Int. J. Communications, Network and System Sciences, 2009, 6, 569-574
doi:10.4236/ijcns.2009.26063 Published Online September 2009 (http://www.SciRP.org/journal/ijcns/).

A Network Intrusion Detection Model Based on Immune Multi-Agent

Nian LIU[1,2], Sunjun LIU[3], Rui LI[3], Yong LIU[4]
[1]*College of Computer Science, Sichuan University, Chengdu, Sichuan, China*
[2]*School of Electrical Engineering and Information, Sichuan University, Chengdu, Sichuan, China*
[3]*The software engineering college of Chengdu University of Information Technology, Chengdu, Sichuan, China*
[4]*Chengdu Institute of Computer Applications, Chinese Academy of Sciences, Chengdu Sichuan, China*
Email: *liusunjun@163.com*
Received March 18, 2009; *revised May* 5, 2009; *accepted June* 18, 2009

ABSTRACT

A new network intrusion detection model based on immune multi-agent theory is established and the concept of multi-agents is advanced to realize the logical structure and running mechanism of immune multi-agent as well as multi-level and distributed detection mechanism against network intrusion, using the adaptability, diversity and memory properties of artificial immune algorithm and combing the robustness and distributed character of multi-agents system structure. The experiment results conclude that this system is working pretty well in network security detection.

Keywords: Artificial Immune, Intrusion Detection, Multi-Agent System,

1. Introduction

Along with the rapid development of network technology and fast upgrade of network attack technologies network security has become the focus of this age. However, current intrusion detection technologies [1,2], like statistical analysis, characteristics analysis and expert system etc, can not meet well all the needs. Firstly, the lack of adaptability makes it difficult to detect unknown attacks; Secondly, the lack of robustness leaves each part isolated without communication. Therefore, the building of a detection system with adaptability and robustness is in pressing needs.

Biological Immune System [3] identifies and eliminates foreign bodies intruding into the organism by immune cells. From the aspect of information processing, BIS is a distributed autonomic system and its self-learning, adaptability and robustness serve as important inspirations for the solving of network security problems. In 1974, Jerne [3] brought forth the first mathematical model in immune system, later in 1994, Forrest [4] put forward the concept of computer immune system for the detection of network intrusion, and up to now the artificial immune system based on biological immune theory has been applied extensively in network security.

Agent [5] refers to such entity as possessing perceiving, analyzing and reasoning mechanism. Multi-agent [5,6] system, with fairly strong distributed character, robustness and coordination, realizes problem solving under complicated environment by harmonizing the interaction and cooperation among various separate Agents.

In this article, a new network intrusion detection model based on immune multi-agent (NIDIMA) is established and the concept of immune multi-agent is advanced in the building of logical structure and running mechanism of immune multi-agent to realize multi-level and distributed detection mechanism against network intrusion. This model provides a new way in network safeguard and proves to be an effective solution to network security detection throughout the experiment.

2. System Principles of the Detection Model Based on Immune Multi-Agent

Apart from inheriting the original characteristics of Agent, immune agent also has the characters of evolution, diversity, tolerance and detection [7,8] properties etc.

1) Evolution: Following the evolution law, IA activates antibodies, which can effectively recognize antigens, into higher form, while eliminates the inefficient one. In this way, the self-learning ability of detection is realized.

2) Diversity: The matching of antibodies and antigens adopts fuzzy matching [9], with just the need to meet the preset value. The incomplete matching, which realizes the diversity of recognition, enables immune antibodies to recognize various kinds of antigens and in this way, it can produce antibodies covering the whole form space in theory.

3) Tolerability: Immune tolerability refers to the non-response status of immune cells towards the peculiarities revealed by certain kinds of antigens [10]. The tolerability of IA is of great significance in the maintaining and balancing of the model.

4) Detection property: The immune system transmits the produced immune cells within each organ in vivo to increase immunologic competence. Network security model based on this mechanism is of great detection ability.

Combined with multi-agent and AIS technology, the detection model constitutes a multi-direction and multi-level intelligent network security model, with its mapping relationship with BIS model as shown in Table 1, and its system structure diagram as shown in Figure 1.

The model adopts large-scale and distributed system structure, and a series of network situation awareness agents and a network security situation evaluation agent is deployed in target networks and its host computer firstly.

Security situation evaluation agent gathers information about the security situation of subordinate subnets and host computers from each security situation awareness agent to evaluate about the whole integrated risks to the whole network, and the information includes the type, quantity, strength and harmfulness of the attacks.

The network security situation awareness agent shown in Figure 1 is itself a sub-network security situation awareness system, defined by recursion, and it mainly monitors on the sub-network security situation within its control, and specifically speaking, real-time monitor on the type, strength and harmfulness of attacks suffered by sub-network. Because there might as well be subnets under subnets, sub-network security situation awareness agents may be composed of sub-network security situation awareness agents at lower level. Eventually, security situation awareness agents, that monitor the specific host computer, are made up of intrusion detection and security situation evaluation of the host computer.

In this architecture, IA distributed at host computer node starts to recognize the intruded events at first, and in case unknown attacks are discovered through learning and memory, information will then be sent to corresponding SMC, while vaccines that has identified new attacks will be distributed to each node within the same network segment to improve the intrusion defense capability of each node. SMC makes analysis on the intrusion information sent by each IA in the network segment and SMC of suffered network segment will send vaccines to

Table 1. The relationship between the BIS and the NIDIMA.

Biological immune system	Network intrusion detection system
Organism	Network
Organ	Network segment
Cell	Host computer
Vaccine distribution	The transmission of intrusion information
Antigen	The binary character string feature-extracted from IP packets
B Cell, Antibody	Antibodies represented in binary character string
Cell clone	Duplication of antibody

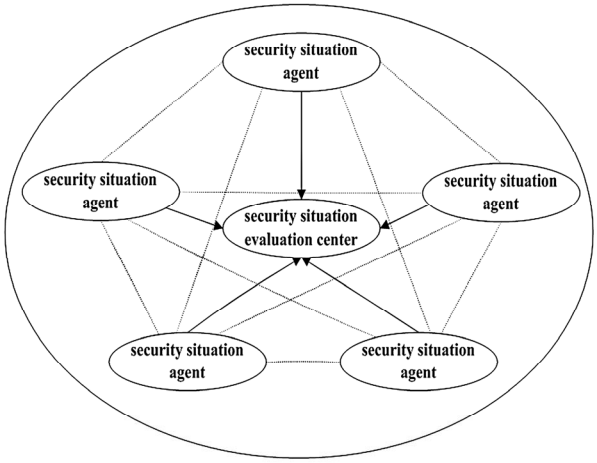

Figure 1. Architecture of NIDIMA.

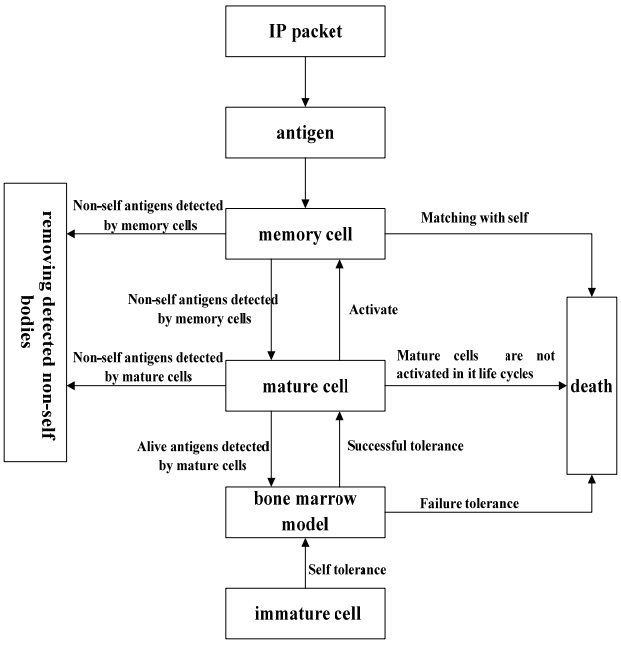

Figure 2. Architecture of immune agent.

other non-intruded network segments for early warnings for the realization of whole detection.

3. System Mechanism of the Network Intrusion Model Based on Immune Multi-Agent

In Figure 2, the logical structure of IA is shown, which includes self antigens, immature immune antibodies, mature immune antibodies and memory immune antibodies etc. The working procedures involve two interplaying and concurrent circulations, which are the circulation of immune antibodies' detection of external antigens and the circulation of immune antibodies' evolution.

3.1. The Definition of Immune Elements

Definition 1: Antigens are binary character strings in the length of l that are feature-extracted from network IP data packets. Let $U=\{0, 1\}^l$ ($l>0$), antigen assembly $Ag \subset U$, it mainly includes IP address, port and protocol type etc.

$$Ag = \{< a,b > | \, a \in D \wedge b \in \Psi \wedge |a| = l \wedge a = APCs(b)\} \quad (1)$$

Definition 2: The antigen assembly Ag is classified into two substes of self assembly *Self* (normal network behavior) and non-self assembly *Nonself* (abnormal network behavior):

$Self \cup NonSelf = Ag$, $Self \cap Nonself = \varnothing$

Antibodies and antigens have binary character strings of the same features and length, the definition of antibody assembly $B \subset U$:

$$B = \{Ab | \, Ab = <s, age, count, ag>\} \quad (2)$$

Antibody Ab is a quadruple, among which s means binary string in the length of l, *age* is the age of antibody, *count* is the quantity of antigens matched with antibodies, *ag* is the antigens that are detected by the antibodies. Antibodies are classified into three categories: mature antibodies, memory antibodies and immature antibodies. Mature antibodies, tolerable to self bodies, refer to the antibodies that are not activated by antigens, mature antibodies assembly $T_{Ab} \subseteq U$; memory antibodies evolve from mature antibodies that are not activated, memory antibodies assembly $M_{Ab} \subseteq U$; immature antibodies are antibodies that have not undergone self-tolerance, immature antibodies assembly $I_{Ab} \subseteq D$.

Definition 3: Affinity serves as the main evidence to judge the matching state between antibodiesand antigens, and the calculation formula is as Formula (3), equaling to 1 means matching, or else non-matching. In the formula, $x \in Ag$, $y \in B$, x_i, y_i are the *i-th* characters of x, y respectively, l is the length of character string, θ is the threshold value of affinity matching.

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

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

3.2. The Changing Process of Immature Antibodies

Let I be the number of immature antibodies included in I_{Ab} at certain time, the dynamic changing formula of immature antibodies assembly is:

$$I(t+\Delta t) = I(t) + I_{new} \cdot \Delta t - (\frac{\partial I_{mature}}{\partial x_{mature}} \cdot \Delta t + \frac{\partial I_{dead}}{\partial x_{dead}} \cdot \Delta t \quad (4)$$

The Formula (4) indicates that the changing process of I_{Ab} assembly is divided into 2, that is, inflow and outflow. Inflow is the process of newly produced immature antibodies' joining in I_{Ab} assembly: $I = I_{new} \times \triangle t$, I_{new} means the production rate of immature antibodies per unit of time. Outflow is the process of removing immature antibodies from I_{Ab} assembly, and there are two directions of outflow: the quantity of immature antibodies decreased out of successful tolerance and evolution into mature antibodies is presented by

$$\frac{\partial I_{mature}}{\partial x_{mature}} \cdot \Delta t \text{ , and } \frac{\partial I_{dead}}{\partial x_{dead}} \cdot \Delta t$$

presents the quantity of immature antibodies decreased out of tolerance failure.

In order to avoid matching between antibodies and self bodies, newly produced immature antibodies can only match with antigens after passing self tolerance. The tolerance process is shown as in Formula (5), and 1 means passing self tolerance, 0 means failure of self tolerance, $x \in I_{Ab}$.

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

3.3. The Changing Process of Mature Antibodies

Let T represent the number of mature antibodies included in T_{Ab} at certain time, and the dynamic changing formula of mature antibodies assembly is:

$$I(t+\Delta t) = I(t) + I_{new} \cdot \Delta t - (\frac{\partial I_{mature}}{\partial x_{mature}} \cdot \Delta t + \frac{\partial I_{dead}}{\partial x_{dead}} \cdot \Delta t) \quad (6)$$

the Formula (6) indicates that the changing of T_{Ab} assembly is divided into two processes: inflow and outflow. The inflow is the process of antibodies' joining the T_{Ab},

and there are two ways: The number increased out of immature antibodies' successful tolerance and evolution is represented by

$$\frac{\partial T_{tolerate}}{\partial x_{tolerate}} \cdot \Delta t \; ; \quad \frac{\partial T_{clone}}{\partial x_{clone}} \cdot \Delta t$$

means the number increase out of clonal selection of memory antibodies. Outflow is the process of removing mature antibodies, it also has two directions: the number of memory antibodies that have been evolved from activation is presented as

$$\frac{\partial T_{active}}{\partial x_{active}} \cdot \Delta t \text{ , while } \frac{\partial T_{dead}}{\partial x_{dead}} \cdot \Delta t$$

represents the number that die from failed activation.

The mature antibodies assembly T_{active} that have been activated and evolved into memory antibodies is shown in Formula (8), and the mature antibodies assembly T_{dead} that have failed in activation is shown in Formula (9), among which β is activation threshold, and λ is the life cycle of mature antibodies.

$$T_{active} := \{x \mid x \in T_{Ab} \wedge x.count \geq \beta \wedge x.age \leq \lambda\} \quad \textbf{(7)}$$

$$T_{dead} := \{x \mid x \in T_{Ab} \wedge x.count < \beta \wedge x.age > \lambda\} \quad \textbf{(8)}$$

3.4. The Changing Process of Memory Antibodies

Let M as the memory antibodies quantity contained in M_{Ab} at certain time, and the dynamic changing formula of memory antibodies assembly is:

$$M(t+\Delta t) = M(t) + \frac{\partial M_{active}}{\partial x_{active}} \cdot \Delta t + \frac{\partial M_{bacterin}}{\partial x_{bacterin}} \cdot \Delta t \quad \textbf{(9)}$$

Because memory antibodies have infinite life cycle, the change of M_b assembly only has the process of inflow, without the outflow process of dead memory cells. The inflow of memory antibodies is conversed by activated mature antibodies T_{active},

$$\frac{\partial M_{active}}{\partial x_{active}} \cdot \Delta t = \frac{\partial T_{active}}{\partial x_{active}} \cdot \Delta t$$

3.5. Immune Surveillance

During the detection process of IA on network behaviors, it mainly adopts mature cells and memory cells to detect antigens, and it is capable to detect non-self antigens efficiently and rapidly, what follow are the detailed steps:

1) Antigen presentation: The feature information of IP packet is extracted from actual network data flow to constitute a binary string in the length of *l,* which is then put in the antigen assembly *Ag* as antigen regularly.

2) Using memory antibodies M_{Ab} to detect antigens: Non-self bodies that match with memory antibodies are removed, and memory antibodies that have detected self bodies in are also removed.

3) Using mature antibodies T_{Ab} to detect antigens: The non-self antibodies that match with T_{Ab} are removed, and the T_{Ab} that has detected enough antigens in the life cycle is then activated and evolved into memory antibodies M_{Ab}; The M_{Ab} that has not been activated or detected self elements in life cycle will die.

4) Self body assembly upgrade: After detection, the left antigens will join in self body assembly, maintain dynamic self body upgrading, undergo self tolerance with immature antibodies and maintain dynamic evolution of antibodies.

4. Simulation Experiment and Result Analyse

4.1. Experiment Environment and Parameter Settings

The experiment environment is classified into two network segments of A, B, and composed of 20 host computers of the same configuration. A_i, B_i ($1 \leqslant i \leqslant 20$) means the *i-th* host computer in A, B segments respectively. The experiment applies part of the data from KDDCUP99 [11] in MIT LINCOLN lab as training and test data. The training set is normal network data without any attack, and the test set includes normal data and attack data. The attack data is classified into 4 categories: DoS, Probe, U2R, R2L. The test data I includes guess_ passwd, buffer_overflow and other attacks, 7 in total, and the test set Ⅱ includes the attacks in test set I and other 10 attacks or more, e.g. land, spy, perl.

Antigen data architecture is composed of source, destination IP address, port number, protocol type, IP tag field, IP packet length and TCP/UDP/ICMP domain etc, l = 172, affinity matching threshold value θ =0.7.

4.2. Experiment Results and Performance Analysis

Activation threshold value β and life cycle λ bear large influence on TP and FP, the test performance of ADNIIMA, therefore, optimization test should be carried out. The experiment results are shown in Figure 3, when activation threshold value β is relatively small, and the mature antibodies are activated without thorough learning, FP is relatively bigger; when the life cycle λ is relatively small, the mature antibodies will die without activation and the memory antibodies will be scarce, which in total may cause TP lower. Along with the increase of β and λ, TP increases and FP decreases. However, when β and λ are too big, TP decreases instead and FP increases. After through analysis, it is found

Table 2. Experiment data list.

Attack Type	Training set		Test set I		Test set Ⅱ	
	Attack Times	Attack Type	Attack Times	Attack Type	Attack Times	Attack Type
Normal	18300	0	17500	0	14400	0
DoS	4580	1	5140	2	5580	5
Probe	1250	1	2700	2	4240	4
U2R	560	1	650	2	420	4
R2L	290	1	300	1	360	3

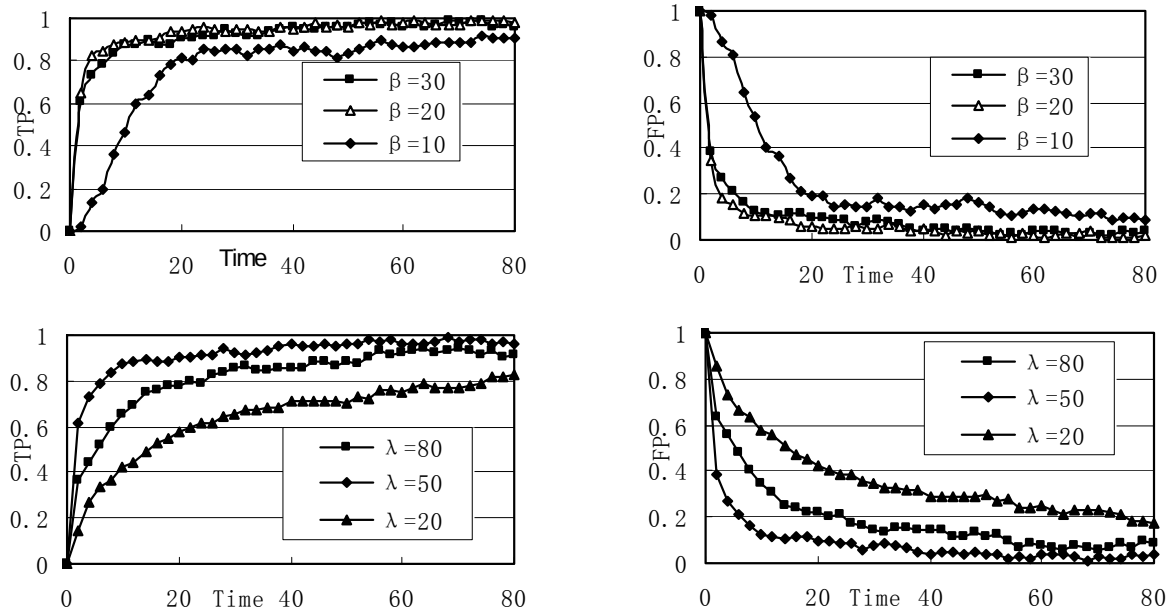

Figure 3. Effect of the activation threshold β and the lifecycle λ.

out that when β =20, λ =50, FP<6%, TP>93%, the effect is better.

In Table 3 and Table 4, the comparison test results of this model and the detection tools matched with the patterns based on, BRO [12], are listed, and from the tables we can infer that the detection model is of higher TP and lower FP, and the types of recognized unknown attacks are more than that of BRO, which demonstrates that this model is of high self-learning and adaptability.

In Table 4, TP and FP curves of host computer A_2 with self evolution and detection, and the host computer A_3, using vaccines emitted from A_1 for detection, are list respectively, and from the table we can conclude that in the later phase of experiment, the TP and FP curves of A_2 and A_3 are almost coincident. But in the early phase of the actual experiment, A_2, that relies on itself for detection, has low detection rate due to a lack of antibodies, and the attacks have made severe damage to the during this exact phase, which is unacceptable for key network node.

4. Conclusions

The active defense model for network intrusion based on artificial immune multi-agent put forth in this article has following advantages compared with other network intrusion defense techniques: 1) Self-learning; The memory mechanism and antibodies generation mechanism can not only detect well-known attacks, but also bear recognition ability towards unknown attacks. 2) Multi-level; The model has introduced in the concept of vaccine, which can strengthen network nodes and connection between each network segment. 3) Robustness; The model applies distributed system structure so that a single node under attack does not impact the detection abilities of other nodes. In a word, the experiment results reveal that the model differs greatly from the isolated and passive defense situation of traditional network security model, and it is a better solution to network security detection.

Table 3. Detection results of ADNIIMA model experiment.

Attack Type	Test Set I			Test Set Ⅱ		
	Recognition Type	TP (%)	FP (%)	Recognition Type	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 4. Detection results of BRO experiment.

Attack Type	Test Set I			Test Set Ⅱ		
	Recognition Type	TP (%)	FP (%)	Recognition Type	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

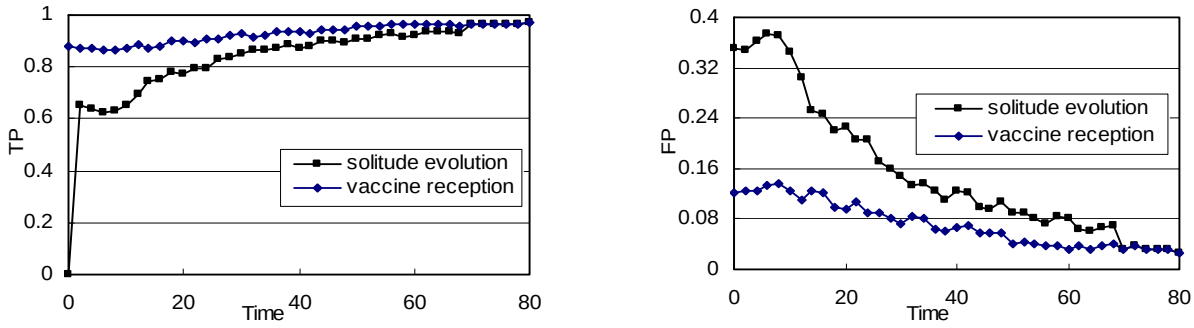

Figure 4. Comparison of detecting effect between solitude evolution and vaccine reception.

5. References

[1] Y. Bai, and H. Kobayashi, "Intrusion detection systems: Technology and development," IEEE Advanced Information Networking and Applications, pp. 710–715, 2003.

[2] A. Pilz and J. Swoboda, "Network management information models," Aeu-International Journal of Electronics and Communications, Vol. 58, pp. 165–171, 2004.

[3] Y. L. Dong, J. Qian, M. L. Shi, "A cooperative intrusion detection system based on autonomous agents," IEEE CCECE 2003, Vol. 2, pp. 861– 863, 2003.

[4] P. D'haeseleer and S. Forrest, "An immunological approach to change detection: Algorithm, analysis and implication," in Proceedings of IEEE Symposium on Research in Security and Privacy, Oakland, pp. 110–119, 1996.

[5] J. Kim and P. Bentley, "The artificial immune model for network intrusion detection," 7th European Congress on Intelligent Techniques and Soft Computing, 1999.

[6] P. K. Harmer and G. B.Lamont, "An agent based architecture for a computer virus immune system," Proceedings of the Genetic and Evolutionary Computation Conference, Orlando, Florida, USA, 1999.

[7] F. Esponda, S. Forrest, and P. Helman, "A formal frame work for positive and negative detection schemes," IEEE Transactions on Systems Man and Cybernetics Part B-Cybernetics, Vol. 34, No. 1, pp. 357–373, 2004.

[8] I. M. Hegazy, H. M. Faheem, T. Al-Arif, and T. Ahmed, "Evaluating how well agent-based IDS perform," Potentials, Digital Object Identifier, IEEE, Vol. 24, 27–30, 2005.

[9] P. Ballet and V. Rodin, "Immune mechanisms to regulate multi-agents systems," GECCO 2000, Las Vegas, Nevada, USA, July 2000.

[10] Z. Z. Shi, "Intelligent agent and its Application [M]," Science Press, Beijing, 2000.

[11] A Hofmeyr and S. Forrest, "Architecture for an artificial immune system," Evolutionary Computation, Vol. 7, No. 1, 2000.

[12] N. K. Jerne, "Towards a network theory of the immune system," Annual Immunology, Vol. 125, 1974.

