2012 International Conference on Image, Vision and Computing (ICIVC 2012)
IPCSIT vol. 50 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V50.22

A Real-time Model of Risk Evaluation Based on Multi-processor

WANG Liang[+]

Dept. of Computer Science, Sichuan University, Chengdu , P.R.China

Abstract. The performance of risk evaluation for network security at high-speed network was improved by using multi-processror architeture. This model was based on immune theory as the theoretical basis, by simulating the immune cells of the external antigen recognition, clone selection, changes of antibody concentration to carry out risk assessment. Results of the simulation verified that the model proposed c evaluate the risk assessment at high-speed network and improve the performance and efficiency .

Keywords: network security; artificial immune; risk evaluation;

1. Introduction

With the promotion of network applications,network attacks rise. Faced with an increasingly high-speed, complex network environment, how to accurately assess the current threats facing the network is becoming the focus of network security research. Network information security risk assessment techniques is an important part of risk assessment. Considering the vulnerability of the systemnad some factors as importance,risk assessment techniques can assess and identify security risks of the system. Network risk assessment methods are mainly two types: static assessment and real-time detection. Static assessment moethods use assessment criteria to evaluate risks,such as TESEC[1],IESEC[2]; You can use some security experts to assess the risk of network systems. As the static evaluation method assessing through the static factors,such as the importance of assets and the vulnerability,it lack the real-time detection evaluating capabilities. Real-time risk detection system compute the quantitative risk base on the current active state of the system. At present,domestic and international real-time evaluation of network risk is at the exploratory stage. In 2002,Madan used a model based on state machine to describe the current system faces network intrusion, and presents a risk assessment method. But the disadvantage is that the model only emphasize the attack results and be lack of real-time detection capabilities to the overall security of the system[3].In 2004,Chu proposed a evaluation framework between static and dynamic assessment testing. He assess the risk of network system with some simple incidents such as the sudden change in operating conditions and the loss of components. However,the main basis of the framework is the time or the probability of the konwn vulnerabilities,so it can not properly assess the current risk of network[4].

Computer security problems and immune system has many similarities[5]. Forrest put some of the human immune mechanisms in network security research and opened up a new situation in this field. Some scholars have proposed real-time risk assessment method based on immune[6]. However, in a large network environment, or a larger number of memory cells within the system, the time and space complexity of risk calculation grow too fast. This paper proposed a multi-processor architecture if real-time network risk assessment model baseed on artificail immune principles of risk assessment. The model take the event sequence of intrusion detection system as input. It simulate the non-self antigen responsing process in different processors,and the calculat the current network risk quantitatively.

[+] Corresponding author.
E-mail address: legend115599@gmail.com

This paper will simplify and improve zdelta to generate the forward difference and reverse difference between the files at the same time. Then we can use the forward difference file and the last time archive file to reconstruct the latest file mirror, and use the reverse difference file for archive management.

2. the evaluation model

2.1. The principles of risk assessment based on the immune

The main function of the immune system is to distinguish between self antigen and non-self antigen and destroy the non-self. The complex process achieved through a variety of immune cell such sa B cells and T cells. When the invasion of human antigen encounter, B cells will try to match non-self antigen and released a large number of antibodies, leading to the concentration of antibodies against such antigens increased; After the death of antigen, the release of the corresponding antibody will be checked and decline the concentration of such antibodies and ultimately stabilized. Because under normal circumstances, the body types of antibody concentration remained unchanged, so you can measure changes in the concentration of various types of antibodies to determine the illness of human and the severity of illness.

The relation between concentration of antibodies and human disease is so similar to the computer security.So we can use the principle of artificial immune to carry out risk assessment. And the corresponding relationship between body's immune system and the evaluation model is in Figure 1.

Antigen	The binary flow of the events monitored by IDS module
Memory cell antibody	A string representation of the antibody system
Lymphocytes	Hosts in monitored network
body	Monitoried network

Figure 1. Mapping Artificial Immune System Into Risk Evaluation Model

Set Ag as the antigen, M_i as the menmery cells. $f_{match}(Ag,M)$ as matching function, P_{M_i} as the antibody concentration of the memory cells, $f_{clone}(M)$ as the cloning function, $r_{l,i}$ as the i type of attack risks in network j , r_l as the overall risk for the host l ,then the entrie risk assessment process can be described as:

If $f_{match}(Ag,M_i)=0$,then Ag is self antigen and must be harmless,and the concentration of the memory cells did not change;Or the memory cell M_i have matched the Ag ,then M_i cloned themselves,and the concentration will be $P_{M_i}^{'}=P_{M_i}\cup f_{clone}(M_i)$. Comes in the risk calculation cycle, according to antibody concentration and the relationship between human diseases, the host classification calculated risk, the overall risk of the host, the network classification of risk and overall risk of the network.

2.2. System Framework

Based on immune network theory,system architecture desinned as Figure 2.

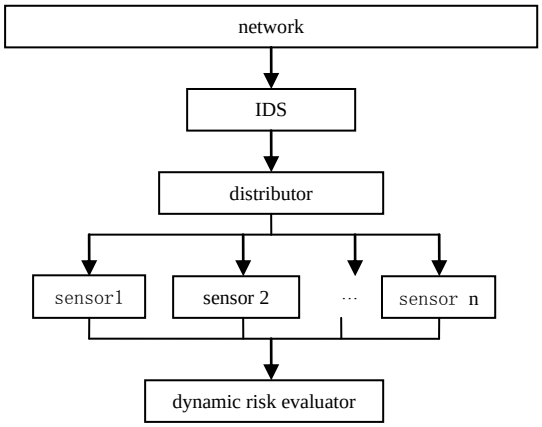


Figure 2. System Framework

IDS capture high-speed data packets from the network analysis, and produce test results. Test results include data packet source, destination address, the event log information, and special permit packet. This information will serve as a follow-up risk assessment of the direct data sources.

To achieve multi-processor parallel, the system adds a distributor, its duty is to conduct the event distribution. Distributor to produce the detection of IDS event stream as input, according to the purpose of the event recorded in the IP, will be allocated to the various events of different sensors, so the sensor can be in different data sets on parallel execution.

Sensor is the core of the system, it is to receive the event as an antigen, antigen simulation time organism by the external concentration of antibodies in the process. The risk of immune-based model, the network security risk value of time and space complexity of the network the number of all memory cells is linear . When monitoring a larger number of memory cells within the network, the calculation of the risk of time and space complexity of the network grew rapidly. In the single-processor architecture, the large number of memory cells match with the concentration operation, the processing efficiency is not high. Although you can use some efficient matching algorithm, but performance is still not obvious. Taking into account the actual processing, sensor computing on the concentration of memory cells is different data collection operation by the same rules to do so, the system uses parallel processing of multiple sensor approach to each sensor must the size of a collection of immune cells, so a single sensor only focus on dealing with a station or a few memory cells within the host monitoring the concentration of antibody concentration by calculating the parallel method to improve the assessment of efficiency.

Device is based on dynamic risk assessment data generated by sensors throughout the network environment of the current risk calculations. Since different sensors have been designated part of the host data were treated in the calculation of network risk, completed by the Perception classification of risk related to the host and the host overall risk calculation. Dynamic risk assessment of each sensor device according to the host computing risk, calculate the overall risk of the current network to further improve the efficiency of risk calculation.

1) Distributor

Distributor is responsible for the IDS module generated by this event to the appropriate sensor. To describe the function of this part, make the following definition:

Let src_ipaddr and dst_ipaddr represent the data packet source and destination addresses and gene on behalf of the characteristics of the packet, the event e defined as triples $< src\_ipaddr, dst\_ipaddr, gene >$

Dispenser works can be expressed as:

$$core\_id = \begin{cases} f_{distribute}(e), & if \quad e.dst\_ipaddr \subset Host \\ 0, & otherwise \end{cases} \tag{1}$$

Sensor number is defined by $core\_id$,and $f_{distribute}(e)$ is the distribution function,and $Host$ is the set of hosts within the network monitored. Hash function uses the allocation method, the sequence of events from different hosts mapped to different sensors in the handle. When generating events The flow of data packets is monitoring network, that is $e.dst\_ipaddr \subset Host$, Using the distribution function to the event assigned to the appropriate sensor processing; the contrary, that the packet is not a threat to the current monitoring network, discard the event. Making the processed data for each sensor downsizing and focused only deal with a station or part of several host-related data for parallel processing of multiple sensor provides a premise.

2) Sensor

Sensor responsible for the completion of immune cells and non-self antigen (attack packets) of the match, the accumulation of memory cells in antibody concentration and attenuation calculation. For the purpose of computing defined as follows:

Let $gene$ represent for the characteristics of the memory cell antibody, $type$ for the antibody type, p on behalf of antibody concentration, age representative antibodies life cycle, the memory cells of the antibody can be expressed as quaternion: $< gene,type,p,age >$

Define the matching function as $f_{match}(e, Ag)$ .Antigens and antibodies to describe the matching process:

$$f_{match}(e,Ag)=\begin{cases}1, & if\ e.gene = Ag.gene\\ 0, & if\ e.gene \neq Ag.gene\end{cases} \tag{2}$$

For the input event e ,if antibodies are $c \subset C$ and make $f_{match}(e,c)=1$,then non-self-antibodies have been detected (attack packets).Then antibody c cloned copy of themslef, so the corresponding rise in antibody concentration. Matching algorithms such as formula (2), the concentration of additive processes such as formula (3).

$$\begin{cases}y(t).p = \eta_1 + \eta_2 \cdot y(t-1).p\\ y(t).age = 0\end{cases} \tag{3}$$

Parameters η_1 ,η_2 represent for initial concentration and reward factors, $y(t)$ for the concentration of antibodie at t time, which caculated from the previous time the number of Cloned $y(t-1)$. Otherwise the immune system detects that the current self-antigen (legitimate data packets), then the concentration of c antibodies should be correspondingly decay, decay, such as formula (4).

$$\begin{cases}y(t).p = \begin{cases}y(t-1).p\cdot(1-\dfrac{1}{\lambda' - y(t-1).age}), & y(t).age < \lambda'\\ 0, & y(t).age \geq \lambda'\end{cases}\\ y(t).age++\end{cases} \tag{4}$$

The parameter λ' said attenuation step, if the cycle of memory cells encounter antigen does not occur again,the corresponding antibody concentration will decay to 0.

The number of monitored hosts located h , and the number of memory cells at each host is c .If the network in the total number of memory cells is $h \times c$,each sensor is responsible for handling the memory cell number is: $(h \times c)/p$. Taking into account the concentration changes during operation, each sensor can run independently, does not require sensors to communicate with each other simultaneously, and thus the speedup can be obtained To: $s = t_s / t_p = (h \times c)/((h \times c)/p) = p$,which have linear speedup, efficiency improved significantly. Even in the worst case, only one host continued to suffer from a type of attack, as the attack information has been mapped to a particular sensor and the sensor is only the total number of immune cells within the immune cell numbers of all , The concentration of antigen and antibody accumulation matched the efficiency of the operation is still very high.

Risk calculation in each cycle of arrival, each sensor only the internal memory of the host cell concentration data, the corresponding risk classification of hosts and host the host the calculation of overall risk. Conducted with the sensor changes in the concentration of memory cells operating as a step in the sensor can be carried out independently in each sensor without the need for communication and interaction between, you can get linear speedup. Dynamic risk assessment devices to collect their hosts and host the overall risk classification of risk data, unified calculate the overall risk of the current network.

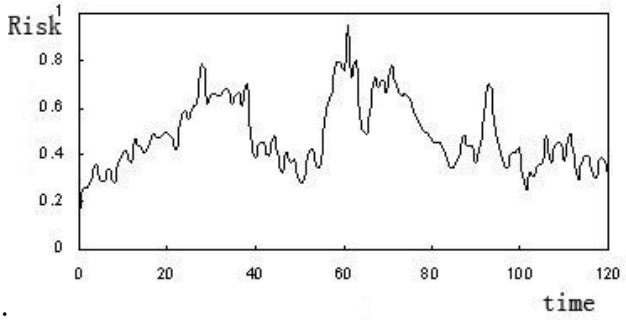
3. Experiment

To assess the effectiveness of the proposed model, based on the framework shown in Figure 1 Construction of a simulation system.

Experimental Platform: cavium's OCTEON CN3860 series of multi-core network processing platform, including 16 cn-MIPS64 processor, clocked at 550MHz, 4G memory, eight 1000Mb/s Ethernet ports, 250G hard drive. To generate real-time high-speed environment, the use of Blade Inc's Blade Informer send test data, IDS module using Snort. The core test platform, distributed as follows: Core0 running IDS, Core1-Core4 run four sensors.

Experimental parameters: the number of sensors is 4,and detect the 40 host.Each host's immune cells used to monitor is 2000 .Initial concentration is 0.001 and reward factor is 0.998 ,and attenuation step is l00. Host

to monitor the use of Blade Informer send dos, backdoor attack packets, etc., recorded attack strength, and will be measured in real time with the actual risk profile comparison of network attack power.



Results:

Figure 3. Host A's risk curve of dos attack

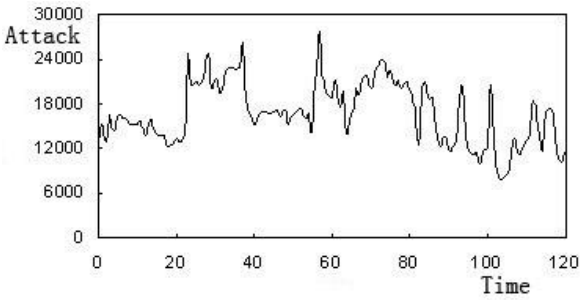


Figure 4. Host A's intensity curve of dos attack

Figure 3 suffered by the host A dos attack power, Figure 4 A according to the formula for the host (5) calculated value for the risk of dos attacks. Comparisons of the two figure shows, when the attack occurred, with the attack intensity increases, the corresponding increase in risk index synchronization; when the attack power reduced, the corresponding risk indicators also simultaneously reduced, and the intensity of attacks at the highest value and highest risk time base synchronization.

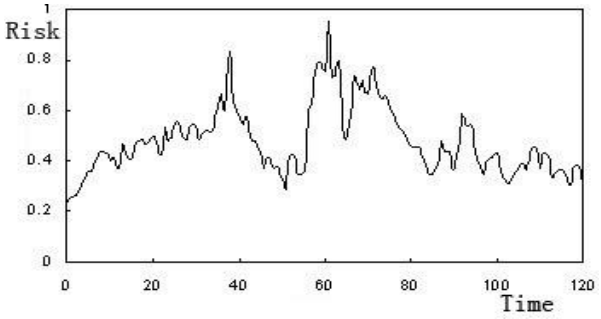


Figure 5. Host A's risk curve of variety of attack

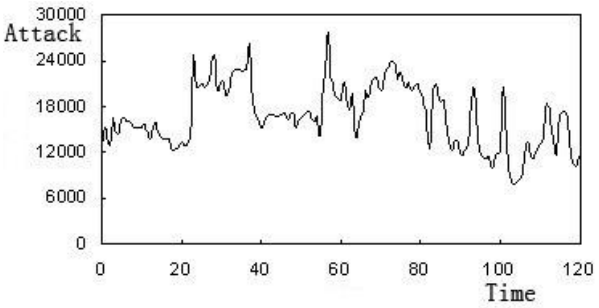


Figure 6. Host A's intensity curve of variety of attack

Figure 5 indicates that the host A variety of attacks suffered by the intensity curve, while Figure 6 was based on formula (6), calculated as the variety of attacks faced by the value of the overall risk of the host. Comparison shows two graphs, when the attack occurred, with the attack intensity increases, the

corresponding increase in risk index synchronization; when the attack power reduced, the corresponding risk indicators also simultaneously reduced, and the intensity of attacks at the highest value and highest risk time base synchronization.

4. Conclusions

The model proposed by this paper assess real-time network risk based on the principle of the body's immune. It take the result of the high-speed processing IDS as external antigen and complete the cloning process of the immune cells based on immune theory. Then it use the concentration of the immune cells to calculate the real-time risk of the network. At the same time, taking into account the traffic network and system in a large number of memory cells are more efficient in case of detection, the model uses multiple parallel sensors. each sensor handled by reducing the scale of the task based on this real-time assessment capabilities to improve system . Simulation results show that the proposed model can effectively evaluate the current network of real-time risk of a large flow traffic and is a practical strong network risk assessment model.

5. References

[1] National Computer Security Center, Dept of Defense, no. DoD 5200.28.STD, Trusted computer system evaluation criteria[S]

[2] ISBN 92-826-7024-4, Information technology security evaluation criteria: provisional harmonized criteria[S].

[3] Wang Yifeng, Li Tao, Hu Xiaoqin, Song Cheng. Based on artificial immune network security risks in real time detection method [J]. Electronics. 2005.

[4] Li Tao. Based on immune network security risk detection [J]. Science in China Series E Information Science. 2005.

[5] Li Tao. Computer Immunology [M]. Beijing: Electronic Industry Press. 2004

[6] Li Tao, "An Introduction to Network Security" [M]. Beijing: Electronic Industry Press, November 2004

[7] Sarafijanovic and J Boudec. An artificial immune system approach with secondary response for misbehavior detection in mobile ad-hoc networks. Technical Report IC/2003/65, Ecole Polytechnique Federale de Lausanne, 2003.

[8] Farmer J D, Packard N H, Perelson.A. S. The Immune System, Adaption, and Machine Learning[J]. Physica, vol.22d, 1986

[9] Hoffmann G W. A Neural Network Model Based on the Analogy with the Immune System[J]. Theory Biology, vol.122, 1986

[10] Liang Kexin, Li Tao, et al. A new theory based on artificial immune based intrusion detection model [J]. Computer Engineering and Applications, 2005.2