paper introduces a feasible structure of NIDS based on artificial immunology and its corresponding basic inspirations from the biological immune system, and puts forward a new recognition algorithm and analyzes the characteristics of the system. Practical experiments prove that the design of detection technologies based on the protective mechanism of the natural immune system has a promising future.

The ultimate purpose of our artificial immune research is to extract practical theories and engineering models for network security. This research is the first step to a whole new world of exploration much more spaces yet to explore.

References

[1] Kumar S. Classification and detection of computer intrusions[D]. Purdue University, 1995. Also available at ftp://coast.cs.purdue.edu/pub/COAST/papers/kumar-intdet-phddiss.ps.Z.

[2] Mukherjee B, *et al*. Network intrusion detection [J]. IEEE Network, 1994,8(3): 26-41.

[3] Dasgupta D, *et al*. Immunity-based systems: A survey[A]. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics[C], Orlando, 1997, 12-15. Available at ftp://ftp.nisci.memphis.edu/comp/dasgupta/papers/smc97-papl.ps.Z.

[4] Forrest S, Perelson A S, Allen L R, *et al*. Self-Nonself discrimination in a computer[A]. Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy[C]. Oakland, CA:1994. 202-212. Also available at ftp://ftp.cs.unm.edu/pub/forrest/virus.ps.

[5] Hofmeyr S A. An immunological model of distributed detection and its application to computer

security[D]. New Mexico: University of New Mexico, 1999. Also available athttp://www.cs.unm.edu/~steveah/steve-diss.ps.gz.

[6] Kim J, *et al*. The human immune system and network intrusion detection [A]. 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99) [C], Achen, Germany, September, 13-19. Also available at http://www.cs.ucl.ac.uk/staff/J.Kim/EUFITthimmune.ps.

[7] Kim J, Bentley P. The artificial immune model for network instrusion detection [A]. 7th European Congress on Intelligent Techniques and Sofe computing (EUFIT'99) [C]. Aachen, Germany, 1999. Available at http://www.cs.ucl.ac.uk/staff/J.Kim/EUFITaimmune.ps.

[8] Kim J, Bentley, P. Negative selection and niching by an artificial immune system for network intrusion detection[A]. Genetic and Evolutionary Computation Conference (GECCO 99)[C]. Orlando, Florida: 1999. 149-158. Available at http://www.cs.ucl.ac.uk/staff/J.Kim/EUFITaimmune.ps.

[9] Burnet F M. The clonal selection theory of acquired immunity[M]. Vanderbilt University Press, 1959.

[10] Qi Anshen, Du Chanying. Nonlinear models in immunity[M]. Shanghai: Shanghai Scientific and Technological Education Publishing House, 1998.

[11] Luo Wenjian, Cao Xianbin, Wang Xufa. NIDS research based on artificial immunology[A]. ICICS 2001, Lecture Notes in Computer Science 2229 [C]. 2001. 371-375.

基于人工免疫的 NIDS 研究进展

罗文坚,张四海,梁 文,曹先彬,王煦法

(中国科学技术大学计算机系,安徽合肥 230026)

摘要:现有网络入侵检测系统的关键不足在于不能识别未知模式的入侵,智能水平低.生物免疫系统的自我保护机制对设计新的网络入侵检测系统具有很好的借鉴意义.论文通过抽取生物免疫系统中所蕴涵的各种信息处理机制,将网络数据传输行为分为正常和异常行为,分别对应为网络的自我与非我,建立了一个基于人工免疫的网络入侵检测系统原型.系统中蕴涵的生物免疫机制主要有非我识别机制、免疫进化机制等.本文着重介绍此原型系统的结构和特征、免疫识别算法,并进行了实际检测实验.实验结果表明生物免疫的自我保护机制在网络入侵检测系统方面具有很强的应用前景.

关键词:网络入侵检测;人工免疫;未知入侵模式;免疫进化;免疫识别