WUJNS
Wuhan University Journal of Natural Sciences

Vol.12 No.1 2007 167-171

Article ID: 1007-1202(2007)01-0167-05

DOI 10.1007/s11859-006-0261-4

Multi-Agent Network Intrusion Active Defense Model Based on Immune Theory

□ LIU Sunjun，LI Tao†，WANG Diangang，HU Xiaoqing，XU Chun

School of Computer Science, Sichuan University, Chengdu 610065, Sichuan, China

Abstract: Inspired by the immune theory and multi-agent systems, an immune multi-agent active defense model for network intrusion is established. The concept of immune agent is introduced， and its running mechanism is established. The method, which uses antibody concentration to quantitatively describe the degree of intrusion danger, is presented. This model implements the multi-layer and distributed active defense mechanism for network intrusion. The experiment results show that this model is a good solution to the network security defense.

Key words: artificial immune system; intrusion detection system; multi-agent system; network security

CLC number: TP 393

Received date: 2006-05-30

Foundation item: Supported by the National Natural Science Foundation of China (60373110, 60573130, 60502011)

Biography: LIU Sunjun(1975-), male, Ph.D. candidate, research direction: artificial immune system and network abnormal events detection. E-mail:liusunjun@163.com

† To whom correspondence should be addressed. E-mail: litao@scu.edu.cn

0 Introduction

With the rapid development of information technology and Internet, many network intrusion technologies have continuously changed, which result in more and more serious damages. However, these intrusion detection technologies[1], including statistics analysis, feature analysis, data mining, etc., all have some limitations, lack self-adaptation and can only detect the known attacks other than new attack models; The system also lacks robustness, which means that even the error in a local place can affect the whole works. So it is very urgent to build an active defense system, which has the features of self-adaptation, early warning and robustness.

The biological immune system (BIS) can identify and kill the intrusion antigens. It can be seen as a distributed autonomous system. Artificial immune systems (AIS)[2-4] derived from BIS, and have become an important research direction in the realm of artificial intelligence technologies. In 1994, the negative selection algorithm and the concept of computer immune system were proposed by Forrest[5]. In 1999, Kim[3] proposed dynamic clone selection algorithm, which was used in the network intrusion detection.

Agent[6,7] is an entity that has the ability of consciousness, solving problems and communication. With the cooperation and coordination during the isolated agents in a multi-agent system (MAS)[8], the problems in the complex environment can be solved and it has the features of distribution, robustness.

An immune multi-agent active defense model for network intrusion(IMAAD) is proposed here, which make use of self-adaptation, diversity, memory ability in artificial algorithm[9], combining the robustness and distribution in multi-agent system's architecture [2,5]. The concept of immune agent (IA) and its running mechanism are presented. The method using antibody concentration to quantitatively describe the degree of intrusion danger is developed. It implements the multi-layer and distributed active defense mechanism for network intrusion. The experiment results show that this model is a good solution to the network security defense.

1 The Theory of IMAAD

As an intelligent independent autonomous entity, immunocytes have the similarities with agent in essence. And a biological immune system can be seen as a distributed multi-agent system [7]. So we use immune theory in multi-agent active defense system for intrusion.

1.1 Concept of Immune Agent

On the whole, AIS has the abilities of self-learning and memory. Immunocytes are distributed and independent. In this case, the concept of IA is introduced here. Beside the common features inherited from the general agent, IA [3,5] has the desirable features of evolution, identification diversity, memory, tolerance, active defense, etc. The mapping relationship between BIS and active defense model is shown in Table 1.

Table 1 The mapping relationship between the BIS and the active defense system

Biological immune system	The active defense system
Organism	The whole net work
Organ	The network segment
Cells	Hosts
Vaccine distribution	The distribution of intruding information
Antigen	Binary strings extracted from IP packets
B cell, T cell, antibody	Antibodies expressed by binary strings
Clone cells	The copy of antibody

1.2 The Architecture of Active Defense Model

The IMAAD model constructs a multi-layer intelligent network security system. The architecture is shown in Fig.1, where IA is the security state of computers surveilled. Local Monitor Agent analyzes the state of the local area network, while Central Monitor Agent surveils the whole network.

IA is the kernel of this model, distributing in every host node, identifying the intrusion affairs. It also quantitatively evaluates the risk state facing by the node and sends the state to its own network segment's local monitor agent (LMA). Meanwhile, it would send the vaccine of the new attack to each node in the same network segment, which improves the defense ability and achieve active defense.

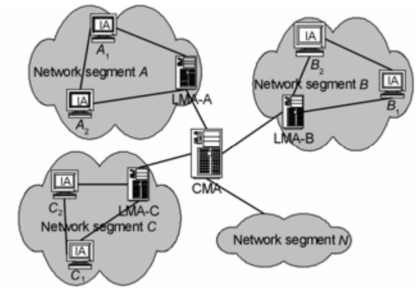


Fig.1 Architecture of IMAAD

LMA takes charge of surveilling the network segment, mixing data for each IA's information, evaluating the risk status of its own network segment, and sending it to Central Monitor Agent (CMA). And LMA of the intrusion segment would send vaccine to some other segments without intrusion to warn them. So the active defense of the whole network is implemented.

CMA takes charge of human computer interaction. It receives the risk status of network segment sent by LMA and shows the secure status through client interface. Then the administrator could take some response measures to protect the whole network timely.

1.3 Active Defending Mechanism of the IA

Figure 2 shows the architecture and work flow of IA, which consists of self antigens, immature antibodies, mature antibodies and memory antibodies, etc. The work flow includes two kinds of circulation: the circulation of immune antibodies' detecting outer intrusion antigens and the circulation of immune antibodies evolution. Both of them mutually affect and run at the same time.

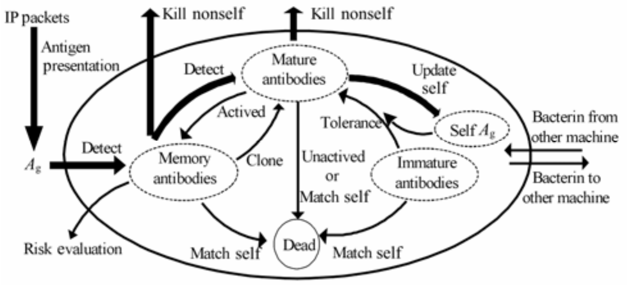


Fig. 2 Architecture of immune agent

1.3.1 The definition of immune elements

Antigens (A) in our approach are binary strings extracted from the IP packets, including IP address, port number, protocol type, etc, APC*s* is the antigen presentation process, which are given by:

$$A_g = \{\langle a,b\rangle \mid a\in D \wedge b\in \Psi \wedge |a| = l \wedge a = \mathrm{APC}s(b)\} \quad (1)$$

Self are normal network transactions, nonself represent attacks from network, Self, Nonself$\subset A_g$, Self$\cup$Nonself $=A_g$ and Self $\cup$ Nonself $=\varnothing$.

The Immunocytes is defines as follows:

$$B=\{\langle d,p,\text{age},\text{count}\rangle \mid p\in R,\ \ \text{age},\text{count}\in N\} \quad (2)$$

Where d is an antibody, p is the antibody concentration, age represents the cell age, and count is the antigen number matched by antibody d. Immunocytes contains two subsets: mature immunocytes (T_b) and memory immunocytes (M_b), where $B=M_b\cup T_b$ and $M_b\cup T_b=\varnothing$. When the amount of matched antigens arrives to a certain threshold, mature immuocytes wouldbe activated and evolve into memory ones. Immature immunocytes set is $I_b=\{\langle d,\text{age}\rangle \mid d\in D,\text{age}\in N\}$, which will evolve into T_b through self-tolerance.

The affinity is used to evaluate the match degree between x and y, l is the length of x, y, θ represents the threshold proportion. It is given by:

$$f_{\text{match}}(x,y)=\begin{cases}1, & f_{\text{h\_dis}}(x,y)\geqslant\theta\\ 0, & \text{otherwise}\end{cases} \quad (3)$$

$$f_{\text{h\_dis}}(x,y)=\sqrt{\sum_{i=1}^{l}(x_i-y_i)^2} \quad (4)$$

1.3.2 The immune-based intrusion detection

The immune-based intrusion detection consists of the evolution of immunocytes and antigens detection, both is concomitant.

The detection antigens process is fulfilled by memory immunocytes and mature immunocytes. The memory immunocytes will match the antigens to antibodies at first and eliminate nonself antigens. The left antigens will be submitted to mature immunocytes for detection and those nonself antigens would be eliminated. After the above detections, the left would be added to the set of self on behalf of maintaining the dynamic updating.

In the evolution of immunocytes, self-tolerance can make the immature immunocytes evolve into mature ones through the negative selection, and avoid antibodies matched with self. Where $A_b\in I_b, y\in\text{self}$, 1 means passing the self-tolerance and 0 means not:

$$f_{\text{tolerate}}(A_b)=\begin{cases}0, & \text{iff } \exists y\in\text{self}\wedge f_{\text{match}}(A_b,y)=1\\ 1, & \text{otherwise}\end{cases} \quad (5)$$

At the same time, the set of mature antibodies that are activated into memory ones is shown in Eq.(6), and the set of mature ones that suffer failing activation is shown in Eq.(7), where β is the activated threshold, and λ is the lifecycle:

$$T_{\text{active}}=\{x\mid x\in T_b\wedge x.\text{count}\geqslant\beta\wedge x.\text{age}\leqslant\lambda\} \quad (6)$$

$$T_{\text{dead}}=\{x\mid x\in T_b\wedge x.\text{count}<\beta\wedge x.\text{age}>\lambda\} \quad (7)$$

1.3.3 The risk evaluation of IA

IA simulates the cells in BIS to apperceive the surrounding, the types and amount of antibodies in IA reflect the attack type and intensity suffered by a system. Therefore, the risk of hosts and network can be quantitatively computed according to the antibody amount change. Set $\phi_j(0\leqslant\phi_j\leqslant1)$ is the danger coefficient of the attack j, n_{ij} is the antibody amount which detects attack j on host i, c_{ij} is the antibody amount which detects attack j on host i in normal state. The $d_{\text{node}-ij}(0\leqslant d_{\text{node}-ij}\leqslant1)$ is the risk on host j suffering attack i , and $d_{\text{node}-i}(0\leqslant d_{\text{node}-i}\leqslant1)$ is the risk suffering all attacks by host j is $d_{\text{node}-i}(0\leqslant d_{\text{node}-i}\leqslant1)$:

$$d_{\text{node}-ij}\leqslant1-\frac{1}{1+\ln(\phi_j(n_{ij}-c_{ij})+1)} \quad (8)$$

$$d_{\text{node}-i}=1-\frac{1}{1+\ln(\sum_j(\phi_j(n_{ij}-c_{ij}))+1)} \quad (9)$$

1.4 Active Defending Mechanism of Network Layer

The LMA on the one side, takes charge of evaluating security risk of the network segment, then sending the intrusion information to other network segment's LMA. On the other side, it receives the vaccination from other LMA, then update the antibody set of IA using the received vaccination so the active defense of the whole network is achieved. Set $\omega_i(0\leqslant\omega_i\leqslant1)$ is the importance coefficient of host i. The $d_{\text{LanK}-j}(0\leqslant d_{\text{LanK}-j}\leqslant1)$ is the risk of network segment k suffering attack j and $d_{\text{LanK}}(0\leqslant d_{\text{LanK}}\leqslant1)$ is the risk of network segment k suffering all attacks:

$$d_{\text{Lank}-j}=1-\frac{1}{1+\ln(\sum_i(\omega_i\phi_j(n_{ij}-c_{ij}))+1)} \quad (10)$$

$$d_{\text{Lank}}=1-\frac{1}{1+\ln(\sum_j(\sum_i(\omega_i\phi_j(n_{ij}-c_{ij})))+1)} \quad (11)$$

1.5 Communication Mechanism of IMAAD

The concept of vaccine is introduced in to the active defense model. And the message mechanism[7] makes the communication during the agent come true. The structure of the messages is defined as:

<Sender> <Receiver> <SendTime> <ValidTime> <Content>

The Sender and Receiver can be a transverse communication during the agents in the same level and also can be the longitudinal communication during the agents in the different levels. Receivers judge whether to receive this message depending on SendTime and ValidTime. Content contains information about the real-time risk evaluation and new antibodies.

Distributing vaccines strengthens the contact during the agents. Sharing the effective antibodies in each IA improves the response ability of the nodes. Then the capability of resist attack is highly improve.

2 Simulations and Experiment Results

2.1 Experiment Environment and Parameters

The experiment environment contains two network segments A and B, both of which consist of the same 20 computers. We select the KDDCUP 99 data set [10] as the experiment data. The training and testing set contains four types of attack data: DoS, Probe, U2R, R2L. The amount of normal data is much more than attack data in testing set I which contains attacks including: Neptune, Guess_passwd, Protsweep, Buffer_overflow. In testing setⅡ, it has same normal data，and attack data have more types of attacks, e.g. Land, Spy, Perl, Mscan, etc.

Antigens are the features of IP packets, e.g., source/destination IP, port number, protocol type, IP flags, TCP/UDP/ICMP fields, etc., where l=172. The primary parameters are as follow: Mature antibody activation threshold satisfies $\beta = 10$; mature antibody's lifecycle $\lambda = 5$; the affinity matching threshold $\theta = 0.7$. The importance coefficient of computer A_i, B_i is same, $\omega = 0.2$. The danger coefficient ϕ of DoS, Probe, U2R, R2L are respectively 0.8, 0.6, 0.4, and 0.4.

2.2 Experiment Results and Relative Analysis

In order to validate the feature of self-learning in AIS, Table 2 and Table 3 shows the comparative results when detecting the testing sets between IMAAD model and a detection tool BRO [11] which is based misuse detection. It can be seen that the IMAAD model ensures a higher true positive rate (TP) and a lower false positive rate (FP), can identify more attack type, which proves AIS owns the ability of self-adaptation and self-learning.

Table 2 Detection results of IMAAD model experiment

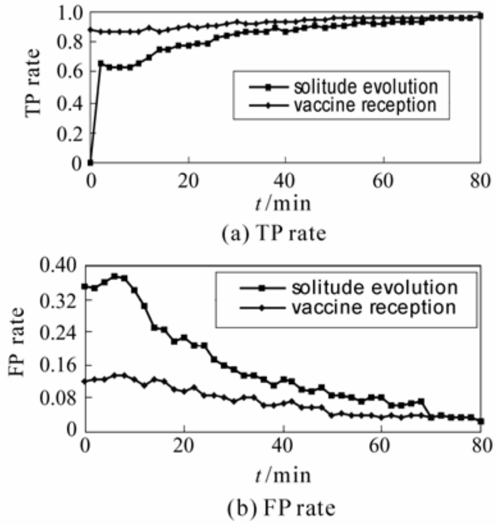
Data type	Testing set Ⅰ			Training set Ⅱ		
	Identified attack types	TP/%	FP/%	Identified attack types	TP/%	FP/%
Normal	0	98.6	0	0	97.2	0
DoS	2	97.2	2.8	5	97.1	2.9
Probe	2	96.5	3.5	4	94.3	5.7
U2R	2	94.5	5.5	4	95.4	4.6
R2L	1	95.2	4.8	3	94.3	5.7

Table 3 Detection results of BRO experiment

Data type	Testing set Ⅰ			Training set Ⅱ		
	Identified attack types	TP/%	FP/%	Identified attack types	TP/%	FP/%
Normal	0	97.5	2.5	0	97.2	2.8
DoS	1	73.3	26.7	2	53.6	46.4
Probe	1	72.2	27.8	2	52.1	47.9
U2R	1	68.5	31.5	1	45.6	54.4
R2L	1	94.5	5.5	2	63.5	36.5

To validate our model's ability of active defense in host node, Figure 3 shows the TP and FP curves of A_2 and A_3 in different instances. The IA in A_2 detects attacks with solitude evolution by itself, while A_3 accepts the vaccine sent by A_1 to detect attacks. It shows at later period of the experiment, the corresponsive TP and FP curves of A_2 and A_3 is similar. But in the early and middle period, the detection efficiency of A_2 is very low, because of absence of antibodies, so attacks do large damages to A_2, which is unaccepted to the key nodes in the network.

To validate the early warning ability of our model to network node and network segments, we use the same intensity to attack network segment A and B. Segment B has received the warning information of A and taken some measures to prevent the damage to the computer

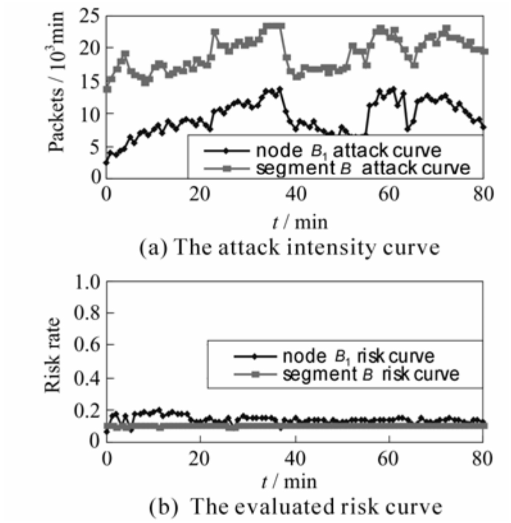


(a) TP rate

(b) FP rate

Fig.3 Comparison of detecting effect between solitude evolution and vaccine reception

and network segment. Figure 4 shows the risk variation curve and the actual attack intensity curve on host B_1 and on segment B. It concludes that when using our model, the risks curve of B_1 is much lower than the real attack intensity curve. The same conclusion is obtained on the comparison between the evaluated risk curve with the actual attack intensity curve on network segment B. It proves that our model can do better in active defending and protecting the network security.



(a) The attack intensity curve

(b) The evaluated risk curve

Fig.4 Compare the evaluated risk with the actual attack intensity on host B_1 and the same compare on segment B

3 Conclusion

In this paper, an immune multi-agent active defense model for network intrusion is proposed. This model has the following advantages: ① Self-learning. Memory mechanism and the producing antibody mechanism make the model can detect both the known and unknown attacks; ② Multi-layer. The concept of vaccine is introduced, and the active defense is achieved in different layers and nodes; ③ Real-time. This model can quantitatively evaluate the risk status facing by the network; ④ Robust. This model uses a distributed architecture, so that the attacks on a single node cannot influent the others. The experiment results show that this model changes the isolated and passive status in the traditional network security models. It is a good solution to establishing active defense for the network security.

References

[1] Bai Y. Intrusion Detection Systems: Technology and Development[J]. *IEEE Advanced Information Networking and Applications*, 2003, **6**(3) :710 – 715.

[2] Forrest S. A formal Frame Work for Positive and Negative Detection Schemes[J]. *IEEE Transactions on Systems Man and Cybernetics*, 2004, **34**(1):357-373.

[3] Kim J, Bentley P. The Human Immune System and Network Intrusion Detection [C]//*Proc of the 7th European Congress on Intelligent Techniques and Soft Computing.* Aachen, Germany, Sept, 1999:374-383.

[4] Hofmeyr A, Forrest S. Architecture for an Artificial Immune System[J]. *Evolutionary Computation*, 2000, (1):23-28.

[5] Forrest S. Self-Nonself Discrimination in a Computer[C] //*Proc of IEEE Symposium on Research in Security and Privac.* Oakland: IEEE Press, 1994.

[6] Dong Yongle. A Cooperative Intrusion Detection System Based on Autonomous Agents[J]. *IEEE CCECE*, 2003, (2): 861- 863.

[7] Shi Zhongzhi. *Intelligent Agent and Their Application* [M]. Beijing: Science Press, 2000(Ch).

[8] Ballet P, Rodin V. Immune Mechanisms to Regulate Multi-Agents Systems[C] //*Proc of* GECCO 2000. Las Vegas, Nevada: IEEE Press, 2000:456-462.

[9] Ayara T, Timmis J, Lemos R D, *et al*. Negative Selection: How to Generate Detectors[C] //*Proc of 1st International Conference on Artificial Immune System.* University of Kent at Canterbury, UK, Sept 9-11,2002.

[10] Richard P. *Evaluating Intrusion Detection Systems: The 1999 DARPA Off-Line Intrusion Detection Evaluation*[R]. Lexington, MA (USA) Lincoln Lab, MIT, 2000.

[11] Paxso V. BRO: A System for Detecting Network Intruders in Real-Time[C]//*Proc of* the *Seven USENIX Security Symposium.* San Antonio, TX, USA, Jan 26-29, 1998.

□