International Journal of Knowledge and Language Processing
Volume **2**, Number 3, July **2011**

www.ijklp.org
KLP International ©2011 ISSN 2191-2734
pp. **21-35**

Research on Dynamic Model for Network Security based on Artificial Immunity

Caiming Liu[1], Yan Zhang[2, *] and Run Chen[3]

[1] Laboratory of Intelligent Information Processing and Application
Leshan Normal University
Leshan, Sichuan, 614004, China
liucaiming@gmail.com

[2] School of Computer Science
Leshan Normal University
Leshan, Sichuan, 614004, China
zhangyan_201016@163.com

[3] School of Computer Science
Sichuan University
Chengdu, Sichuan, 610065, China
cr.run@163.com

[*] Corresponding author

Received May 2011; revised July 2011

ABSTRACT. *The computer network confronts the complicated and changeful security environment. The protection process of computer network security is a series of behaviors. A scientific security model of network needs to dynamically recognize and evaluate the situation of network security. Then the protection policy of network security is worked out and the protection method of network security is deployed according to the above results. To avoid the problem of relax relation of the stages in the conventional network security architectures, this paper introduces the principles and mechanisms in Artificial Immune System (AIS) into the research of network security model based on the classical network security architectures. The excellent attributes of AIS is made full use of to construct a dynamic network security model in this paper. The proposed model consists of Immune Detection Sub-model, Risk Assessment Sub-model and Response Sub-model based on immune antibody intensity. The elements of network behavior and detection for network security threats are simulated. The detection elements evolve dynamically to adapt the dynamic change of the network security environment. The proposed model uses immune mechanisms to detect, assess and respond the current status of network security. The results of detection, assessment and response act on the protection policy and methods. The proposed model is dynamic and circular to protect network security.*

Keywords: AIS, Network security model, Detection, Risk Assessment, Response

1. **Introduction.** The computer network has become a complicated and huge system. Its openness leads to the complexity and unvarying change of the network security environment. Attackers without authorization use the leaks of network and information systems to obstruct normal running of networks. This brings a series of security problems to the network steadiness. The problems of network security challenge the usability and of reliability of computer network and threaten the data security of network and information systems. Network security threats which cause network security problems are not static. They change along with the interests and benefits of threat makers. Therefore, the network security environment is dynamic. The dynamic trend requires that the protection system can not be invariable, but judge the newest network situation and work out purposeful protection methods against network security threats. The work to maintain network security is a systemic engineering and dynamic process. It needs historical protection experiences. Furthermore, it is necessary to judge the network status according to the current network security data and formulate some scientific protection policy and plan to provide convincing foundation for researching and deploying reasonable protection methods.

In 1998, The National Security Agency (NSA) of USA drew up *IATF* [1]which put forward *deep defense police* and defined the deep defense target including network and infrastructure defense, region boundary defense, computation environment defense and support infrastructure [2]. To effectively protect the security of network and information, China also put forward constructing the security defense architecture [3] which requires strengthening the performance of risk assessment, protection in rank, network monitor system, network trust hierarchy, emergency response system, disaster recovery, and etc[4]. However, at present, people pay plenty of attention to protection methods but not entire construction of network and information security defense system. People universally ignore the other links of the network security architecture [5] except protection method or isolate the links. The scientific data of the links of intrusion detection, security risk assessment and security response is not made full use of. In the other hand, the defense strategy of network security is worked out nearly hastily and blindly. It causes that the deployment of network security protection methods cannot achieve the expectant target, but lacks rationality and pertinence, consumes cost of network security defense and wastes much resource of manpower and material. Currently, some network security models [6] are used to realize the network security architecture. However, most of them cannot fully associate the links of the network security architecture in the practical application. Therefore, it is urgent to construct a theoretical model which can closely associate all the links of the network security architecture, adapt dynamic network security environment and scientifically guarantee the network security.

Much research indicated that the problems found in computer security are quite similar to those encountered in a Biological Immune System (BIS) [7]. Researchers used the Artificial Immune System (AIS) [8] which simulates BIS to put forward a series of theoretical models [9], realization methods [10] and technique plan [11] to solve the problems in the network security architecture. The inspiration which is provided for the

engineering science by BIS attracts many scholars to study AIS. A lot of researchers have given much attention to AIS [12, 13]. AIS developed in high-speed since the special conference on artificial immunity was convened in *World Congress on Computation Intelligence* (WCCI) in 1998 for the first time. AIS has become a new branch of computation intelligence. Some authoritative journals and academic conference reported AIS and its research progress. The special conferences in some international academic conferences were open to discuss AIS in particular. The *International Conference on Artificial Immune Systems* (ICARIS) [14] has been held for ten times since 2002. Scholars and researchers in many research areas studied AIS in different points of view and acquired outstanding achievements. AIS has been applied in the fields of network and information security [15-23], machine learning [24], automatic control [25], combinatorial optimization [26], pattern recognition [27], fault diagnosis [28], and etc. It provides a new method to solve many complicated problems.

AIS has the good attributes of diversity, distributed and parallel treatment, self-organization, self-adaptation, robustness, and etc. The above attributes make that AIS is good at being applied in network security. Researchers consulted AIS and put forward *Computer Immune System* (CIS) [7] which is applied in solving the problems of network security broadly. Traditional network security technologies adopt the technology of static pattern match commonly. It lacks diversity and self-adaptation which are owned by immune system. The attributes in AIS can remedy the defect of traditional network security technologies. At present, AIS has been widely applied in the areas of network security including intrusion detection [15-17], virus detection [18, 19], risk assessment [20, 21], network monitoring [22], network forensics [23], and etc.

This paper uses the good characteristics in AIS for reference and applies the principles and mechanisms of AIS in the research of network security architecture. Dynamic network security model based immunity is proposed and expected to provide a new idea for constructing effective, exercisable and automated network security architecture. In the rest of this paper, first, classical network security architectures are introduced summarily. Second, the dynamic network security model based immunity proposed in this paper is described in detail. Finally, our work is summarized.

2. **Classical Network Security Architecture.**

Some standard organizations and commercial establishments drew up classical network and information security architectures including ISO/OSI security architecture, TCP/IP security architecture, PDR, P2DR (PDRR) and P2DR2 (PPDRR), and etc. The classical architectures carry out the policy of network security defense through management and technologies.

2.1. **ISO/OSI Security Architecture.**

The ISO/OSI reference model plays an important part in the international standardization of computer network. To defend the security of ISO/OSI reference model, International Organization for Standardization (ISO) drew up the international standard *Information Processing Systems-Open Systems Interconnection-basic Reference Model-Part 2: Security Architecture* [29] in which ISO/OSI security architecture which is shown in Figure 1 is given. ISO/OSI security architecture was put forward based

on the analysis of threats and vulnerabilities faced by computer network in ISO/OSI reference model. It has the significance of guidance to protect the computer network constructed with ISO/OSI reference model [30]. It adds security services, security mechanisms and security management in the layers of ISO/OSI reference model to ensure the safe running of computer network. It defines five kinds of security service including authentication, access control, data confidentiality, data integrity and non-reputation. Meanwhile, it uses eight kinds of security mechanisms to realize the security services. The security mechanisms include encipherment, digital signature mechanisms, access control mechanisms, data integrity mechanisms, authentication exchange mechanism, traffic padding mechanism, routing control mechanism and notarization mechanism.

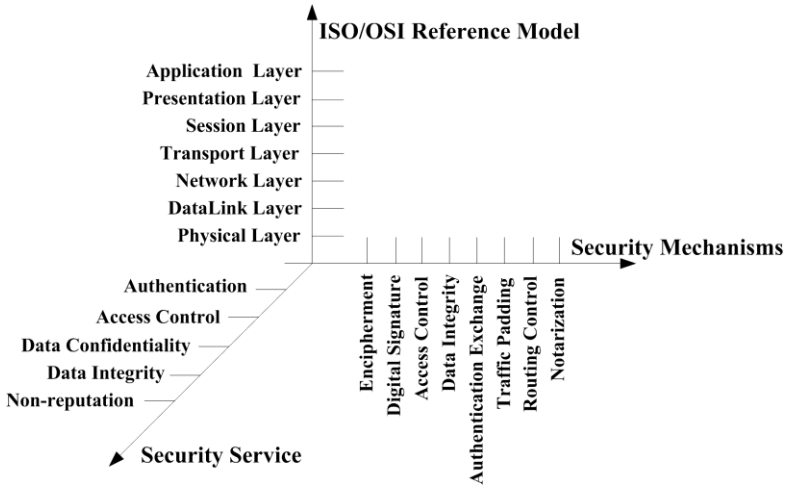

FIGURE 1. ISO/OSI security architecture [30].

2.2. **TCP/IP Security Architecture.** Referring to ISO/OSI security architecture, TCP/IP security architecture was put forward [31]. It applies some security services and security mechanisms to TCP/IP reference model's layers including application layer, transport layer, internetwork layer and network interface layer. It adapts some technologies of information and network to guarantee the security of data and services in the layers of TCP/IP reference model.

2.3. **PDR.** Internet Security Systems (ISS) [32] in USA put forward the network security architecture named PDR (Protection, Detection and Response). PDR includes three stages including protection, detection and response. It makes use of time scale to measure the ability of network security. It established the theoretical foundation for a series of network security architectures which were generated based on the concept of PDR. It has the guidance significance of many network security architectures. It delivers the requirement of network security by a famous equation which is $P_t > D_t + R_t$, where, P_t denotes the time span of system protection, D_t is the time span of detection from starting intrusion by intruders to recognizing intrusion behavior, R_t means the time span of response from starting intrusion by intruders to finishing response.

2.4. **P2DR.** ISS improved PDR and put forward the network security architecture P2DR (Policy, Protection, Detection, Response) which is shown in figure 2. P2DR is an adaptive network security model. It includes four stages including security policy, protection, detection and response. The latter three stages protection, detection and response constitute a dynamic and rounded circle of network security process. Meanwhile, they ensure the network security under the guidance of the stage of policy.

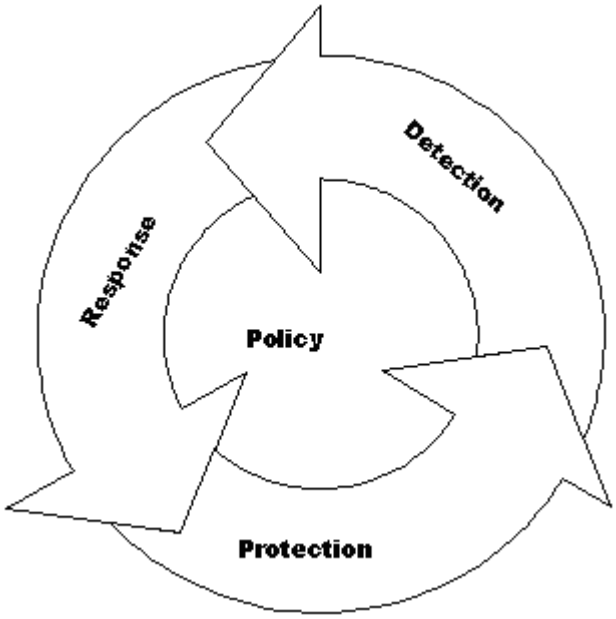

FIGURE 2. P2DR security model [29].

2.5. **P2DR2.** The security architecture P2DR2 (Policy, Protection, Detection, Response, Recovery) adds a stage of recovery based on the security architecture P2DR. It takes the stage of recovery for the same importance of the four stages of policy, protection, detection, response. The five stages of P2DR2 constitute integrated network security architecture.

3. **Proposed Model.**

3.1. **Security Architecture of Proposed Model.** In this paper, a Dynamical Model for Network Security based on Artificial Immunity (DMNSAI) is proposed. The architecture of the proposed model is shown in figure 3. The rectangular with dotted lines denotes the sections of traditional network security defense systems. The ellipse with real lines denotes the links of DMNSAI based on artificial immunity. The thick lines with arrowhead show the flow direction of network status data. DMNSAI consists of Immune Detection Sub-model (IDS), Risk Assessment Sub-model based on immune antibody intensity (RAS) and Response Sub-model based on risk value (RS). IDS adapts the principles and mechanisms of AIS to detect anomaly IP packets in the network traffic. It feeds the detected network threats back to the key defense link of protection which recognizes new harmful network behavior according to the signatures sent by IDS. Meanwhile, it provides the result of detection elements' dynamic evolution for the RAS. RAS generates immune

antibody intensity through detection result of IDS to evaluate the risk of hosts, sub-networks and the whole network. RS responds the network security events according to the risk value. It classifies risk value into different grades. Different network security threats with risk grade leads to special response methods. The results of IDS, RAS and RS are synthesized to dynamically work out the protection policies which guide protection methods in the real computer network. DMNSAI uses the excellent attributes of AIS to dynamically detect the intrusions, evaluate the security risk and respond network security events and provide basis for policy making. The security architecture of DMNSAI is based on the current situation of computer network. It adopts the style of dynamic circle to defend the network security.

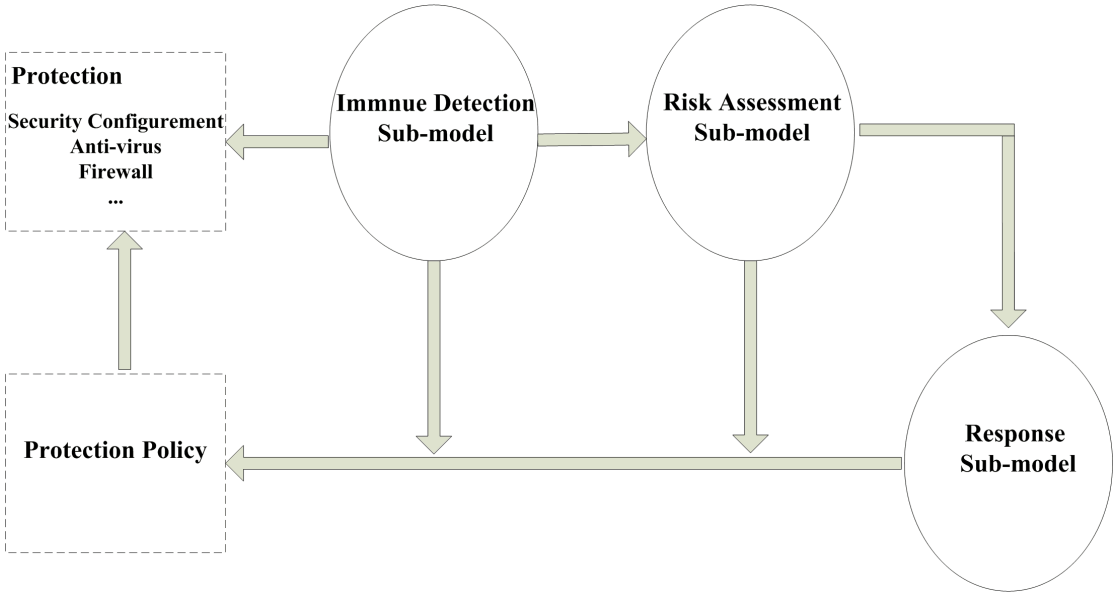

FIGURE 3. The architecture of proposed model.

In the real application, the deploy method of DMNSAI is shown in figure 4. IDS Agent is a distributed point which is connected to the gateway of sub-networks by pass. It captures network traffic and detects network security threats hid in IP packets. It doesn't affect the normal running of sub-networks. Every gateway of sub-networks has an IDS Agent. All the IDS Agents constitute the IDS. An IDS Agent synchronizes with the other agents to improve the ability of global detection. RAS and RS are connected to the router which links the internal network and Internet. RAS receives the dynamic result of detection change in IDS and computes the risk value of computer networks. RS receives the risk value from RAS, deals with the risk value and chooses reasonable response strategy and mechanisms. The result data of IDS, RAS and RS is applied to scientific protection policy of network security to correct the defects of firewalls, anti-virus software and security management. It constitutes a dynamic circle process to defend the network security.

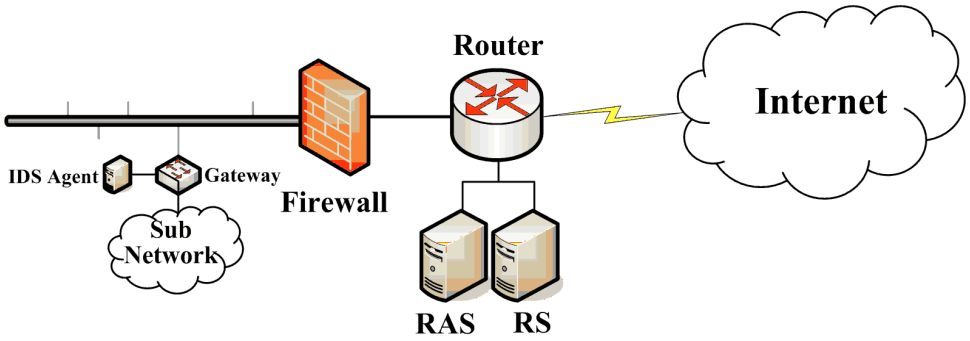

FIGURE 4. Deployment method of proposed model.

3.2. **IDS.** IDS consists of many automated immune detection agent named IDS Agent (IDSA). Its architecture is shown in figure 5. An IDSA is connected to the gateway of a sub-network by pass. It detects network security threats in the scope of local sub-network with the principles and mechanisms of AIS. It works independently. It makes IDS detect network security threats in distribution and parallelity. Furthermore, all IDSAs communicate and share their excellent detection elements (memory detectors) with each other.

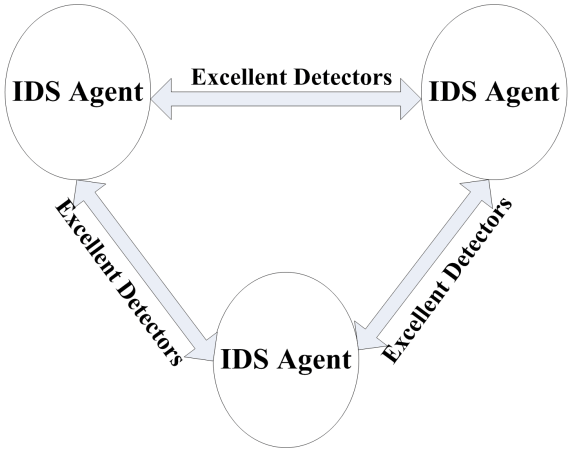

FIGURE 5. The architecture of IDS.

3.2.1. **IDSA.** The architecture of IDSA is shown in figure 6. IDSA captures the network traffic from the gateway of sub-network. It converts the IP packets to immune antigen through the method of presentation. In BIS, antigen presenting cells (APCs) capture and handle antigens. They send the antigens to immune cells which recognize pathogens [7]. The above process is called antigen presentation. In IDSA, detectors are defined to evolve dynamically and detect the abnormal antigens in the antigen set. The network security threats recognized by IDSA are sent to the protection section which directly uses the signatures of detected network security threats to remedy the network security leaks. The foregoing process makes that the proposed model DMNSAI feeds detection results back to the protection methods. Furthermore, the dynamic evolution of detection elements produces

the intensity of detectors. The intensity is sent to RAS which uses detectors' intensity to evaluate the risk value of network security.

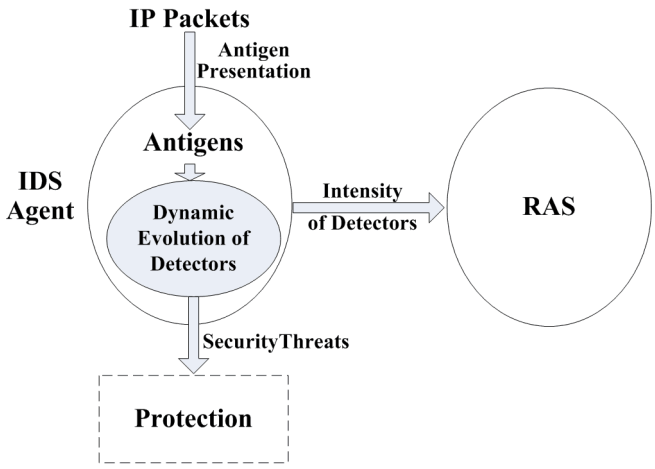

FIGURE 6. The architecture of IDSA.

3.2.1.1. **Simulation of AIS Principles.** In this paper, the AIS principles are used to discover the network security threats in the local sub-network. The first step of judging whether an IP packet is a security threat is to transfer the packets in the network to antigens which have immune styles. We use signature information of packets in the local sub-network to simulate the antigens in the immune system. Let the antigen set in the local sub-network environment be *Ag* that meets $Ag = \{ag | ag \in U, |ag| = l, ag = GetSig(packet)\}$, where, $Ag \subset U$, $U = \{0,1\}^l$, $GetSig()$ is a function which extracts the signature information of network data package, *packet* is a network data package in the sub-network. The antigen *ag* is made up of *l*-long (*l* is a nature number) binary strings. Let the normal packet set and abnormal packet set with network security threats be S and *N*, separately. *S* and *N* meet $S \cup N = Ag, S \cap N = \varnothing$. Furthermore, *S* and *N* are shown in Eq. (1) and (2), respectively.

$$S = \{self \,|self \in Ag, self = GetSig(NormalPacket)\} \tag{1}$$

$$N = \{nonself \,|nonself \in Ag, nonself = GetSig(AbnormalPacket)\} \tag{2}$$

The immune cells in the immune system are used to discover pathogens hid in the antigens. In IDSA, the detector is defined to simulate the immune cells in the immune system. Let the detector set be $D = \{\langle gene, age, count, type, family\rangle | gene \in Ag, age, count, type, family \in N\}$, where, *gene* is the detector's gene, it is a binary string which matches antigens, *N* is a nature number set, *count* is the number of antigens matched by the detector, *age* is the life generations of the detector, *type* denotes the type of the detector, $type \in \{i, m, r\}$, the three elements delegate immature detector, mature detector and memory detector respectively, *family* is the serial number of the detector ethnic group, it is

corresponding to the ID number of a network security threat.

The detector set includes immature, mature and memory detectors. Let the data set of them be D_I, D_M and D_R, respectively. D_I simulates the initial stage of immune cells in AIS. They are newly generated detectors. It meets $D_I = \{d \mid d \in D, d.type = i, d.age < \alpha, d.count = 0, d.family = parent.family\}$, *parent.family* is the serial number of the ethic group of a memory detector which generates the immature detector, α is the tolerance threshold of the immature detector, *count* is the number of normal antigens matched by the immature detector, once the detector matches a self antigen, namely, $count > 0$, it dies. The mature detector set D_M simulates the medium stage of immune cells in AIS. It is evolved to by an immature one. It meets $D_M = \{d \mid d \in D, d.age < \lambda, d.count < \delta\}$, where, λ is the lifecycle of the mature detector, δ is the active threshold of the mature detector. The memory detector set D_R simulates the highest evolution stage of immune cells in AIS. It is evolved to by a mature one or switched to by the system manager with the signature information of a known network security threat. It meets $D_R = \{d \mid d \in D, d.age \geq \lambda, d.count \geq \delta\}$. It contains the accurate signature which can recognize network security threats.

3.2.1.2. **Simulation of AIS Mechanisms.** The function $f_{match}()$ is constructed to compute whether a detector matches an antigen. Presently, feasible matching methods include *r*-Contiguous, Hamming, Euclidean, and etc. Let a detector be *d* and an antigen be *ag*. $f_{match}()$ is shown in Eq. (3).

$$f_{match}(d, ag) = \begin{cases} 1, & \text{match} \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

Where, the return value 1 denotes that *d* matches *ag*, and vice versa.

In BIS, the self-tolerance process is used to judge whether an immature detector recognizes self-elements in the self-set. The immature detectors which match any self-elements come to death. Let $f_{tolerance}()$ be the math function used to accept self-tolerance. $f_{tolerance}()$ is shown in Eq. (4).

$$f_{tolerance}(D_{I\_new'}) = \{d \mid d \in D_{I\_new'}, d.age \geq \alpha, \exists s \in S \wedge f_{match}(d, s) = 0\} \tag{4}$$

Where, $D_{I\_new'}$ is an immature detector set, α is the threshold of the tolerance time of the immature detector, the function returns the immature ones which did not recognize (match) any self-elements and would evolve to mature ones.

3.2.1.3. **Dynamic Evolution of Detectors.** IDSA adopts dynamic immune evolution mechanisms to make detectors be more excellent. The process of dynamic detector evolution is shown in figure 7. The whole evolution stages mean a circle. Memory detectors may generate immature detectors. Immature detectors evolve to mature detectors through self-tolerance. Mature detectors which are activated by antigens evolve to memory detectors. At the same time, in IDSA, the concept of gene library is adopted to generate more effective immature detectors. It can improve the livability of immature detectors.

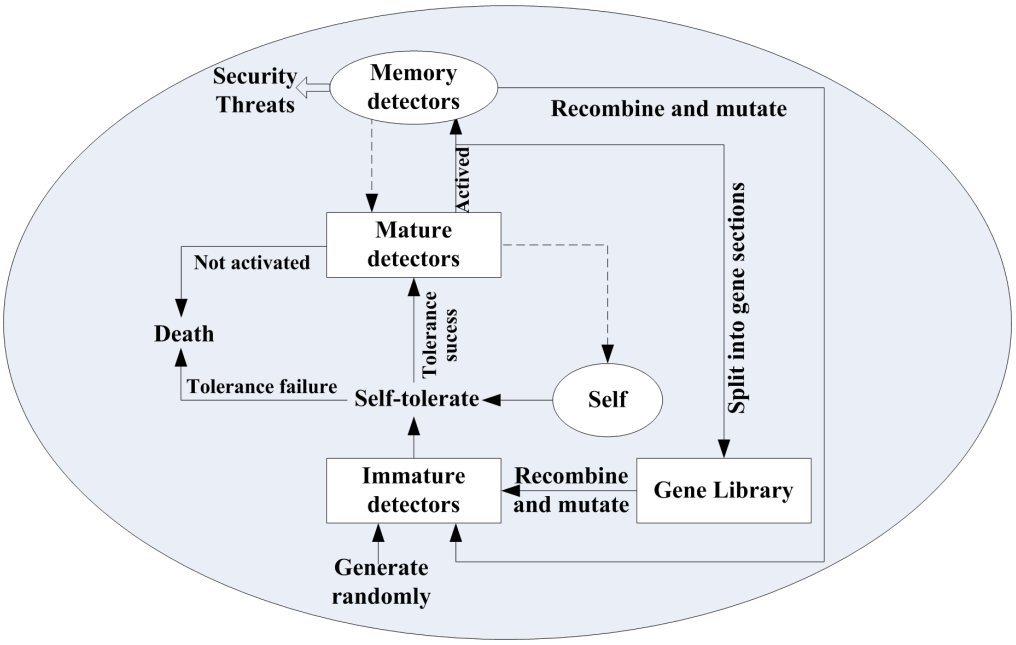

FIGURE 7. Dynamic evolution of detectors.

In IDSA, heterogeneous immature detectors are generated to improve the detection ability of the proposed model. The main task of the immature detector generation is to produce its gene string. IDSA adopts the following two generating ways. First, the immature gene is produced by the ways of cross, mutation and recombination with memory detectors' genes. Second, *l*-long binary string is randomly generated to form the gene of an immature detector.

The immature detector set $D_I(t)$ at the moment *t* is shown in Eq. (5).

$$D_I(t)=\begin{cases}\varnothing,\ t=0\\ D_I(t-1)-f_{tolerance}\left(D_I(t-1)\right)-D_{I\_death}(t-1)\cup D_{I\_new}(t),\ t>0\end{cases} \tag{5}$$

Where, $D_{I\_death}(t-1)$ denotes the immature detectors which failed to pass the self-tolerance. $D_{I\_new}(t)$ denotes the immature detectors newly generated at the moment *t*.

After the immature detectors passed the process of self-tolerance, they take possession of the initial ability to detect network security threats and will evolve to mature ones. Partial captured antigens in *Ag* are proportionally selected to be input into IDSA to train mature detectors. The mature detector set $D_M(t)$ at the moment *t* is shown in Eq. (6).

$$D_M(t)=\begin{cases}\varnothing,\ t=0\\ D_M(t-1)-D_{M\_death}(t-1)-D_{M\_toR}(t-1)\cup ToMatureCell(\ ),\ t>0\end{cases} \tag{6}$$

Where, $D_{M\_death}(t-1)$ denotes the mature detectors which failed to be activated, $D_{M\_toR}(t-1)$ denotes the mature ones which were activated, the function of $ToMatureCell(\ )$ is to transform immature detectors to mature ones, the parameter of

$ToMatureCell(\ )$ is the immature detector set $f_{tolerance}\left(D_I(t-1)\right)$ which succeeded to pass self-tolerance.

After the mature detectors are activated, they have owned enough detection ability against security threats. In IDSA, a message about the activation event of a mature detector is sent to the network security administrator. The administrator co-stimulates the mature detector and confirms that it is switched to a memory detector. The memory detector is immortal. When it matches a harmful antigen(network security threat), it enters the status of activation and new immature detectors proliferate with it. Through the above mechanism, the activated memory detector expands the amount of its ethic group. The memory detector set $D_R(t)$ at the moment *t* is shown in Eq. (7).

$$D_R(t)=\begin{cases}\{r_1,\ldots,r_i,\ldots r_n\},\ i,n\in N,\ t=0\\ D_R(t-1)\cup ToMemoryCell\left(D_{M\_toR}(t-1)\right),\ t>0\end{cases} \tag{7}$$

Where, the function of $ToMemoryCell()$ is to transform $D_{M\_toR}(t-1)$ to memory detectors, $ToMemoryCell\left(D_{M\_toR}(t-1)\right)$ returns the memory detectors newly generated.

After being detected, the antigen set *Ag* is classified into network security threats and normal antigens. To improve the self-adaptation ability of IDSA in the local sub-network environment, the validated normal antigens will be switched to self-elements to train the immature detectors newly generated. Let the set of the validated normal antigens be $Ag_{normal}(t-1)$ at the moment *t*-1. The self-set $S(t)$ at the moment *t* is shown in Eq. (8).

$$S(t)=\begin{cases}\{s_1,\ldots,s_i,\ldots,s_n\},\ i,n\in N,\ t=0\\ S(t-1)\cup ToSelfCell\left(Ag(t-1)\right),\ t>0\end{cases} \tag{8}$$

Where, the function of $ToSelfCell()$ is to transform the validated normal antigens to self-elements.

3.2.2. **Detection of Network Security Threats.** Let the library of network security threats set be *A* which is shown in Eq. (9).

$$\begin{aligned}A=\{\langle attackID,name,content,count\rangle\,|\,\forall d\in D_R,attackID=\\ d.attackID,attackID,count\in N,name,content\in ASCII\}\end{aligned} \tag{9}$$

Where, *attackID* is the sequence number of the network security threat, it is equal to *attackID* of the corresponding memory detector, *name* is the name of network security threat, *content* is the description of the network security threat, *ASCII* is the ASCII character set.

Every memory detector is related to a network security threat. The memory detector uses its gene to capture antigens. Once its gene matches an antigen, the proposed model queries the corresponding network security threat information of the memory detector in the library and sends alarm information to the network administrator.

Let $D_{R\_detect}(t)$ be the memory detectors which recognize harmful antigens at the moment *t*. $D_{R\_detect}(t)$ is shown in Eq. (10).

$$D_{R\_detect}(t)=\left\{d\left|\forall d\in D_R(t),\exists ag\in Ag(t),\ f_{match}(d,ag)=1\right.\right\} \quad (10)$$

Where, $D_R(t)$ and $Ag(t)$ denote the memory detector set and the antigen set at the moment *t*, respectively.

3.2.3. **Synchronization of IDSAs.** The Synchronization process of all IDSAs is shown in figure 5. In BIS, the conception of vaccination is that a vaccinum is injected into biological bodies to make the biological bodies be immune to special pathogens. In this paper, the above mechanism is simulated to vaccinate all the IDSAs in the global scope of the networks. The process of vaccination is called synchronization of IDSAs. It can make all the detection agents have the recognition ability of new network security threats. Each local IDSA generates excellent learning achievements (memory detectors). In a local detection agent, detectors detect and accept the training of the input antigens. With the mechanisms of self-adaptation and self-learning, antigens can train some enough excellent detectors to recognize mutated, even new unknown security threats. These good detectors which own the accurate detection ability to recognize harmful antigens and are good at adapting local network environment are new memory detectors. However, it takes the cost of much resource and time to generate new memory detectors. The other detection agents are not necessary to consume some cost to train the same memory detectors. Therefore, the learning achievements in a local agent need to be shared with the other agents to improve the global detection ability in the whole computer networks.

3.3 **RAS.** The key question of quantitative risk assessment of network security is how to compute the intensity value of security threats confronted by networks. In this paper, the intensity formulation mechanism of immune cells in an immune system is simulated to quantificationally express the security threat intensity. In the biological immune system, when recognizing specific pathogens, the activated immune cells quickly perform the process of clonal expansion. They generate plasmacytes to form a lot of antibodies. The new antibodies expand the scale of ethic group of the activated immune cells to eliminate massive pathogens. Through the above mechanism, memory detectors in the proposed model use the clonal expansion to form the intensity of security threats which are relative to their corresponding memory detectors.

Let the memory detector which recognizes an harmful antigen be r_{detect}. IDS uses r_{detect} to implement the process of clonal expansion. It takes advantage of the gene of r_{detect} to generate new immature detectors with the operations of cross, mutation and recombination. The new immature detectors inherit the serial number of r_{detect}. In the process of ethic group expansion of r_{detect}, when r_{detect} recognize an antigen, the amount of new immature detectors cloned by r_{detect} is $\xi=\lceil \tau ar\sinh(d_{detect}.count)\rceil$, where, τ is a coefficient of ethic group expansion. Along with the constant growth of harmful antigens detected by r_{detect}, the number of ethic group increases sharply to form the intensity of network security threats.

The above mechanism of ethic group change of a memory detector reflects the real-time intensity change of security threats in network environment. The coned immature detectors

which succeed to accept self-tolerance will evolve to new mature detectors. Therefore, the number of ethic group of r_{detect} is equal to the number of immature and mature detectors whose ethic group number is $r_{detect}.family$. The intensity of security threats confronted is expressed by the number of ethic group of r_{detect}.

Let the harmfulness value of a security threat be h_i (i is the ID number of No. i security threat). Let the importance value of a sub-network be v_j (j is the ID number of the No. j sub-network). The security risk R_j of the No. j sub-network is shown in Eq. (11).

$$R_j = 1 - \frac{1}{1 + \ln\left(v_j \sum_{i=1}^{m} \left(h_i \left(Count\left(d_I.family = i \right) + Count\left(d_M.family = i \right) \right) \right) + 1 \right)} \tag{11}$$

Where, m is the sum of the security threats confronted by No. j sub-network, $d_I \in D_I$, $d_M \in D_M$, $d_I.family = d_M.family = i$, the function $Count(\ )$ counts the sum of detectors according to the condition in accordance with its parameter.

The total security risk R of the global computer network is shown in Eq. (12).

$$R = \sum_{j=1}^{n} \left(\frac{v_j}{\sum_{i=1}^{n} v_i} * R_j \right) \tag{12}$$

Where, n is the sum of all the sub-networks.

3.4. **RS.** The risk value R computed by RAS is sent to RS which classifies the risk value into different danger grades. The greater the risk value is, the more dangerous the network is. The risk value 0 and 1 are theoretical limitation values. The former denotes that there are not any dangerous factors in the network. The latter denotes that the network confronts the highest danger and is broken down. According to the sections of the risk value of network security, the danger grade of network security is divided into seven grades including Lowest, Lower, Low, Common, High, Higher and Highest. The division of security risk value is shown in Table 1.

TABLE 1. Division of security risk value

Risk Value	(0, 0.1]	(0.1, 0.2]	(0.2, 0.4]	(0.4, 0.6]	(0.6, 0.8]	(0.8, 0.9]	(0.9, 1)
Danger Grade	Lowest	Lower	Low	Common	High	Higher	Highest

The seven sections of risk value delegate seven danger grades of the network. Special network security threats cause the danger grade of the sub-network and the whole computer network. The library set A of network security threats is shown in Equation (9). In the expert knowledge base of response, a network security threat has a corresponding treatment policy. A special response tool or method is chosen to deal with the network security threat

detected by IDS.

4. **Conclusion.** The openness of computer network makes the network security environment be complicated and changeful. It requires that the protection process of network security needs to synthesize the data of all links of the network security architecture. To avoid the problem of relax relation of the stages and links in the conventional network security architectures, a dynamical model for network security based on artificial immunity named DMNSAI is proposed. The proposed model uses the principles and mechanisms of AIS to detect, evaluate the security risk of and respond network security threats. It improves the ratio of detection, accuracy of risk assessment and rationality of response. Furthermore, the proposed model synthesizes the results of the stages detection, risk assessment and response. It provides the scientific basis for the formulation of security defense policy and the choice of security defense methods. It makes the defense process of computer network be dynamic and circular.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (No. 61103249), the Scientific Research Fund of Sichuan Provincial Education Department (No. 10ZC106) and the Scientific Research Fund of Leshan Normal University (No. Z1113 and Z1065).

REFERENCES

[1] National Security Agency, Information assurance technical framework (IATF), 1998.

[2] C. X. Shen, Thinking of strengthening the defense architecture of information security, *Network & Computer Security*, no. 9, pp. 7-10, 2002.

[3] http://www.gov.cn/gzdt/2011-05/06/content_1858667.htm.

[4] http://www.miit.gov.cn/n11293472/n11295344/n11297007/12425553.html.

[5] C. Y. Zhang, *Network security architecture*, University of Electronic Science and Technology of China Press, Chengdu, 2006.

[6] C. Su and Z. L. Yin, Model of network security based on immune agents, *Computer Engineering and Design*, vol. 24, no. 2, pp. 30-32, 2003.

[7] T. Li, *Computer immunology*, Publishing House of Electronics Industry, Beijing, 2004.

[8] H. W. Mo and X. Q. Zuo, *Artificial Immune System*, Science Press, Beijing, 2009.

[9] S. A. Hofmeyr and S. Forrest, Architecture for an artificial immune system, *Evolutionary Computation*, vol. 8, no. 4, pp. 443-473, 2000.

[10] S. Forrest and A. S. Perelson, Self-nonself discrimination in a computer, *Proc. of IEEE Symposium on Security and Privacy*, Oakland, CA, pp. 202-213, 1994.

[11] P. K. Harmer, P. D. Williams, et al, An artificial immune system architecture for computer security applications, *IEEE Transaction on Evolutionary Computation*, vol. 6, no. 3, pp. 252-280, 2002.

[12] R. B. Xiao and L. Wang, Artificial immune system: principle, models, analysis and perspectives, *Chinese Journal of Computer*s, vol. 25, no. 12, pp. 1281-1293, 2002.

[13] L. C. Jiao and H. F. Du, Development and prospect of the artificial immune system, *Acta Electronica Sinica*, vol. 31, no. 10, pp. 1540-1548, 2003.

[14] http://www.artificial-immune-systems.org/icaris.shtml.

[15] P. D'haeseleer, S. Forrest, and P. Helman, An immunological approach to change detection algorithms: Analysis and implication, *Proc. of IEEE Symposium on Security and Privacy*, Las Alamitos, CA, USA, pp. 110-119, 1996.

[16] D. Dasgupta, An immune agent architecture for intrusion detection, *Proc. of GECCO'2000*, Las Vegas, Nevada, USA, 2000.

[17] J. Kim and P. J. Bentley, Evaluating negative selection in an artificial immune system for network intrusion detection, *Proc. of GECCO'2001*, 2001.

[18] J. O. Kephart, G. B. Sorkin, et al. Blueprint for a computer immune system, *Proc. of the 1997 International Virus Bulletin Conference*, SanFrancisco, California, 1997.

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

[20] T. Li, An immunity based network security risk estimation, *Science in China Series F-Information Sciences*, vol. 48, no. 5, pp. 557-578, 2005.

[21] Y. F. Wang, et al. A real-time method of risk evaluation based on artificial immune Ssystem for network security, *Acta Electronica Sinica*, vol. 33, no. 5, pp. 945-949, 2005.

[22] T. Li, An immune based model for network monitoring, *Chinese Journal of Computers*, vol. 29, no. 9, pp. 1515-1522, 2006.

[23] J. L. Ding, X. J. Liu, et al. Dynamic computer forensics based on artificial immune system against network intrusion, *Journal of Sichuan University(Engineering Science Edition)*, vol. 36, no. 5, pp. 108-111, 2004.

[24] L. N. De Castro, F. J. Von Zuben. An evolutionary immune network for data clustering, *Proc. of the IEEE SBRN'00 (Brazilian Symposium on Artificial Neural Net-works)*, Rio de Janeiro, Brazil, 2000.

[25] K. KrishnaKumar and J. Neidhoefer, Immunized adaptive critics for level 2 intelligent con-trol, *Proc. of the IEEE SMC'97*, Orlando, FL, 1997.

[26] K. Ogawa, Application of immune algorithms to combinatorial optimization for traffic safety countermeasures, *Proc. of SICS&ISIS*, San Diego, CA, 2002.

[27] S. Forrest, B. Javornik, R. E. Smith and A. S. Perelson, Using genetic algorithms to explore pat-tern recognition in the immune system, *Evolutionary Computation*, vol. 1, no. 3, 1993.

[28] Y. Ishida, Fully distributed diagnosis by PDP learning algorithm: towards immune network PDP model, *Proc. of the Int. Joint Conf. on Neural Networks*, 1990.

[29] ISO 7498-2-1989, Information Processing Systems-Open Systems Interconnection-basic Reference Model-Part 2: Security Architecture.

[30] T. Li, An introduction to computer network security, *Publishing House of Electronics Industry*, Beijing, 2004.

[31] L. Li, Information and Network Security, http://home.sysu.edu.cn/wisdom/download/network_security.ppt, 2007.

[32] IBM Internet Security Systems, http://www.iss.net/.