International Journal of Knowledge and Language Processing
Volume **2**, Number 2, April **2011**

www.ijklp.org
AKLP International ©2011 ISSN 2191-2734
pp. **23-34**

Research on Network Security Situation Awareness Technology based on AIS

SunJun Liu[1]
[1]Department of Computer Science
ChengDu University of information Technology
Chengdu, 610225, China
bigluckboy@163.com

Le Yu[2]
[2]Military Representative office of PLA in No.3531 plant
Box.No.4, P.O.Box.301
Guiyang, Guizhou, 550009, China
wazxy1987@163.com

Jin Yang[3]
[3]Department of Computer Science
LeShan Normal Univ., LeShan, China
jinnyang@163.com

Received March 2011; revised April 2011

ABSTRACT. *With the applying of artificial immune technology in the field of network security situation awareness, this article puts forward a new immune network security situation awareness model to enable self-learning and self-adapting of network system, and increase its immunity and viability. When network is under attack, it can find out the current network security situation and future trend in an all-around way, provide grounds for reasonable and accurate response to guarantee the usability of system.*
Keywords: network security situation, intrusion detection, artificial immunity, network security

1. **Introduction.** Along with the popularization of network, the threat it faces is growing bigger, for example, computer virus, Trojan horse program and DOS/DDOS attack are increasingly rampant. So as to guarantee the smooth running of network, presently adopted traditional technology of intrusion detection, firewall and virus detection are all in passive defense way and in independent working status, therefore, they don't have cognition on the network resource they are protecting for. And this cognition disjunction increases the time needed for operator to make a decision for alarm raised, and therefore, misses the optimal timing of handling.

This article applied artificial immunological technique in the field of network security

situation awareness, designed and established an immune network security situation awareness system. It is aimed to carry out real-time monitor on network security situation, realize real-time and quantitative awareness of network security situation before malicious network behavior becomes out of control, and help make timely and effective network security strategy adjustment for better general security safeguard of system.

2. **Brief Research Status on current network security situation awareness technique.** Because network security situation technology is a newly emerging one, domestic and overseas research on this field is still at starting stage, and related research results are less common. Some research is based on information warfare ground situation awareness and some other emphasizes on improvement on traditional intrusion detection model.

From the view of information warfare, main situation awareness model frame now popular in foreign countries currently is one using data fusion technology and data mining to extract security situation put forward by Edward Waltz [1]. The JDL(Joint Director of Laboratories)[2]model brought forth by US Defense Department makes association analysis and data combination of received data from sensors and information source to obtain overall evaluation of warfare ground and threat degree. And from the view of network security, there is mainly network security situation awareness frame based on intrusion detection fusion brought forth by Tim Bass[3]. Jason Shifflet[4] made analysis and comparison on corresponding concepts of network security awareness, and put forth technology free structure based on modularization.

3. **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 [4,5] properties etc.

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.

Diversity: The matching of antibodies and antigens adopts fuzzy matching, 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.

Tolerability: Immune tolerability refers to the non-response status of immune cells towards the peculiarities revealed by certain kinds of antigens [7]. The tolerability of IA is of great significance in the maintaining and balancing of the model.

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.

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

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 network s 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.

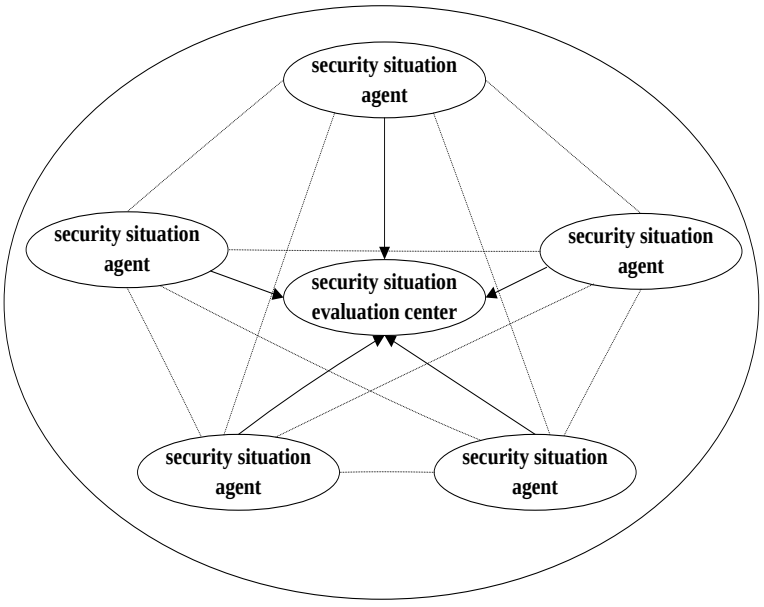

FIGURE 1. Architecture of NIDIMA

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

3.1. 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.

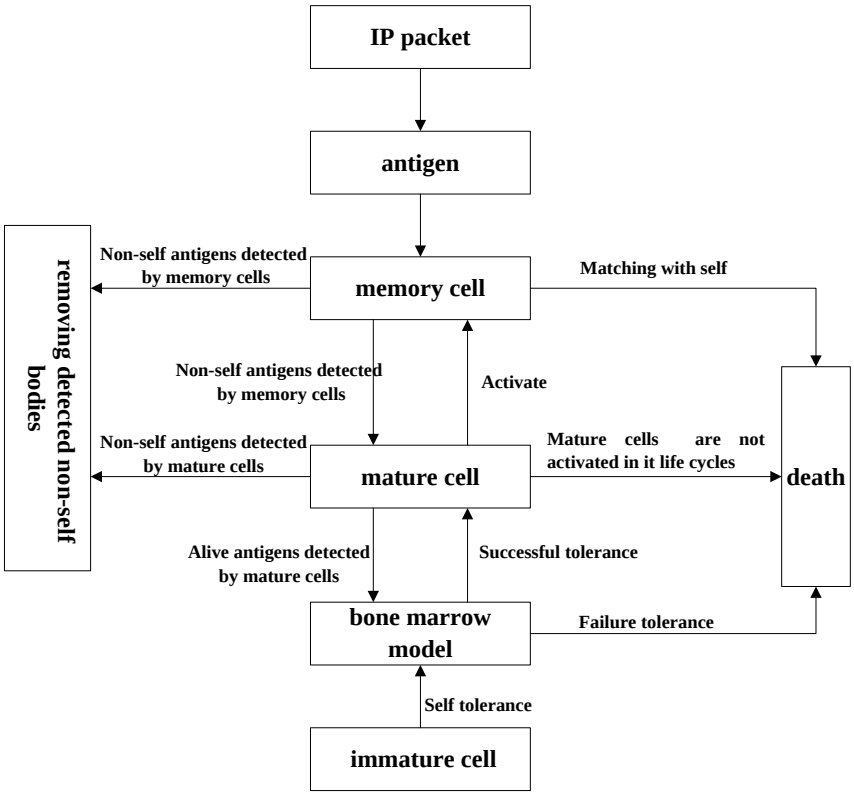

FIGURE 2. Architecture of Immune Agent

3.2. 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 ⊂ U, it mainly includes IP address, port and protocol type etc.

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

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 ∪ NonSelf = Ag, Self ∩ Nonself = ∅

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

$$B = \{Ab \mid Ab =< s, age, count, ag >\} \tag{2}$$

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 TAb ⊆ U; Memory antibodies evolve from mature antibodies that are not activated, memory antibodies assembly MAb ⊆ U; Immature antibodies are antibodies that have not undergone self-tolerance, immature antibodies assembly IAb ⊆ 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 ∈ Ag, y ∈ B, xi, yi are the i-th characters of x, y respectively, l is the length of character string, θ is the threshold value of affinity matching.

$$f_{match}(x,y) = \begin{cases} 1, & (f_{h\_dis}(x,y)/l) \geq \theta \\ 0, & otherwise \end{cases} \qquad f_{h\_dis}(x,y) = \sqrt{\sum_{i=1}^{l}(x_i - y_i)^2} \tag{3}$$

3.3. The changing process of immature antibodies. Let I be the number of immature antibodies included in IAb at certain time, the dynamic changing formula of immature antibodies assembly is:

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

The formula (4) indicates that the changing process of IAb assembly is divided into 2, that is, inflow and outflow. Inflow is the process of newly produced immature antibodies' joining in IAb assembly: I = Inew×Δt, Inew means the production rate of immature antibodies per unit of time. Outflow is the process of removing immature antibodies from IAb 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 $\frac{\partial I_{mature}}{\partial x_{mature}} \cdot \Delta t$, 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∈IAb.

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

3.4. The changing process of mature antibodies. Let T represent the number of mature antibodies included in TAb at certain time, and the dynamic changing formula of mature antibodies assembly is:

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

The formula (6) indicates that the changing of TAb assembly is divided into two processes: inflow and outflow. The inflow is the process of antibodies' joining the TAb, and there are two ways: The number increased out of immature antibodies' successful tolerance and evolution is represented by $\frac{\partial T_{tolerate}}{\partial x_{tolerate}}\cdot\Delta t$; $\frac{\partial T_{clone}}{\partial x_{clone}}\cdot\Delta t$ 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 $\frac{\partial T_{active}}{\partial x_{active}}\cdot\Delta t$, while $\frac{\partial T_{dead}}{\partial x_{dead}}\cdot\Delta t$ represents the number that die from failed activation.

The mature antibodies assembly Tactive that have been activated and evolved into memory antibodies is shown in formula （8）, and the mature antibodies assembly Tdead 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.

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

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

3.5. The changing process of memory antibodies. Let M as the memory antibodies quantity contained in MAb at certain time, and the dynamic changing formula of memory antibodies assembly is:

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

Because memory antibodies have infinite life cycle, the change of Mb 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 active, $\frac{\partial M_{active}}{\partial x_{active}}\cdot\Delta t=\frac{\partial T_{active}}{\partial x_{active}}\cdot\Delta t$.

3.6. 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 MAb 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 TAb to detect antigens: The non-self antibodies that match with TAb are removed, and the TAb that has detected enough antigens in the life cycle is then activated and evolved into memory antibodies MAb; The MAb 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. **Immune network security situation awareness technology.** Biological Immune System (BIS) is a complicated system with the ability of self-adapting , self-learning, self-organizing , parallel processing and distributed coordinating, and it also has the basic function to distinguish self and non-self and clean non-self. The problems in the field of computer security and Artificial Immune Systems have the astonishing similarity of keeping the system stable in a continuous changing environment. Artificial Immune System[5-7] can use biological immune theoretic for references to search and design relevant models and algorithms to solve the various problems occurred in the field of computer security.

Technology for Network Security Situational Awareness, which is a positive defense technology, has become the orientation of research in the field of network security. Based on the analysis of the papers from domestic and foreign on technologies for network security situational awareness, this paper designs and builds a network security situational awareness system based on the profound research of BIS. The system uses network intrusion detection, which based on the theory of biological immunity as the base of situational awareness, to detect known and unknown intrusions with the help of biological technology such as self/non-self discrimination, self-tolerance, self-learning, evolution mechanism, immunological surveillance, etc. According to correspondence relations of density change of antibody in the artificial immune systems and pathogen invasion intensity, a novel network risk evaluation model is also established. Based on the current real-time network risk evaluation, the thesis also makes risk evaluation on short- term, medium-term、long-term network in different span. In the tendency prediction for network security, this paper uses Grey Markov Model to make quantitative prediction on short- term, medium-term、 long-term risk in different span. These methods make overall and quantitative identification about network security, and it is also helpful to resemble network security tragedy effectively, therefore, protect network infrastructure greatly.

The self-adaptability, distributed character and quantization of antibody concentration that biological immune system bears are just the effective method to solve the technological problems of network security situation awareness, thus this article applies the characteristics of biological immune mechanism in the field of network security situation awareness research, and establishes immune network security situation awareness system to make real-time and quantitative analysis on network security condition and its changing trend.

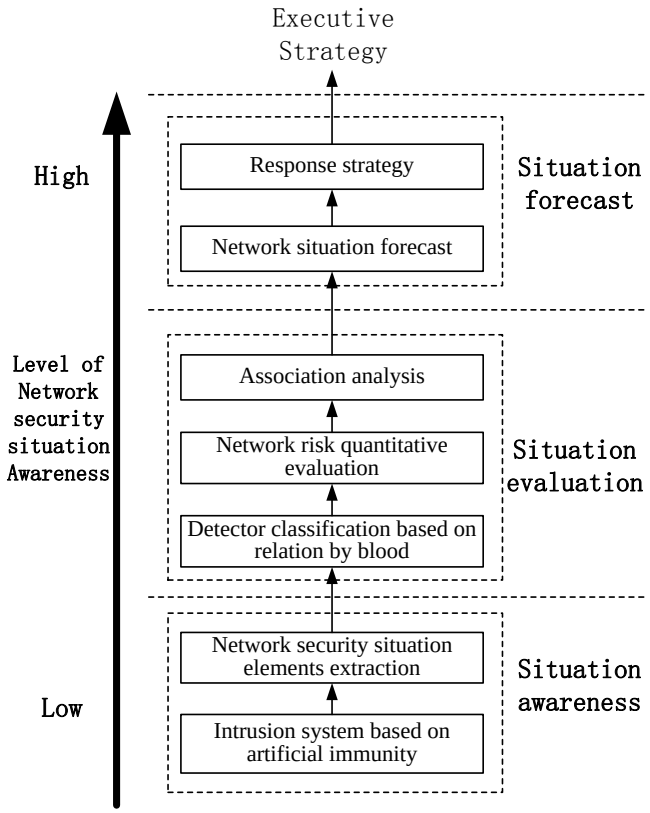

FIGURE 3. System structure of network security situation awareness

Network security situation is a macro reaction to the running status of network information system, is a process of mining, understanding and forecasting situation elements which reflect network security condition, thus the network security situation awareness system based on artificial immunity raised here is divided into three levels in system structure, namely network security situation awareness, situation evaluation and situation forecast in succession, as shown in figure 3.

Here comes next is a detailed introduction on system structure of network security situation awareness system.

4.1. Situation awareness. Situation awareness is the foundation of network security situation awareness, which filters、simplifies and combines the corresponding states and properties of various factors which bear influence on network security situation, and get situation factors which reflect system security state to make preparation for situation

evaluation. But due to lack of self-adaptability and self-learning, traditional intrusion detection system cannot recognize unknown attack or virus varieties, thus it is hard for it to provide overall and effective situation information to network administrator.

However, intrusion detection technique based on artificial immunity has solved this problem, and figure 2 illustrates the working process of intrusion detection model based on immunity. The working process of this model is composed of two parts, one is recognizing intrusion process by immune detector, which are in simple line; the other is the evolving process of immune detector, in hair strip, the two processes are mutually affected and in process simultaneously.

During the evolving process of immune detector, it is divided into immature detector, mature detector and memory detector according to the self evolvement of detector, among which newly generated immature detector evolves to mature detector after self-tolerance, and mature detector is activated and evolves to memory detector if it matches non-body antigens to a certain amount in its lifecycle, or else it shall die of aging. And memory detector has infinite lifecycle.

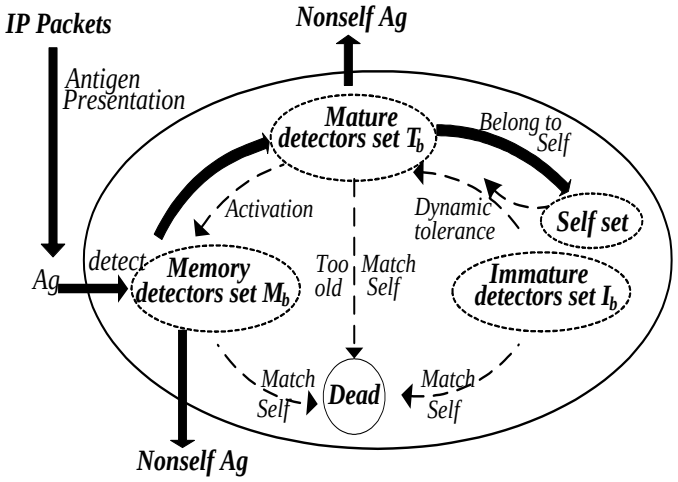

FIGURE 4. Working process of intrusion detection model based on immunity

During the course of detector's recognizing of antigens, IP data packet transmitting in network forms antigen assembly after being presented by antigen. Antigen assembly is detected firstly by memory detector, then mature detector and at last antigens left which have passed the detection are added into auto-assembly for tolerance training with immature detector.

4.2. Situation evaluation. Situation evaluation is the core of situation awareness, and is a dynamic understanding process of current security situation. Situation evaluation makes association analysis of security events among factor information and concludes on risk level according to the degree of threat in order to reflect the security situation of the whole network.

Based on the corresponding relationship of the change of antibody concentration of

human immune system and pathogen's intrusion rate, it is put forth that network risk evaluation model based on immunity can realize real-time and quantitative evaluation of network security situation. This method can make network risk evaluation in dynamic way, realize overall evaluation of the attacks in each level of host computer, sub-network and whole network, get current system risk and reflect the security situation of present network timely and accurately.

In figure 5, distributed structure of network security risk evaluation model is given. In this structure, massive LCRS distributed in network makes local security risk evaluation and at the same time, sends information such as antibody concentration and types etc to SREC for fusion, furthermore, it calculates out the whole risk of whole network as well as categorized risk of each kind of attack and makes real-time and quantitative description of network security situation.

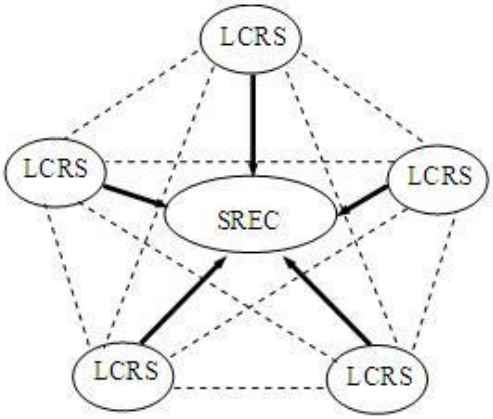

FIGURE 5. Network security risk evaluation model structure based on immunity.

On the foundation of AIS based network risk evaluation, it could make evaluation towards short-term, medium-term, long-term network in different span, then make analysis on the results, discuss the randomness of risk changes in real-term and short-term, as well as the periodicity in mid-term and long-term network risk changes. The model takes an overall overview on risk change tendency on every hierarchy of network from different viewpoints, therefore, it is likely to build a safeguard system.

4.3. Situation forecast. Situation forecast is the highest level of situation awareness, it is based on historical and present network security situation information and makes quantitative prediction of the network security situation some period in the future so that decision-maker can have more complete network security situation and provides accurate grounds for reasonable response strategy to restrain network attack.

As to the fuzziness, randomness and uncertainty of future security situation change, it is put forth that gray theory can be adopted for establishing network security situation forecast model. Meanwhile, considering that network security situation awareness system is non-linear and the data is of high random fluctuation, Markov's state transition matrix [10] is adopted to modify gray model's forecast results and make up for the limitation of gray forecast model. Therefore, gray theory and Markov theory are combined to bring the

advantages of both to full play and overcome the defects of both, thus Gray Markov forecast model came into being. During the forecast process, the classical GM (1, 1) model of gray theory is adopted to make prediction of network security situation data and find out its changing trend, and then Markov theory is used to make modifications on model error to improve the forecast accuracy of network security situation changing trend.

5. **Brief Summary.** With the applying of artificial immune technology in the field of network security situation awareness, this article puts forward a network security situation awareness model based on immunity, and it is divided into three levels in brief: security situation awareness, security situation evaluation and security situation forecast, among which security situation awareness is the basis of the whole system, it extracts situation elements and makes preparation for situation evaluation; Situation evaluation is the core of situation awareness as well as a dynamic reasoning and understanding process of current security situation; Situation forecast makes prediction of future network security trend based on historical and present network security situation information. When network information system is under attack, network security situation awareness model based on immunity has all-around and whole knowledge of current network security situation and its future trend and can provide grounds for reasonable and accurate response to guarantee the availability of system.

It can change current passive defense situation using traditional network security approaches such as firewall, leaks scan techniques, ids and so on, and is helpful to establish new generation proactive defense theories and realization techniques. Meanwhile, the work is not only theoretic values to design network security awareness system in any complex network circumstances, but also very significant to protect network infrastructure for our country.

Acknowledgment. This work is supported by the National Natural Science Foundation of China under Grant (No.61003310).

REFERENCES

[1] Endsley M.R,, “Design and evaluation for situation awareness nehancement,” Proc. 7th IFAC/IFIP/IFORS/IEA symposium on Analysis, Design and Evaluation of Man-Machine System, Kyoto,1998, pp. 425-430

[2] Bass T. “Intrusion Detection Systems and Multisensor Data Fusion:Creation Cyberspace Situation Awareness”, Communications of the ACM, 2000, vol (43), April ,pp.99-105.

[3] Steinburg A.N,Bowman C.L, White F.E, “ Revision to the JDL Data Fusion Model”, Joint NA TO/IRIS Conference , Quebec, Octorber 1998.

[4] Shifflet J, “ A Technique Independent Fusion Model For Network Intrusion Detection ”, Proc of the Midstates Conference on Undergranduate Research in Computer Science and Mathematics, 2005, vol(3), pp.13-19.

[5] Jerne.N, K. Towards, “a Network Theory of the Immune System”. Annnual Immunology, 1974,

125:86-93.

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

[7] Perelson A, “Weisbuch G.Immunology for physicists”. Review of Modern Physics, 1997, 69(4):65-71.