2012 4th International Conference on Computer Engineering and Technology (ICCET 2012)
IPCSIT vol.40 (2012) © (2012) IACSIT Press, Singapore

Intrusion Detection Based on the Danger Theory of Digital Differential

Hui Fang

School of Computer, Wuhan University, 430072,
Hubei China
fanghui@whu.edu.cn

Abstract. Artificial immune theory is an important method of intrusion detection system, the immune system includes the innate and adaptive immune two-tier, reverse the selection model draws on the mechanism of the adaptive immune system, however, how to distinguish between the mass of the Self and Nonself is the plight of reverse selection theory. Risk theory is to explain the doctrine of the innate immune system works, just concerned about whether the system is "dangerous" can be. Presenting danger signals is the main problem to solve a dangerous theory. This article draw on the mathematical description of the function changes in law, borrowed the concept of the differential description of the computer system changes, defined on this basis and expression of danger signals, as a sign of intrusion detection. Finally, a simulation test to prove the feasibility of this model in the judgment of the sudden invasion.

Keywords: IDT, AIS, IDS.

1. Introduction

With the rapid development of computer network applications, network security issues become increasingly prominent. Although most known attacks based on the traditional IDS (of Immune danger theory) [1] can be detected, but unable to do anything but unknown intrusion; intrusion detection system based on artificial immune principle [2-3] is able to identify unknown attacks, but there are problem [4-5]: (1) from the body and non-self is difficult to accurately distinguish between the dynamic conversion render the system difficult to achieve; (2) as time grows, autologous library will become very large, autologous tolerance time will increase exponentially.

The immune risk theory suggests that the immune system immune response based on the danger signals, without regard to autologous and autologous tolerance problems to solve based IDS problems of traditional AIS (artificial immune system) provides an important theoretical tool. This paper presents a new network intrusion detection method based on Immune Danger Theory (IDT). For the establishment of an adaptive, the dangerous theory of the diversity of the immune model, reflecting the inherent intelligence of the immune model, danger signals and artificial antigen presenting cells for the main object of study, focused on solving the problem of the danger signals of presentation and risk perception proposed a solution can be achieved, and as a basis to determine network behavior.

2. Intrusion Detection System Based on Danger Theory

Computer immune system is to learn from the immune system works a biomimetic method is an adaptive defense system. The immune system consists of innate and adaptive immune two-tier computer immune system involved in this two-tier.

Dangerous mode theory (referred to as the dangerous theory) to explain the doctrine of the innate immune system works, in accordance with the view of the danger theory, the immune system function is found on the system, potential hazards, to maintain system balance, to prevent or delay a change of state.

For the establishment of an adaptive, the dangerous theory of the diversity of the immune model, reflecting the inherent intelligence of the immune model, danger signals and artificial antigen presenting cells for the main object of study, focused on solving the problem of the danger signals of presentation and risk perception, a solution can be achieved.

In order to solve the problem of risk perception, learn the functions and principles of the antigen-presenting cells, building artificial antigen presenting cells, used to identify the fusion of danger signals from fragmented micro danger signals, refining the macro system status, and risk awareness. This paper discusses the structure of the artificial antigen presenting cells, workflow and life cycle; focused on the key components of the antigen-presenting cells recognize the danger signals - Toll-like receptors in the role, structure and related algorithms.

3. Theoretical model based on the theory of numerical differentiation of immune danger

3.1. The basic idea

Based on the study of biological immunity, 1994 Polly Matmger immune dangerous theory (of Immune Danger, Theory, IDT) [6-7]. The theory is that the appropriate protection mechanisms in the sensitivity of the immune system to feel the danger signal, danger signal generation and detection is closely related to the immune biochemical reactions, and immune response is a response to changes in cell number. The immune risk theory is that these mechanisms lead to quantitative changes caused by different biochemical reactions, biochemical reactions will produce different levels of danger signals, these signals constitutes the basis of the immune response. Immune risk theory and immune theory in the IDS application, the main theoretical difference can be such as shown in Table 1.

Table 1 IDT IDS and traditional AIS-based IDS basic concepts of control

Biological immune system	Immune dangerous theory IDS	Traditional immune theory IDS
Cell	Network behavior	Attack or detector
Antibody	Characterization of a class I antigens and its structure the same binary code	Able to identify antigens and its structure the same binary code
Gene	The most basic unit of antibody, antigen, is also a variation of the unit	The most basic unit of antibody, antigen, is also a variation of the unit
Changes in cell number	Abnormal network behavior	The corresponding concept
The relationship between antigen and antibody	Antigen to stimulate antibody production	Antibody antigen recognition
The concentration of antibody	Danger signals of the corresponding antigen	Specific antigen attack that

3.2. Basic concept

3.2.1 Antigens and antibodies

Antigen and antibody immunity concept, mentioned in this article comply with Perelson and Oster in 1979, the shape space model. On this basis, using a binary string that antibody Ab and the antigen of Ag.

For binary coding, the antigen Ag B, where B = {0,1} length on behalf of all the collection of length is the length of the binary string consisting of the antigen Ag composed by m feature gene segment (gene), the collection of antigens in the system Ag, such as formula expressed as

$$Ag = \begin{pmatrix} ag_1 \\ ag_2 \\ \vdots \\ ag_n \end{pmatrix} = \begin{pmatrix} ag_{11} & ag_{12} & \cdots & ag_{1m} \\ ag_{21} & ag_{22} & \cdots & ag_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ ag_{n1} & ag_{n2} & \cdots & ag_{nm} \end{pmatrix} \tag{1}$$

Among them, the l_j is the length of the ag_{ij}. Formula (1) of ag_i, said the i antigen, ag_{ij} the j-th gene component in the i antigen.

Antigen and antibody has the same structure, composed by the gene segment. Antibody collection of Ab for

$$Ab = \begin{pmatrix} ab_1 \\ ab_2 \\ \vdots \\ ab_n \end{pmatrix} = \begin{pmatrix} ab_{11} & ab_{12} & \cdots & ab_{1m} \\ ab_{21} & ab_{22} & \cdots & ab_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ ab_{n1} & ab_{n2} & \cdots & ab_{nm} \end{pmatrix} \tag{2}$$

Formula (2), ab_i said the i-th antibody, ab_{ij} the j-th gene component of the antibody, i=1,2, ..., k: j = 1,2, ..., m.

3.2.2 danger signals

From the method and categories of danger signals in the body can be seen, the danger signals have the following characteristics:

The danger signal is the endogenous signal that it is released by damage to the body itself. Broad, PAMPs also can be used as a dangerous signal, said that the distinction between, known as exogenous danger signals.

Danger signals the body's balance is destroyed. DAMPs release in the body damage to internal and external environment of the body damaged cells will change, forcing some of the material does not show up in the normal state appears. The danger signals is the key to start the adaptive immune response, is a dangerous theory must focus on the core content.

3.2.3 Antigen presenting cells

The danger theory is to explain the immunization process: the damage of living organisms to release danger signals, antigen-presenting cells to receive danger signals, refining and conversion costimulatory signal. Costimulatory signals and antigen-activated T-helper cells, activated T-helper cell activation of B lymphocytes or T-killer cells, and immune response.

The surface of antigen presenting cells capture antigen receptor and expression of TLRs receptors receiving danger signals present antigen fragments major histocompatibility complex (Major Histocompatibility Complex, MHC) molecules and costimulatory signals. APC is a signal processing module. The input value is a danger signal, the output value of costimulatory signals and antigenic fragments.

3.2.4 The definition and expression of danger signals

The danger signal is the imbalance in the system variables and system-changing collection of DS = {dsi | i ∈ N}, it is a subset of the system variables change DS ⊆ the dV.

the changes of system variables deemed as "possible" danger signals, DS=dV, the screening of dangerous irrelevant variable changes by artificial APCs cell population and the natural evolution of the TLRs receptors and identify the complete the natural evolution of with the group algebra of the change, the change has nothing to do with the danger will be eliminated, not to be identified.

Learn from the methods of numerical differentiation, the derivative, differentiate the process of discretization. According to the numerical differentiation method of calculation, respectively, the forward difference, backward difference and central-difference approximation, given in this paper the expression of danger signals DS are as follows, where R is the frame of reference:

$$DS = dV = \{dv_1, dv_2, \ldots, dv_n\} = \{dg_1(R), dg_2(R), \ldots, dg_n(R)\}$$

The danger signal is a collection of multiple system variables change value. The light of the numerical differentiation method of calculation, we can use the value of the forward and backward, the central difference method of expression of danger signals.

(1) the danger signals of the forward difference approximation of the expression:

$$ds_i \approx g_i(R_{i+1}) - g_i(R_i)$$

$$DS \approx \{(g_1(R_{i+1}) - g_1(R_i)), (g_2(R_{i+1}) - g_2(R_i)), \ldots, (g_n(R_{i+1}) - g_n(R_i))\}$$

The ds_i said the danger signals of a specific system variables, DS said that the entire collection of the danger signals.

(2) the danger signals of the backward difference approximation of the expression:

$$ds_i \approx g_i(R_i) - g_i(R_{i-1})$$
$$DS \approx \{(g_1(R_i) - g_1(R_{i-1})), (g_2(R_i) - g_2(R_{i-1})), \ldots, (g_n(R_i) - g_n(R_{i-1}))\}$$

(3) danger signals of the central-difference approximation to express

$$ds_i \approx \frac{g_i(R_{i+1}) - g_i(R_{i-1})}{2}$$
$$DS \approx \left\{ \frac{(g_1(R_{i+1}) - g_1(R_{i-1}))}{2}, \frac{(g_2(R_{i+1}) - g_2(R_{i-1}))}{2}, \ldots, \frac{(g_n(R_{i+1}) - g_n(R_{i-1}))}{2} \right\}$$

In this paper, the expression of danger signals is the backward difference approximation expression

4. Structure of the artificial antigen cell presenting cells

The definition of danger signals, expression and extraction is computer immune model based on danger theory which must be resolved

The first key issue. The state of the system is formed by a large number of microscopic danger signals together to a common decision. To achieve risk

Risk perception needs to be integration of these danger signals, composed of a costimulatory signal to start the adaptive immune response, the artificial antigen mention

Cell, which receives the stimulus of danger signals and to provide costimulatory signals to lymphocytes. Which bears the fusion of danger signals, sub-contractors

Set a dangerous state, start the task of the adaptive immune response.

Table 2 The reference group and the latency software group alarm contrast to the situation

	Reference group		Latent software group	
Groups	Normal	Notepad	Spybot	Worm.Win32.Smelles
Time	10:00~10:05	14:47~14:53	17:35~17:44	18:59~19:00
Length	4:45	6:00	9:00	3:00
APCs algebra	58	72	102（31~133 generations）	36（36~72 generations）
Alarm the number of	5	7	23	35
Alarm rate	8.6%	9.7%	22.5%	97.2%
Alert TLRs distribution	ARP CPU Usage ICMP File Keylogger	Keylogger ICMP File ARP CPU Usage	CPU Usage File Keylogger Scoket	CPU Usage

Immune in the APC surface by MHC molecules and pattern recognition receptors constitute. The main function of MHC molecules presenting cells, the main function of the pattern recognition receptors to identify the danger signals (DAMPs) or pathogen-associated molecular patterns (PAMPs). Identify the danger signals of pattern recognition receptors TLR2 and TLR4 are two kinds of different types of TLRs receptor recognition of the danger signal types differ. Artificial APC contains three main parts: (1) (2) of TLRs APC_Adaption (3) APC_Serial are TLRs receptors, the fitness value of the APC and the APC number. Fitness value with the danger signal to identify the concentration of APC recognize the danger signals, the adaptation value. When the fitness value exceeds the migration threshold APC produce costimulatory signals, otherwise keep resting.

5. Experiments and results analysis

Experimental Objective: To validate the danger theory of immunity model proposed in this paper, the feasibility of the discovery of latent software. Including the feasibility and risk perception of the danger signals offered (ie, costimulatory signal generator) feasibility.

The experimental procedure: The experiment was divided into four groups. Among them, the length of time for the Normal group collected data for 4 minutes and 45 seconds during the APCs population change of 58 generations. Group Worm.Win32.Smelles the total time of data acquisition was 9 minutes, APCs and a total of 107 generations, and Spybot similar, only the time of implantation of worms, so take the time to 3 minutes, APCs and population change of 36 generations.

Results: Contrast latent software implanted with no latent software implanted, the system generates an alarm condition. The obtained experimental results as shown in Table 2.

Latent software group, the alarm rate is higher than the reference group can be seen from Table 2. And by observation of the alarm

Police, can be found, the alarm in the reference group is sporadic, there is no aggregation, and alarm distribution of TLRs was

V software group, the relative concentration of alarm.

Worm group, the alarm is very concentrated, and the continuous and large. The cause of the alarm is basically caused by the CPU Usage. This is because the worm at runtime CPU-intensive.

6. Conclusion

Latent software - zombie program Spybot and the worm Worm.Win32.Smelles example, in two computer systems as a reference to Notepad and do not run the normal procedure for any additional procedures to verify the danger signals presented in this paper to present and dangerous perception method inlatent software found in the feasibility of the proposed model since the adaptability and diversity. Experimental results show that the risk of the proposed theoretical model can be found lurking software, and the discovery of the potential of the different categories of software, of TLRs receptors are quite different in the proportion of receptor types and the proportional distribution of TLRs, can roughly determine the latent software type and hazard intensity. During the experiment, to identify the proportion of certain types of danger signals of TLRs receptors to improve decreased, and vice versa. This shows the type and intensity of the danger signals with different system state and adaptive, and thus artificial APCs also will be adjusted adaptively. Verify that the risk of the proposed theoretical model has better adaptability.

7. References

[1] DASGUPTA D. Advances in artificial immune systems [J]. Computational Intelligence Magazine, IEEE, 2006, 1(4): 40-49.

[2] HOFMEYR S, FORREST S. Immunity by Design: An Artificial Immune System[C] // Proceedings of the Genetic and Evolutionary Computation Conference(GECCO). San Francisco, CA: Morgan-Kaufmann, 1999: 1289-1296.

[3] HOFMEYR S, FORREST S. Architecture for an Artificial Immune System[J]. Evolutionary Computation, 2000, 7(1): 45-68.

[4] AICKELIN U, CAYZER S. The Danger Theory and Its Application to AIS [C] // 1st International Conference on AIS. 2002: 141-148.

[5] CAYZER S, AICKELIN U. Recommender System based on the Immune Network [C] // Proceedings of the2002 Congress on Evolutionary Computation (CEC2002). 2002: 807-813

[6] GALLUCCIS, MATZINGERP. Danger signals: SOS to the immune system[J]. Current Opinions in Immunology, 2001, 13:114-119.

[7] MATZINGER P. The Danger Model: A Renewed Sense of Self [J]. Science, 2002, 296: 301-305