Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, 2015, *9,* 2597-2604

Open Access

A New Intrusion Detection Model Based on Artificial Immune Algorithm

Jian Liao*, Zhi Li and Zhimin Li

Hunan Mechanical & Electrical Polytechnic, Hunan, Changsha, 410151, China

Abstract: This paper introduces artificial immune to intrusion detection system through the analysis of the similarity of artificial immune and intrusion detection and puts forward a model of intrusion detection system based on artificial immune distributed agent. Firstly the system model structure is introduced and a hierarchical structure of intelligent agent is presented as well as a dynamic evolution model. At the same time a kind of vaccine immunization algorithm is put forward and network risk evaluation operator is given to evaluate real-time network security situation. This algorithm can keep the diversity of antibodies, and simultaneously has high convergence speed. The experimental results show that the proposed model has the feature of real-time processing that provides a good solution for heterogeneous fleet high-speed network environment.

Keywords: Srtificial immune, dynamic evolution, ıntrusion detection, network security.

1. INTRODUCTION

The security of computer network plays an important role in modern computer systems with the widespread use of network [1, 2]. Intrusion diction technology has become increasingly important in the area of network security research [3]. But the infrastructure of network becomes more complicated. More extensive application of distributed environment, mass storage, high bandwidth transmission speed and a few novel or cooperative intrusion happen constantly, which cause new interest in intrusion detection research [4, 5]. Soft computing is a novel method constructing computational intelligence system. How to construct high intelligent intrusion detection system is of great practical significance to obtain ability of self-learning and self-adapting in intrusion detection system and to satisfy the need of real time monitor and quick response in intrusion detection system [6, 7].

Intelligence and distribution is the two hot research directions of intrusion detection. A distributed intrusion detection based on agent technology is superior to the traditional distributed technique and has become a hot spot in the field of distributed intrusion detection. An artificial immune system for E-mail classification was proposed in 2003 [8]. A soft computing intrusion detection system was proposed by Ajith Abraham in 2004 [9]. Using labeling to prevent cross-service attacks against smartphones is proposed by C. Mulliner in 2006 [10]. A study of android application security was proposed by Georgios Portokalidis in 2010 [11]. Malware detection on mobile devices using distributed machine learning was proposed in 2010 [12]. Behavior-based malware detection system for android was proposed in 2011 [13]. An android application sandbox system for suspicious software detection was proposed in 2010 [14]. Using machine learning for network intrusion detection was proposed in 2010 [15]. Estimation of distribution algorithm for optimization of neural networks for intrusion detection system was proposed by Y. Chen in 2006 [16]. An approach to implement a network intrusion detection system using genetic algorithms was proposed by M.M. Pillai [17]. Intrusion detection on sensor networks using emotional ants was proposed by S. Banerjee [18]. Development process of intrusion detection system is basically synchronous with the intruder's attack technology development, from the host based intrusion detection system to intrusion detection system based on network, and then to distributed intrusion detection system. Advanced intrusion technology presents the characteristics of distribution and collaboration, which requires that distributed intrusion detection system have characteristics of intelligence, distribution and cooperative work [19-21].

In recent 20 years, attack types become more and more complex than it in the past, and intrusion detection systems need a new way to replace an important part of network protection. Immune system is defense mechanism of human, which can protect the body from a variety of pathogenic bacteria invasion. The two main types of immune system are specific immune and nonspecific immune. Nonspecific immune is also known as congenital immune. Specific immune is also called acquired immune through a study on the environment. Specific immune is a reflection of the body to adapt to the environment, completed by immune cells and it is a major object of study of immunology. The immune system is a complex system made up of immune active molecules, immune cells, immune tissues and organs. The immune function is mainly performed by T cells and B cells. B cells are an essential part of the immune system. B cell has three main functions, producing antibodies, presenting antigen and taking part in immune regulation. Main function of T cells is specific cells immune and immune regulation. AIS is a name of all kinds of information processing technology, computing technology and its application in engineering and science based on principle and mechanism of biological immune system. Natural immune system is a complex distrib-

1874-110X/15

uted information processing learning system which has the function of immune protection, immune tolerance, immune memory, immune surveillance and has strong adaptability, diversity, learning, memory and recognition characteristics. Rich ideas contained by its characteristics and mechanism provide a new opportunity to solve engineer problem, which has attracted wide interest of researchers both at home and abroad. Its application fields have gradually extended to pattern recognition, intelligent optimization, data mining, robotics, automatic control and fault diagnosis and many other fields. AIS is a hot research topic following the evolutionary algorithms, fuzzy system and neural network.

The immune system is an important part of the biology information processing system, which has task to protect the safety of the body and is essentially a large-scale distributed information processing system [4-7]. It has the ability of self-learning, self-organization and the parallel processing at the same time. Cross part of biology and computer science are of great help for two subjects. Using computer to model biological systems will help to improve the understanding of biological systems. On the other hand, the understanding of mechanism hidden by biological systems can improve the way we design computer systems. Intrusion detection system has many similarities with the immune system, and they are charged with the mission of ensuring their safety and also distinguish "self" or "non-self" information. Therefore the applications of the technique of artificial immune to intrusion detection system will greatly improve the performance of the system.

This paper firstly analyzes the basic principle of biological immune. By analyzing the similarity between the principle of artificial immune and intrusion detection, artificial immune is applied to intrusion detection system. This paper proposes a distributed intrusion detection agent model based on artificial immune system. It describes the application of agent to distributed information and safety protection in network security, and presents a hierarchical structure of the intelligent agent and dynamic evolution model. We also propose a vaccine extraction and vaccination algorithm, giving the network dangerous condition assessment operator and using the operator to evaluate real time network security situation.

The remainder of this review is divided into several sections, organized as follows In the next section, we introduce model structure of distributed intrusion detection agent model based on artificial immune system. In Section 3 we propose dynamic mode of this agent model. In Section 4, we test the performance of different network intrusion detection model. In Section 5 we conclude the paper and give some remarks.

2. MODEL STRUCTURE OF DISTRIBUTED INTRUSION DETECTION AGENT MODEL BASED ON ARTIFICIAL IMMUNE SYSTEM

The methods based on artificial immune have been used in the intrusion detection of computer security. In most practical applications, self and non-self is difficult to get accurate one-time definition. Legal network behavior may become a dangerous behavior tomorrow, so real time update of definition of self and non-self is necessary Normal behavior model is based on observable behavior of the system. Sensor agent is bottom components of intrusion detection model, and is in the main position, which is shown in Fig. (**1**). The sensor agents are on a host computer to monitor changeable environment and search for abnormal behavior, which become the main location of intrusion-related information. Analysis agents are the middle components of the intrusion detection model, which accumulate and weight information collected by sensor agents. Manager agent is high-level components of intrusion detection model, which support system overall structure, which complete comprehensive analysis of information collected by alarm agent and analysis agents. Information agents are set up by sensors, which get information packets and passes to other sensors. Alarm agents are consisted of multiple blocks, including timestamp created by alert, intrusion detection time and embedded IP packet, network connection, network flow, CPU state, user status and processor status. How each agent works collaboratively is detailed below.

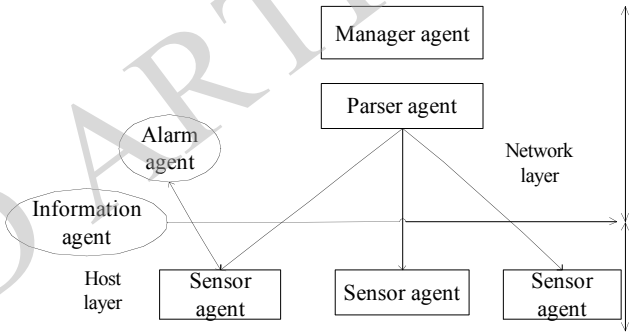

Fig. (1). System function structure.

Computer security system and the biological immune system have many similarities. A biological immune system can produce antibody to resist pathogens by dispersing B cells into A biological immune system can produce antibody to resist pathogens by B cells into the entire body. T cells can regulate the antibody level. Imitating biological immune cells, we set up a certain number of immune cells in the network(sensor agent), to perceive the surrounding environment. Distributed agents are deployed on the sensitive which are in urgent need of safety and protection the network. Sensor agent are divided into mature and memory sensor agent. Memory sensor agent will firstly match antigen, and eliminate non-self antigens. Memory sensor agent will have infinite life cycles, unless they are matched to the newly created self. It is obvious that a lot of memory sensor agent will be created. And mature cells evolve into memory cells or die in their life time. Once sensor agent detects attacks, cells begin to clone, and create a large number of similar cells against the fierce attack, at the same time remind network risk level. Once the network risk reduces, the number of cell antibodies will reduce accordingly. The total number and type of agent affects the density and type of attack. Sensor agents can be divided into three categories according to their own evolution process, which are immature, mature and memory detectors. Dynamic evolution of agent is shown in Fig. (**2**).

In the model, antigen is defined as network behavior and feature of service. $Ag = \{ag \mid ag \in D\}, D = \{0,1\}$. Antigens are fixed length of binary strings from IP packets in the network. Antigen includes the source IP address, destination IP address, port, protocol type, IP sign, IP packet length, the TCP/UDP/ICMP domain and so on. The structure of the antibody is the same with structure of antigen. For intrusion detection, non-self sets represent the IP packet from the computer network attack, and self sets are normal web service transactions. Ag set includes two subsets $Self \subseteq Ag$ and $Nonself \subseteq Ag$.

$$Self \vee Nonself = Ag,\ Self \wedge Nonself = \varnothing.$$

For the convenience of using antigen domain of x, we use a subscript operator ". " for a particular domain of x. In the model, agent set SA is made up of agents.

$$SA = \{< d, age, count > \mid d \in D, age \in N, count \in N\} \quad (1)$$

Where d is the antibody gene used to match an antigen. age is age of agent d. $count$ is the number of agent corresponding to antibody d. N represents natural number set. SA includes two subsets mature subset Mat_{SA} and memory subset Mem_{SA}. Mature SA is a SA, which is tolerant to self set and not activated by antigen. Memory SA is evolved from a mature SA by matching enough antigens in its life cycle.

$$SA = Mat_{SA} \cup Mem_{SA},\ Mat_{SA} \cap Mem_{SA} = \varnothing \quad (2)$$

$$Mat_{SA} = \{x \mid x \in SA, \forall y \in Self, (< x.d, y > \notin Match \wedge x.count \prec \theta\} \quad (3)$$

$$Mem_{SA} = \{x \mid x \in SA, \forall y \in Self, (< x.d, y > \notin Match \wedge x.count \geq \theta\} \quad (4)$$

$\theta > 0$ represents activation threshold. $Match$ represents a matching relation, which is defined as (5).

$$Match = \{< x, y > \mid x, y \in D, f_{match}(x, y) = 1\} \quad (5)$$

The matching function is defined as (6).

$$f_{match}(x,y) = \begin{cases} 1 & \exists i, j, j - i \geq r \wedge 0 \prec i \prec j \leq l, x_i = y_i \\ 0 & otherwise \end{cases} \quad (6)$$

Vaccine va is defined as follows.

$$va \in s, s = \{0,1,*\}^{'} (l \in N, l > 0) \quad (7)$$

va^k represents coding of the k-th gene position of va. The number of antibody population A is $a_1, a_2, \cdots, a_n$. a_i^k represents coding of the k-th gene position of the i-th antibody. $a_1, a_2, \cdots, a_s$ are excellent individuals of antibody population A under a certain evaluation standard. The extraction of vaccine is defined as (8).

$$a^k = \begin{cases} 1, & \frac{1}{s}\sum_{i=1}^{s} a_i^k \succ \alpha \\ 0, & \frac{1}{s}\sum_{i=1}^{s} a_i^k \prec \beta \\ *, & other \end{cases} \quad (8)$$

$\alpha \geq 0.18$, $\beta \leq 0.12$. A vaccine is a good model, gene which is not $*$, is excellent gene. Vaccination operation is the process of using excellent gene of vaccine to replace allele of antibody. a is antibody and va is vaccine. $\hat{a}$ is coding form of antibody a after vaccination operation. Vaccination operation is defined as (9).

$$\hat{a}^k = a^k \Theta va^k = \begin{cases} va^k, & va^k = 0 or 1 \\ a^k, & va^k = * \end{cases} \quad (9)$$

3. DYNAMIC MODE OF THE MODEL

Initial immature agent is generated in a random way. After the algorithm completes an evolutionary process, if the number of iterations is smaller than a given value, then enter the next iteration process. At this time, it is necessary to produce the next generation of immature agent, on the one hand in order to make the child population find local optimal antibody in this subgroup with a high accuracy. On the other hand avoid too replication of similar antibody and improve the generalization ability of the whole antibody population to search target of interest within the largest scope. The algorithm has good global search ability. First of all, memory antibody is clustered. Choose several optimal individuals in each classification of memory antibody as excellent representative of a class to form a population. Do crossover and mutation operation on the population, then go into the next generation of immature antibody collection. In a real time network environment, some network services and behaviors often change, and these changes are allowed in the past, but it may not be allowed in the future.

$$Self(t) = \begin{cases} \{x_1, x_2, \ldots, x_n\} & t = 0 \\ Self(t-1) - Self_{va}(t) \cup Self_{new}(t) & t \geq 1 \end{cases} \quad (10)$$

$Self_{va}(t)$ is a set of x, which is the self antigen forbidden at time t. $Self_{new}(t)$ is a set of x, which is the self antigen permitted at time t. Dynamic mature agent mode is defined as follows.

$$Mat_{SA}(t) = \begin{cases} \varnothing & t = 0 \\ Mat_{SA}^{'}(t) \cup Mat_{new}(t) - Mat_{ac}(t) - Mat_{de}(t) & t \geq 1 \end{cases} \quad (11)$$

$$Mat_{SA}^{'}(t) = Mat_{SA}^{''}(t) - S(t) \cup S^{'}(t) \quad (12)$$

$$Mat_{SA}^{''}(t) = \{y \mid y \in SA, x \in Mat_{SA}(t-1), x.age \prec \lambda, y.d = x.d, y.age = x.age + 1, y.count = x.count\} \quad (13)$$

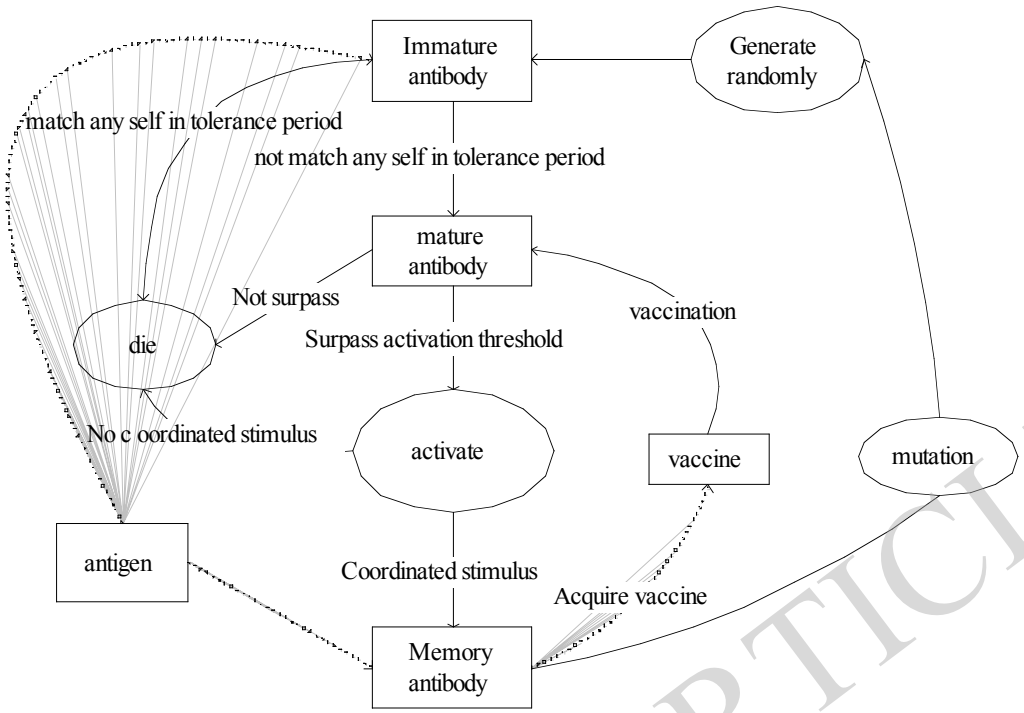

Fig. (2). Dynamic evolution of agent.

$$S(t)=\{x \mid x \in Mat''_{SA}(t-1), \exists y \in SA(t-1), < x.d, y > \in Match\} \quad (14)$$

$$S'(t)=\{y \mid y \in SA, x \in S(t), y.d = x.d, y.age = x.age, y.count = x.count + 1\}$$

$$Mat_{new}(t)=\{y \mid y \in SA, y.d = x.d, y.age = 0, y.count = 0, x \in I_{maturation}(t)\}$$

$$Mat_{ac}(t)=\{x \mid x \in S'(t), x.count \geq \beta\}.$$

$$Mat_{de}(t)=\{x \mid x \in Mat'_{SA}(t) \wedge (x.age \succ \lambda, x.count \prec \beta)\} \cup \{x \mid x \in Mem''_{SA}(t) \wedge \exists y \in SA(t-1), < x.d, y > \in Match\}.$$

Formula (11) describes life cycle of mature agent, which simulates mature agent to evolve to the next generation. All mature agents have a fixed life cycle λ. If a mature agent can match enough antigen in its life cycle, it will evolve into a memory agent. If a mature agent can not match enough antigen in its life cycle, this agent will be deleted and is replaced by newly generated mature agent.

$Mat_{new}(t)$ is the new generation of mature agent set. $Mat_{de}(t)$ is mature agent set, which can not match

with antigen. $S(t)$ simulates agent set after one step evolution. $S'(t)$ indicates the mature agent set through

further evolution. $Mat_{ac}(t)$ mature agent sets which degenerate as the least recently used memory set. $T > 0$ and $\beta > 1$, because degenerate memory agent set has better detection capability than mature agent set. When the same antigen appears, it will immediately be detected by memory agent set. In the life cycle of mature agent set, agents of invalid classification of antigen will die in the clone selection process. Therefore, when abnormal behaviors invade system, the method can strengthen the detection efficiency. Dynamic memory agent mode is expressed as follows.

$$Mem_{SA}(t)=\begin{cases} \varnothing & t=0 \\ Mem'_{SA}(t-1) \cup Mem_{new}(t) \cup Mem_{fr}(t) & t \geq 1 \end{cases} \quad (15)$$

$$Mem'_{SA}(t) = Mem''_{SA}(t) \cup Mem_{cl}(t) - Mem_{de}(t) \quad (16)$$

$$Mem''_{SA}(t)=\{y \mid y \in Mem_{SA}, y.d = x.d, y.age = x.age + 1, y.count = x.count. x \in Mem_{SA}(t-1) - Mem_{cl}(t)\} \quad (17)$$

$$M_{de}(t)=\{x \mid x \in Mem''_{SA}(t), \exists y \in SA(t-1), f_{match}(x,d,y)=1\} \quad (18)$$

$$Mem_{cl}(t)=\{x \mid x \in Mem_{SA}, x.d = y.d, x.age = 0, x.count = y.count + 1. y \in Mem_{cl}(t)\} \quad (19)$$

$$Mem_{new}(t)=\{x \mid x \in Mem_{SA}, x.d = y.d, x.age = 0, x.count = y.count. y \in Mem_{ac}(t)\} \quad (20)$$

$$Mem_{fr}(t)=\{x \mid x \in Mem_{SA}, x.d = y.d, x.age = 0, x.count = 0. y \in \cup_{l=(1,2,\ldots,k) l \neq k} Mem'_{cl}(t)\} \quad (21)$$

(15) represents dynamic evolution of memory agent and

$Mem'_{SA}(t)$ simulates the process of memory agent set evolving into a new generation.

$$Mem_{SA}=\{x \mid x \in SA, \forall y \in Self.(< x.d, y > \notin Match \wedge x.count \geq \theta)\} \quad (22)$$

Mem_{new} is memory agent set immediately activated by antigen. The mature agency matching antigen will be immediately activated and translated into memory agent. $M_{de}(t)$ is deleted memory agent which matches the known self antigen. Mem_{cl} is regenerate memory agent because agent recognizes antigen. $Mem_{fr}(t)$ is memory agent translated from other computers. K represents the identification number of the computer, so the dynamic model of the memory agent strengthens the adaptive ability of the system. In the process of iteration, a vaccine extraction operation is done to extract vaccine corresponding to each type of memory antibody in every period. Memory antibody vaccine collection is divided into several subsets and in each subset vaccine va_i is extracted to join the vaccine library. Vaccine extraction operation and memory antibodies classification operation simultaneously run. The reason for this strategy is that it is impossible to extract a suitable vaccine for all types of invasion. So feasible strategy is to carry out vaccine extraction operation according to the classification of memory antibody. A vaccine is only effective to some sort of antigen. Update of vaccine library is that in the running process of algorithm invalid vaccines are eliminated and new extracted vaccines are added. In order to achieve the library update operation, we firstly define the vaccine effect evaluation method. va is vaccine of antibody population A. The individual of A is a_i. Vaccine effect evaluation value of va is calculated by (23).

$$E(va) = E^{'}(va) + \sum_{i=1}^{n}(fit(\hat{a}_i, ag) - fit(a_i, ag)) \quad (23)$$

$E^{'}(va)$ is effect accumulated value before vaccine. fit is affinity function of antibody and antigen. $\hat{a}_i$ is individual after vaccination of a_i. The update of vaccine library is as follows.

Step1. Each vaccine records its life cycle and vaccination effect evaluation.

Step2. If a vaccine does not achieve effect evaluation value in the specified life period, it will be removed from the vaccine library.

System imitates realization process of metabolism and competition through continuous response. So system assesses security of the network by perception of risk around. Mat_{SA} and Mem_{SA} influence the density of the current network intrusion. The bigger values of Mat_{SA} and Mem_{SA} mean the more serious degree of network intrusion. By recognizing type of Mat_{SA} and Mem_{SA}, we can see different kinds of network intrusion. In dynamic mature agent mode, values of λ and β reflect activity degree of mature cells. $n_{ij}(t)$ represents the number of the j-th type of invasion of the i-th computer at time t. $w_i(0 \le w_i \le 1)$ is important coefficient of the i-th computer in the network. $\alpha_j(0 \le \alpha_j \le 1)$ is risk coefficient of the j-th invasion in the network. Invasion density of the j-th invasion $R_j(t)$ and corresponding network risk $r_i(t)$ are defined in (24) and (25).

$$R_j(t) = \frac{2}{1+e^{-\alpha_j \sum_i w_i n_{ij}(t)}} - 1 \quad (24)$$

$$r_i(t) = \frac{2}{1+e^{-\sum_j \alpha_j n_{ij}}} - 1 \quad (25)$$

According to (24) and (25), we can get the network risk state and evaluate real-time network security.

4. EXPERIMENT AND ANALYSIS

Experiment is done on heterogeneous fleet with a total of 16 nodes, including six HPDX PC machines, 2 IBM Netvista PC machines and 8 Netvista MPC machines. Operating system running on each node is RedHatLinux9 and we use Lincoln lab data set to simulate network traffic.

Kdd_cup.data_10_percent.gz in KDD data set is taken as testing data and this data set has labeled data. The normal samples are labeled as normal samples. Attack samples are marked with attack name such as smurf, land. We divide data set into training set Trainset and testing set Testset. Testing set contains a small number of samples which do not appear in the training set. Trainset is used for training in the simulation and Testset is used to detect efficiency of algorithm. We extract samples in kdd_cup.data_10_percent.gz, which is divides into 5 groups to train testing data set. Each training set contains 8000 samples and the number of normal sample and abnormal sample is 4000. Each testing set contains 2000 samples. In KDD data set, some types of attack samples are too small, which are not suitable for testing, so choose the following 16 kinds of attack testing samples, back, buffer-overflew, guess-pass,imap, ip sweep, land, neptune, nmap, pod, portsweep, rootkit, satan, smurf, teardrop, warezelien, warezmaste. Feature attribute adopts each network connection to record nine attributes of basic TCP characteristic, protocol-type, service (purpose site service type), connection time, src_bytes(the number of bytes of the source host to destination host), dst_ bytes (the number of bytes of destination host to the source host), flag(connection state), land (whether the source main host and the destination host have the same port), wrong_fragment(error subdivision number), urgent(the number of emergency packet). Value of feature attribute is encoded to binary string of 128 bits as antigen.

It can be seen from dynamic evolution process of the agent, that value of tolerance period Tl changes with the values of TP and FP inversely. Because increasing of Tl value makes the immature antibodies experience a sufficient long time of tolerance, the generated memory antibodies have low probability to match themselves, thereby reducing the value of false alarm rate FP. At the same time, the increasing of Tl

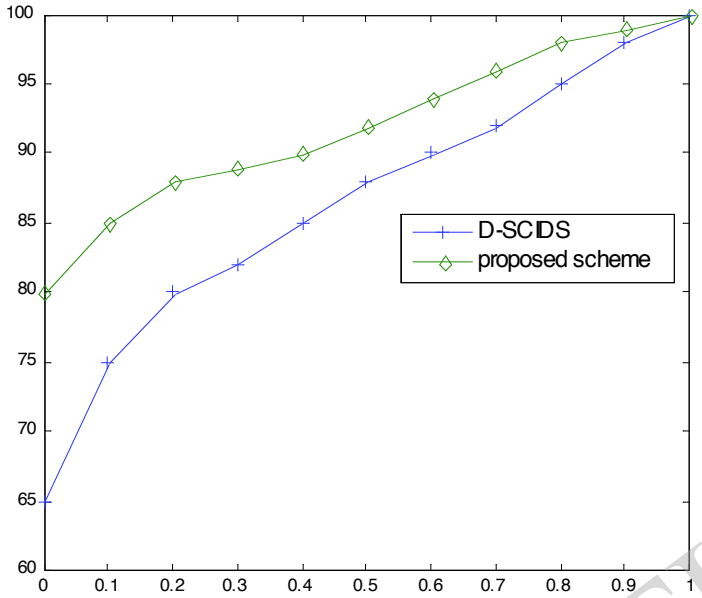

Fig. (3). Roc curve of system.

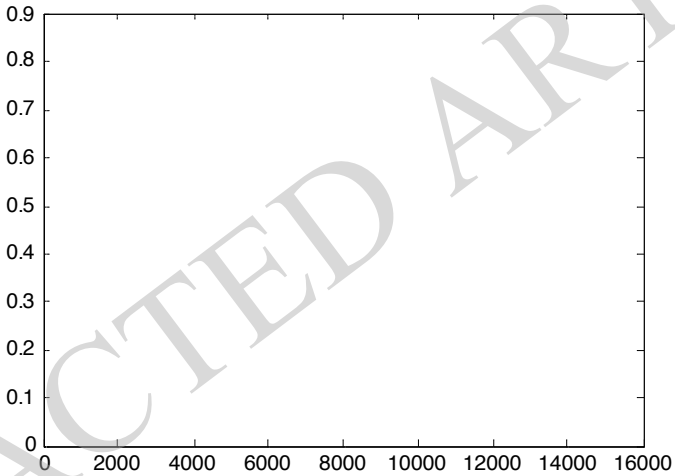

Fig. (4). Network risk situation.

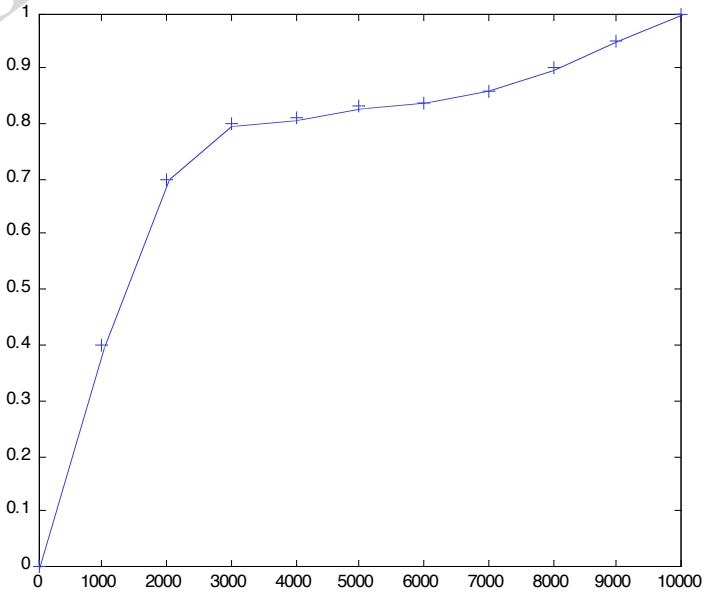

Fig. (5). Relation between iteration times and detection rate.

value makes the number of mature antibody decrease, and thus reduces the number of memory antibodies and value of detection rate TP is reduced.

Death age of T2 of mature antibodies are inversely proportional to the values of FP and TP. This is because the increasing of T2 makes life period of mature antibodies lengthen and probability of matching threshold increase, which makes the probability of generating memory antibodies increase and values of TP and FP increase. If value of activating threshold A is bigger, probability of mature antibody transformed into memory antibody is reduced, so the value of A is inversely proportional to the number of memory antibodies, which also is inversely proportional to the values of TP and FP. Matching number r is inversely proportional to the values of FP and TP. This is because the increasing of r makes the probability of antibody matching with itself and non-self reduced. So TP and FP has decreased and take length of the tolerance period T1=40, mature antibody lifetime T2=50. For further analysis of system performance of the model, this algorithm is compared with D-SCIDS proposed by Snapp and receiver operating characteristic curve is shown in Fig. (**3**). Roc is the most commonly used curve which is used to describe ability of intrusion detection algorithm. X axis of ROC often denotes false alarm rate and Y axis denotes detection rate under different false alarm rate.

In the case of a very low false alarm rate, intrusion detection method based on artificial immune distributed agent can get higher detection rate than D-SCIDS intrusion detection method. In high-speed network fleet environment, this model can achieve good detection performance.

Fig. (**4**) represents changing situation of network risk $r_j(t)$ with the change of rate of attack packets. X axis denotes packets per second and Y axis denotes network danger. As is shown, when the attack level changes, network risk $r_j(t)$ changes subsequently. When the attack level increases, network risk $r_j(t)$ increases subsequently. when the attack level decreases, after delay of a few seconds, network risk $r_j(t)$ decreases subsequently. In a very short period of time, when the attack occurs, the network can keep alert. Fig. (**5**) represents changing situation of detection rate TP with the number of iterations. X axis denotes iteration times and Y axis denotes detection rate. With increasing of the number of iterations, detection rate of the system is improved. In the experiment, affinity calculation uses algorithm with r number of continuous matching rules and r=8. Initial the number of self set and n=40, the number of the new generation of immature cells is 4, mature antibody activation threshold value is A = 5, cloning rate is 5%, the cross rate is 0.105, and mutation rate is 0.103. The detection performance of the system is shown in Table **1**.

Detection performance of distributed agent model based on artificial immune is compared with other models, which is shown in Table **2**. Detection accuracy of proposed algorithm on U2R data set is 97.50%, detection accuracy of SVM algorithm on U2R data set is 64.00%, detection accuracy of BP algorithm on U2R data set is 48.00%. Detection accuracy of proposed algorithm on R2L data set is 93.70%, detection accuracy of SVM algorithm on R2L data set is 97.33%, detection accuracy of BP algorithm on R2L data set is 95.02%. Detection accuracy of proposed algorithm on DOS data set is 97.33%, detection accuracy of SVM algorithm on DOS data set is 99.11%, detection accuracy of BP algorithm on U2R data set is 97.47%. Detection accuracy of proposed algorithm on Probe data set is 96.25%, detection accuracy of SVM algorithm on Probe data set is 98.57%. From the view of classification accuracy, average performance of distributed agent intrusion detection based on artificial immune is superior to other algorithms. The proposed model has good stability for different types of attacks and has higher detection rate on U2R data set, which is difficult to detect.

Table 1. Detection performance of system.

Type	TP	FP
DOS	97.33%	1.05%
R2L	93.70%	5.13%
U2L	97.50%	0.69%
Probing	96.25%	0.78%

5. CONCLUSION

In information security areas, detecting unknown intrusion activities becomes more and more important at present, traditional anomaly detection systems face problems on following aspects: updating normal profiles; dynamic real-time detection; distributed detection. New intrusion detection approach based on Biological Immune System principle provides solutions to settle many difficulties that traditional anomaly intrusion detection encountered. But nowadays immune intrusion detection techniques are in their early

Table 2. Detection performance comparison of distributed agent model based on artificial immune with other models.

Algorithm	Probe	DOS	U2R	R2L
BP	92.71%	97.47%	48.00%	95.02%
Wenke L	97.00%	79.9%	75.00%	60.87%
SVM	98.57%	99.11%	64.00%	97.33%
Proposed scheme	96.25%	97.33%	97.50%	93.70%

stage. Intrusion detection technology has become increasing important in the area of network security research. Distributed and self-organizing characteristics of immune system can match with the development trend of intrusion detection system. So the immune system theory used to design the network intrusion detection system has incomparable advantages. A novel model of intrusion detection based on distributed agents is presented according to the similarity of artificial immune systems and intrusion detection in the paper. Dynamical evolution model is proposed. Recursive equations for self, antigen, immune tolerance, mature agents lifecycle and immune memory are presented, and the hierarchical and distributed management framework of the proposed model is built. Furthermore, agents can be used to distributed information and security surveillance in network security. The experimental results show that the proposed model has the features of real-time processing that provide a good solution for network surveillance.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work is sponsored by scientific research project in 2014, the Education Department of Hunan province (No.14C0403).

REFERENCES

[1] C. R. Haag, G. B. Lamont, P. D. Williams, and G. L. Peterson, "An artificial immune system inspired multiobjective evolutionary algorithm with application to the detection of distributed computer network intrusions," In: *Proceedings of the 6th International Conference on Artificial Immune Systems (ICARIS),* vol. 4628 of Lecture Notes in Computer Science, Springer, 2007.

[2] J. Li, G.Y. Zhang, and G.C. Gu, "The research and implementation of intelligent intrusion detection system based on artificial neural network," In: *Proceedings of 2004 International Conference on Machine Learning and Cybernetics*, IEEE Press, vol. 5, 2004.

[3] S. T. Powers, and J. He, "Evolving discrete-valued anomaly detectors for a network intrusion detection system using negative selection," Proceedings of the 2006 UK Workshop on Computational Intelligence(UKCI 2006), University of Leeds, 2006.

[4] J. Kim, and P. J. Bentley, "Evaluating negative selection in an Artificial Immune System for network intrusion detection," Proceedings of the 2001 Genetic and Evolutionary Computation Conference (GECCO'01), Morgan Kaufmann, 2001.

[5] J. Ma, Y. Shi, Z. Zhong, and X. Liu, "An Anomalistic Electromagnetism Signal Detection Model Based on Artificial Immune System," In:*International Conference on Communications and Intelligence Information Security (ICCIIS)*, NanNing, China, pp. 256-260, 2010.

[6] V. Engen, "Machine Learning for Network Based Intrusion Detection: An Investigation into Discrepancies in Findings with the KDD Cup '99 Data Set and Multi-Objective Evolution of Neural Network Classier Ensembles for Imbalanced Data," PhD thesis, School of Design, Engineering and Computing, Bournemouth University, 2010.

[7] D. Dal, S. Abraham, A. Abraham, S. Sanyal, and M. Sanglikar, "Evolution induced Secondary Immunity: An Artificial Immune System based Intrusion Detection System," In:*7th International Conference on Computer Information Systems and Industrial Management Applications (CISIM'08), Ostrava*, The Czech Republic, IEEE Computer Society press, USA, pp. 61-66, 2008.

[8] S. Andrew, A. F. Alex, and T. Jon, "AISEC: an Artificial Immune System for E-mail", *Classification Evolutionary Computation*, pp. 131-138, 2003.

[9] A. Abraham, R. Jain, S. Sanyal, and S. Y. Han, "SCIDS: A Soft Computing Intrusion Detection System," In: *6th International Workshop on Distributed Computing (IWDC 2004)*, A. Sen *et al.* (Eds.) Springer Verlag, Germany, Lecture Notes in Computer Science, vol. 3326, pp. 252-257, 2004.

[10] C. Mulliner, G. Vigna, D. Dagon, and W. Lee, "Using labeling to prevent cross-service attacks against smartphones", In: *Proceedings of the Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*, Springer, Berlin, Germany, pp. 91-108, 2006.

[11] W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri, "A study of android application security", In: *Proceedings of the 20th USENIX Security Symposium, USENIX Association*, pp. 21-32, 2011.

[12] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid android: versatile protection for smartphones", In: *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC'10, New York, NY, USA, pp. 347-356, 2010.

[13] A. S. Shamili, C. Bauckhage, and T. Alpcan, "Malware detection on mobile devices using distributed machine learning", In: *Proceedings of the 2010 20th International Conference on Pattern Recognition*, CPR '10, Washington, DC, USA, pp. 4348-4351, 2010.

[14] I. Burguera, U. Zurutuza and S. N.Tehrani, "Crowdroid: Behavior-Based Malware Detection System for Android", Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (SPSM'11), Chicago, Illinois, USA, pp. 15-26, 2011.

[15] R. Sommer, and V. Paxson, "Outside the Closed World: On Using Machine Learning For Network Intrusion Detection", *IEEE Symposium of Security and Privacy 2010 (SP'2010)*, Oakland California USA, pp. 305-316, 2010.

[16] Y. Chen, J. Zhou, and A. Abraham, "Estimation of distribution algorithm for optimization of neural networks for intrusion detection system", In: *The 8th International Conference on Artificial Intelligence and Soft Computing (ICAISC '06)*, pp. 9-18, 2006.

[17] M. M. Pillai, J. H. Eloff, and H. S. Venter, "An approach to implement a network intrusion detection system using genetic algorithms", In: *Proceedings of the 2004 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*, pp. 221-221, 2004.

[18] S. Banerjee, C. Grosan, A. Abraham, and P. Mahanti, "Intrusion detection on sensor networks using emotional ants", *International Journal of Applied Science and Computations*, pp. 152-173, 2005.

[19] W. Enck, M. Ongtang, and P. McDaniel, "On Lightweight Mobile Phone Application Certification", ACM Proceedings of the 16th ACM conference on Computer and communications security (CCS'09), Chicago, Illinois, USA, pp. 235-245, 2009.

[20] W. Enck, P. Gilbert, B.G. Chun, L. P. Cox, J. Jung, P. McDaniel and A.N.Sheth, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones", In: *Proceedings of the 9th USENIX conference on Operating systems design and implementation*, OSDI'10, Berkeley, CA, USA. USENIX Association, pp. 1-6, 2010.

[21] T. Blasing, A. D. Schmidt, L. Batyuk, S. A. Camtepe, and S. Albayrak, "An android application sandbox system for suspicious software detection", In: *5th International Conference on Malicious and Unwanted Software (MALWARE'2010)*, Nancy, France, pp. 55-62, 2010.

Received: June 10, 2015 Revised: July 29, 2015 Accepted: August 15, 2015