Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2016, Article ID 4517019, 10 pages
http://dx.doi.org/10.1155/2016/4517019

Research Article

A Quantitative Risk Evaluation Model for Network Security Based on Body Temperature

Y. P. Jiang, C. C. Cao, X. Mei, and H. Guo

School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou, Henan 450002, China

Correspondence should be addressed to C. C. Cao; caocongcong0418@163.com

Received 8 April 2016; Revised 29 June 2016; Accepted 20 July 2016

Academic Editor: Tzonelih Hwang

These days, in allusion to the traditional network security risk evaluation model, which have certain limitations for real-time, accuracy, characterization. This paper proposed a quantitative risk evaluation model for network security based on body temperature (QREM-BT), which refers to the mechanism of biological immune system and the imbalance of immune system which can result in body temperature changes, firstly, through the r-contiguous bits nonconstant matching rate algorithm to improve the detection quality of detector and reduce missing rate or false detection rate. Then the dynamic evolution process of the detector was described in detail. And the mechanism of increased antibody concentration, which is made up of activating mature detector and cloning memory detector, is mainly used to assess network risk caused by various species of attacks. Based on these reasons, this paper not only established the equation of antibody concentration increase factor but also put forward the antibody concentration quantitative calculation model. Finally, because the mechanism of antibody concentration change is reasonable and effective, which can effectively reflect the network risk, thus body temperature evaluation model was established in this paper. The simulation results showed that, according to body temperature value, the proposed model has more effective, real time to assess network security risk.

1. Introduction

With the continuous expansion of network size and the increasingly complex network structure and the rapid development of information technology, the research of assessment model has become one of the hot topics in network security field. Bass was the first one who proposed the definition of network situation awareness [1]. The boom of the network security situation awareness has been laid out. In the past two decades, the experts and scholars not only use Analytic Hierarchy Process (AHP) [2, 3], attacking graph [4, 5], and Bayesian network [6, 7] to study the risk assessment but also make use of the hidden Markov model [8, 9] to discuss the field. With the advent of Computer Immunology, the researchers began to study the domain based on artificial immune [10, 11], such as that based on antibody concentration [12] of network risk assessment. In the meantime, from static to dynamic state, it is relatively according with the realistic environment.

Kotenko and Chechulin had proposed a safety assessment framework based on attack graph [13]. The method has higher computational complexity. Taking into consideration the impact of time and environmental factors, Khosravi-Farmad et al. proposed a quantitative risk assessment method by using Bayesian attack graph [14]. Literature [15] has put forward an architecture based on feed propagation neural, intelligent computing of the probability of occurrence of a network attack. Rezvani et al. proposed a new risk assessment methodology [16], and the algorithm included two concepts: the first one, the dependence of risk score between the source host and destination host, and, the second one, the risk of transmission between the network flows. Based on these two concepts, they have developed an iterative algorithm to calculate the host of risk scores and network flow, which make the algorithm convergence speed fast. Not only is the study of risk assessment very important for government agency, research institutes, and large-scaled enterprises, but

it is also important for risk assessment of military networks. Hemanidhi et al. have put forward a military network risk assessment framework [17]. Using the experiments of Wu et al., it has been proven that the effectiveness of the security threats recognition and analysis method was based on attack graph [18]. Situation assessment method was based on hidden Markov model (HMM), by Li et al. [8], which can be relatively more accurate to reflect the security situation of the current complex network environment. However, some experiences can affect the objectivity of the results. Xi et al. improved the network security situation assessment method based on the HMM [9], so that the quantitative result is more reasonable. Nevertheless, the method of collecting the accuracy of the data source needs to be improved. Literature [19] proposed a network security situation assessment method based on immune danger theory, but the method cannot perceive more situational factors and complex network security situation.

Although the above literature can be accurately used to evaluate network security, the result of evaluating the network environment lacks certain flexibility. And due to people unattended and hostile deployment in wireless sensor networks [20], it is a critical security issue. In the meantime, some scholars refer to sensors for human activity monitoring [21, 22]. Thus, this paper puts forward a quantitative risk evaluation model for network security based on body temperature (QREM-BT), and the model makes characterization of the network of the immune system more in line with the biological immune system. It can be used to assess network security risk.

2. The Model of Basic Theory and Design Idea

Biological immune system is a highly distributed, self-adaption, and self-learning system. It has a sound mechanism to resist the invasion of foreign pathogens. After the body is infected with a pathogen, it can produce specific antibody and effector T cells to improve the immunity of the pathogen. But when the biological immune system itself is before the recovery of adaptive regulation, it will produce fever and other symptoms; with the increase in virus threats intensity, the biology of temperature also can be increased. Thus, when computer is attacked by outside illegal attacks or internal network illegal activity, according to the mechanism of biological immune system, antibody in computer immune system can quickly recognize these antigens. By increasing the antibody concentration, corresponding to the body temperature of the computer will also increase with a certain rising trend; at the same time, the network of multiple computers can also evaluate body temperature status of the entire network based on the importance of each computer. According to the body temperature evaluating the network risk, the body temperature value size can be more convenient, more directly determine risk levels, and make the corresponding protective measures.

QREM-BT model is composed of three parts, namely, intrusion detection, antibody concentration, and body temperature assessment. Design idea is briefly summarized as follows. (1) These detected attacks are classified by the blood [23]. (2) According to the matching process of antigen and antibody, it could calculate the corresponding attack types of antibody concentration. (3) For body temperature based on antibody concentration, the body temperature range could also be mapped to a defined body temperature area through the body temperature to assess network risk.

3. Risk Analysis and Calculation Based on QREM-BT Model

In order to more accurately and real-time assess network security risk, the model uses r-contiguous bits nonconstant matching rate algorithm to improve the detection quality of detector [24]. In order to meet the real network environment, self, various detectors, and the corresponding tolerance all are dynamic changes. For more intuitively obtaining risk assessment, the model determines risk level by temperature change.

Let self/nonself in the domain $X \in \{0,1\}^l$ $(l > 0)$, S is the self-set (the normal behavior of the network), and N is the nonself-set (network illegal behavior or attack), with $S \subset X$, $N \subset X$, $S \cup N = X$, $S \cap N = \varnothing$. Detector set D: $D = \{d_1, d_2, \ldots, d_n\}$ $(l_i \le l,\ i \in N)$. Antigen $(\mathrm{Ag} \subset X)$ is defined as network intrusion behaviors, identifying antigen of antibody $(\mathrm{Ab} \subset D)$ as detector.

3.1. The Dynamic Evolution Process of Self. In the actual network environment, S and N are usually unsteady. The dynamic evolution equation of self is defined as

$$S(t) = \begin{cases} S(0), & t = 0, \\ S(t-1) - S_{S \to N}(t), & t > 0 \wedge S(t) \le \delta, \\ S(t-1) - S_{\mathrm{dead}}(t) - S_{S \to N}(t) + S_{\mathrm{new}}(t), & t > 0 \wedge S(t) > \delta, \end{cases} \quad (1)$$

where δ is the threshold of self-set size, $S_{S \to N}$ is the change of network environment caused by self-variation (self-change into nonself), and S_{dead} show when the self-set size is more than the threshold on the basis of LRU principle to eliminate the number of self-sets.

3.2. r-Contiguous Bits Nonconstant Matching Algorithm. Because the constant r-contiguous bits matching algorithm will be unable to more accurately detect illegal network behavior, the matching process of antigen and antibody uses r-contiguous bits nonconstant matching rate algorithm [10].

The algorithm utilizes the segmentation technology and key position according to the importance of each section set different from the matching threshold.

In order to avoid the "black hole" and reduce missing rate or false detection rate, while improving the detection quality of the detector, we have the following matching calculation

method, where "1" represents "match" and "0" represents "mismatch":

$$
\begin{aligned}
g_{\text{match}}\left(F_1, F_2, r\right) &= \begin{cases} 1, & f \geq r,\ F_1 \in D,\ F_2 \in X \\ 0, & \text{otherwise,} \end{cases} \\
f &= \sum_{i=1}^{n} \alpha_i \text{match}\left(i\right), \\
\sum_{i=1}^{n} \alpha_i &= 1, \\
\text{match}\left(i\right) &= \begin{cases} 1, & \text{iff } \exists i, j \left(x_{\text{Key}_{i,j}} = x_{\text{Key}_i},\ i, j \in N^*\right) \vee \exists i, m, n \left(n - m \geq r,\ 0 < m, n \leq \dfrac{L}{M},\ r \in N^*\right) \\ 0, & \text{otherswise,} \end{cases}
\end{aligned}
\tag{2}
$$

where the length of the match string F_1, F_2 was L and they are, respectively, divided into M segments, set key position is represented by $\text{Key}_{i,j}$ in key field, the matching threshold of each field is set as α_i, $x_{\text{Key}_{i,j}} = x_{\text{Key}_i}$ represents the key position of fragment i the same as $\text{Key}_{i,j}$, and f is defined as the sum of each fragment of the matching threshold multiplied by 1 or 0.

3.3. The Dynamic Evolution Process of Detector Self-Tolerance. In order to prevent the detector match with self, detector will experience self-tolerance (if detector and S matching succeeds, discard the detector) to improve the effectiveness of the detector. The dynamic evolution equations of detector self-tolerance are as follows:

$$
\begin{aligned}
&T\left(t\right) \\
&= \begin{cases} T\left(0\right), & t = 0, \\ T\left(t-1\right) - T_{\text{tolerance}}\left(t\right), & t > 0 \wedge t < T, \\ T\left(t-1\right) - T_{\text{tolerance}}\left(t\right) + T_{\text{random}}\left(t\right), & t > 0 \wedge t \geq T, \end{cases}
\end{aligned}
$$

$$
T_{\text{tolerance}}\left(t\right) = \left\{ y \mid y \in T\left(t\right),\ \exists x \in S \wedge f_{\text{match}}\left(x, y\right) = 0 \right\},
\tag{3}
$$

where T is the updating cycle of detector, $T_{\text{tolerance}}(t)$ is that t moment of mature detectors through the process of tolerance, and $T_{\text{random}}(t)$ is randomly generated immature detector.

3.4. The Dynamic Evolution Process of Mature Detectors. In a certain period of time, mature detector accumulates enough matching string (greater than or equal to n), the memory detector will be activated, and, after activation, matching number will reset as zero. When the set size of memory detector reaches the limit, a part of the memory detector will be converted to mature detector (use LRU elimination rule).

Definition 1. Mature detector changes can be divided into two parts: increase and reduction. The increase of mature detector is defined as $D_{\text{Ma}}^{\text{increase}}$; the reduction of mature detector is defined as $D_{\text{Ma}}^{\text{reduction}}$.

The increase of mature detector is as follows:

$$
D_{\text{Ma}}^{\text{increase}}\left(t\right) = \begin{cases} D_{\text{Ma}}^{\text{initial}\to\text{Ma}}\left(t\right) + D_{\text{Ma}}^{\text{clone}}\left(t\right), & t > 0 \wedge D_{\text{Mr}}\left(t\right) < \theta, \\ D_{\text{Ma}}^{\text{initial}\to\text{Ma}}\left(t\right) + D_{\text{Ma}}^{\text{clone}}\left(t\right) + D_{\text{Ma}}^{\text{Mr}\to\text{Ma}}\left(t\right), & t > 0 \wedge D_{\text{Mr}}\left(t\right) \geq \theta. \end{cases}
\tag{4}
$$

The reduction of mature detector is as follows:

$$
D_{\text{Ma}}^{\text{reduction}}\left(t\right) = D_{\text{Ma}}^{\text{Ma}\to\text{Mr}}\left(t\right) + D_{\text{Ma}}^{\text{dead}}\left(t\right) \quad \left(t > 0\right).
\tag{5}
$$

Mature detector overall evolution equation is as follows:

$$
\begin{aligned}
&D_{\text{Ma}}\left(t\right) \\
&= \begin{cases} D_{\text{Ma}}\left(0\right), & t = 0, \\ D_{\text{Ma}}\left(t-1\right) + D_{\text{Ma}}^{\text{increase}}\left(t\right) - D_{\text{Ma}}^{\text{reduction}}\left(t\right), & t > 0, \end{cases}
\end{aligned}
\tag{6}
$$

where $D_{\text{Ma}}^{\text{initial}\to\text{Ma}}(t)$ is that t moment when the number of initial detector self-tolerances changes into mature detectors, $D_{\text{Ma}}^{\text{Mr}\to\text{Ma}}(t)$ is that t moment when the number of

memory detectors changes into mature detectors when the set size of memory detector reached the limit, $D_{\mathrm{Ma}}^{\mathrm{Ma}\to\mathrm{Mr}}(t)$ shows that t moment when the number of mature detectors reaching activation threshold becomes memory detectors, $D_{\mathrm{Ma}}^{\mathrm{clone}}(t)$ denotes that t moment the number of clone mature detectors, $D_{\mathrm{Ma}}^{\mathrm{dead}}(t)$ shows that, in a certain period of time, mature detector cannot accumulate enough matching string causing the number of dead mature detectors, and θ is the max value of memory detector scale.

3.5. The Dynamic Evolution Process of Memory Detectors. The size of clone scale and activation threshold can change the number of memory detectors. Under certain conditions, memory detector may mutate. Although memory detector relatively has a long life cycle, this kind of detector size has certain limits. Therefore, the value of more than one predefined threshold will be eliminated in accordance with the LRU rule.

The dynamic evolution equations of memory detector are as follows:

$$\begin{aligned}
&D_{\mathrm{Mr}}(t)\\
&= \begin{cases} D_{\mathrm{Mr}}(0), & t = 0,\\ D_{\mathrm{Mr}}(t-1) + D_{\mathrm{Mr}}^{\mathrm{new}}(t) - D_{\mathrm{Mr}}^{\mathrm{reduction}}(t), & t > 0 \wedge D_{\mathrm{Mr}}(t) < \theta,\\ D_{\mathrm{Mr}}(t-1) - D_{\mathrm{Mr}}^{\mathrm{Mr}\to\mathrm{Ma}}(t) - D_{\mathrm{Mr}}^{\mathrm{dead}}(t), & t > 0 \wedge D_{\mathrm{Mr}}(t) \geq \theta, \end{cases}\\
&D_{\mathrm{Mr}}^{\mathrm{new}}(t) = D_{\mathrm{Ma}}^{\mathrm{active}}(t) + D_{\mathrm{Mr}}^{\mathrm{clone}}(t),\\
&D_{\mathrm{Mr}}^{\mathrm{reduction}}(t) = D_{\mathrm{Mr}}^{\mathrm{dead}}(t) + D_{\mathrm{Mr}}^{\mathrm{variation}}(t),\\
&D_{\mathrm{Mr}}^{\mathrm{dead}}(t)\\
&= \{x \mid x \in D_{\mathrm{Mr}}(t-1),\ \exists y \in S(t-1) \wedge f_{\mathrm{match}}(x,y) = 1\},
\end{aligned} \tag{7}$$

where $D_{\mathrm{Mr}}^{\mathrm{dead}}(t)$ is the number of memory detectors which matches self, $D_{\mathrm{Ma}}^{\mathrm{active}}(t)$ shows the amount of memory detectors activated by mature detector, $D_{\mathrm{Mr}}^{\mathrm{clone}}(t)$ is the number of clone memory detectors, and $D_{\mathrm{Mr}}^{\mathrm{variation}}(t)$ means the amount of memory detectors mutating into immature detectors.

3.6. The Antibody Concentration Quantitative Calculation Model. Antibody concentration change is due to the illegal intrusion (antigen) computer immune system producing the immune response caused by the imbalance in the immune system; more antigens caused more serious imbalance; that is, the antibody concentration change is more obviously rising, after the antigen disappeared (killed), and gradually tends to be normal, but there is a certain duration; if for a long time there is no matching with antigen, the antibody concentration will be attenuated according to certain rules.

Definition 2. The formula of increasing antibody concentration is defined as

$$C_{\mathrm{ab}}(t) = C_{\mathrm{ab}}(0) + kC_{\mathrm{ab}}(t-1), \quad k \in (0,1), \tag{8}$$

where $k = (D_{\mathrm{Ma}}^{\mathrm{active}}(t) + D_{\mathrm{Mr}}^{\mathrm{clone}}(t))/(D_{\mathrm{initial}}(t) + D_{\mathrm{Ma}}(t) + D_{\mathrm{Mr}}(t))$.

The above formula can be converted to $C_{\mathrm{ab}}(t) = ((1-k^t)/(1-k))C_{\mathrm{ab}}(0)$ $(0 < k < 1 \wedge t > 0)$, when $t \to +\infty$ antibody concentration tends to be

$$C_{\mathrm{ab}}(t) = \frac{1}{1-k}C_{\mathrm{ab}}(0), \quad k \in (0,1), \tag{9}$$

where the initial of antibody concentration is $C_{\mathrm{ab}}(0)$, k is antibody concentration increase factor, and $D_{\mathrm{initial}}(t)$ shows the number of immature detectors.

Definition 3. The formula of attenuating antibody concentration is defined as

$$\begin{aligned}
&C_{\mathrm{ab}}(t + \Delta t)\\
&= \begin{cases} C_{\mathrm{ab}}(t)\prod_{1}^{n}\left(1 - \frac{1}{T} - \Delta t\right), & \Delta t < T - 1 \wedge \Delta t \in N^*,\\ 0, & \Delta t \geq T - 1 \wedge \Delta t \in N^*, \end{cases}
\end{aligned} \tag{10}$$

where T is antibody concentration decay cycle and Δt is the duration of the antibody concentration decrease to zero.

Definition 4. Without considering the threat of attack types and the importance of equipment in the network, the host s under q attack of antibody concentration formula is defined as

$$C_{\mathrm{ab}}^{sq}(t) = C_{\mathrm{ab}}^{sq}(0) + k_{sq}C_{\mathrm{ab}}^{sq}(t-1), \tag{11}$$

where $k_{sq} = (D_{\mathrm{Ma}}^{\mathrm{active}(q)}(t) + D_{\mathrm{Mr}}^{\mathrm{clone}(q)}(t))/(D_{\mathrm{initial}}^{q}(t) + D_{\mathrm{Ma}}^{q}(t) + D_{\mathrm{Mr}}^{q}(t))$, k_{sq} is under q attack of antibody concentration increase factor, $D_{\mathrm{Ma}}^{\mathrm{active}(q)}(t)$ shows the number of activated memory detectors under q attack, $D_{\mathrm{Mr}}^{\mathrm{clone}(q)}$ shows the number of clone memory detectors under q attack, $D_{\mathrm{initial}}^{q}(t)$ is the number of immature detectors under q attack, $D_{\mathrm{Ma}}^{q}(t)$ denoted the number of mature detectors under q attack, $D_{\mathrm{Mr}}^{q}(t)$ is the number of memory detectors under q attack, and before q attack the initial of antibody concentration is $C_{\mathrm{ab}}^{sq}(0)$.

Definition 5. The threat of τ attack is σ_τ and $\sigma_\tau = 1 - 2e^{-\sqrt{10\mathrm{num}_{\mathrm{attack}}^{\tau} + 10^{\mathrm{str}^{\tau}}}}$; the host s under all of the attacks of antibody concentration formula is defined as

$$C_{\mathrm{ab}}^{s}(t) = \frac{1}{q_n}\sum_{\tau=q}^{q_n}\delta_\tau C_{\mathrm{ab}}^{s\tau}(t), \tag{12}$$

where $\mathrm{num}_{\mathrm{attack}}^{\tau}$ is that τ attack of the number of attacks; the intensity of the attacks about τ attack is str^{τ}.

Theorem 6. *If the threat is constant, the antibody concentration of the host s is strengthened with the increase of categories of attacks, that is,*

$$\begin{aligned}
\delta_q C_{ab}^{sq}(t) &< \frac{\left(\delta_q C_{ab}^{sq}(t) + \delta_q C_{ab}^{sq_1}(t)\right)}{2} < \cdots\\
&< \frac{\left(\sum_{\tau=q}^{q_n}\delta_q C_{ab}^{s\tau}(t)\right)}{q_n},
\end{aligned} \tag{13}$$

where q_n shows types of attacks and $q_n \in N^*$.

Proof. When t is zero,

$$\delta_q C_{\mathrm{ab}}^{sq}(0) = \frac{\left(\delta_q C_{\mathrm{ab}}^{sq}(0) + \delta_q C_{\mathrm{ab}}^{sq_1}(0)\right)}{2} = \cdots = \frac{\left(\sum_{\tau=q}^{q_n} \delta_q C_{\mathrm{ab}}^{s\tau}(0)\right)}{q_n}. \tag{14}$$

When t is greater than zero and τ is equal to q_1,

$$\frac{\left(\delta_q C_{\mathrm{ab}}^{sq}(t) + \delta_q C_{\mathrm{ab}}^{sq_1}(t)\right)}{2} = \frac{\left(\sum_{\tau=q}^{q_1} \delta_q C_{\mathrm{ab}}^{s\tau}(t)\right)}{2} = \frac{\left(\sum_{\tau=q}^{q_1} \delta_q \left(\left(1-k_{s\tau}^t\right)/\left(1-k_{s\tau}\right)\right) C_{\mathrm{ab}}^{s\tau}(0)\right)}{2} = \frac{\left(C_{\mathrm{ab}}^{sq}(0)\, \delta_q \sum_{\tau=q}^{q_1} \left(\left(1-k_{s\tau}^t\right)/\left(1-k_{s\tau}\right)\right)\right)}{2}, \tag{15}$$

and so on; when t is greater than zero and τ is equal to q_n,

$$\frac{\left(\sum_{\tau=q}^{q_n} \delta_q C_{\mathrm{ab}}^{s\tau}(t)\right)}{q_n} = \frac{\left(C_{\mathrm{ab}}^{sq}(0)\, \delta_q \sum_{\tau=q}^{q_n} \left(\left(1-k_{s\tau}^t\right)/\left(1-k_{s\tau}\right)\right)\right)}{q_n}. \tag{16}$$

Therefore, we only need to prove $(1-k_{sq}^t)/(1-k_{sq}) < ((1-k_{sq}^t)/(1-k_{sq}) + (1-k_{sq_1}^t)/(1-k_{sq_1}))/2 < \cdots < \sum_{\tau=q}^{q_n}((1-k_{s\tau}^t)/(1-k_{s\tau}))/q_n$.

Because the immune system according to the rules of the LRU is to weed out all kinds of detectors, but the overall size stays the same, $k_{sq} = (D_{\mathrm{Ma}}^{\mathrm{active}(q)}(t) + D_{\mathrm{Mr}}^{\mathrm{clone}(q)})/(D_{\mathrm{initial}}^{q}(t) + D_{\mathrm{Ma}}^{q}(t) + D_{\mathrm{Mr}}^{q}(t)) = (D_{\mathrm{Ma}}^{\mathrm{active}(q)}(t) + D_{\mathrm{Mr}}^{\mathrm{clone}(q)})/(D_{\mathrm{initial}}(t) + D_{\mathrm{Ma}}(t) + D_{\mathrm{Mr}}(t))$, with the increase of categories of attacks; from the above formula we can see molecular increases and the denominator remains the same; then $k_{sq} < k_{sq_1} < \cdots < k_{sq_n}$.

$$\frac{\left(\left(\left(1-k_{sq}^t\right)/\left(1-k_{sq}\right) + \left(1-k_{sq_1}^t\right)/\left(1-k_{sq_1}\right)\right)/2\right)}{\left(1-k_{sq}^t\right)/\left(1-k_{sq}\right)} \approx \left(\frac{\left(1/\left(1-k_{sq}\right) + 1/\left(1-k_{sq_1}\right)\right)}{2}\right) * \left(1-k_{sq}\right) = \frac{\left(1 + \left(1-k_{sq}\right)/\left(1-k_{sq_1}\right)\right)}{2}. \tag{17}$$

Because $k_{sq} < k_{sq_1}$, $(1 + (1-k_{sq})/(1-k_{sq_1}))/2 > 1$, that is, $(1-k_{sq}^t)/(1-k_{sq}) < ((1-k_{sq}^t)/(1-k_{sq}) + (1-k_{sq_1}^t)/(1-k_{sq_1}))/2$.

Similarly, $(\sum_{\tau=q}^{q_n}((1-k_{s\tau}^t)/(1-k_{s\tau}))/q_n)/(\sum_{\tau=q}^{q_{n-1}}((1-k_{s\tau}^t)/(1-k_{s\tau}))/q_{n-1}) > 1$.

Thus, with more kinds of attacks increasing, the antibody concentration is also rising. □

Theorem 7. *The antibody concentration of the host s was strengthened with the increase of the number of attacks and the intensity of the attacks; that is, if $\mathrm{num}_{attack}^{\tau}$ was increased or str^{τ} increased, then $\sum_{\tau=q}^{q_n} \delta_\tau C_{ab}^{s\tau}(t)$ was also increased.*

Proof. Because when $\mathrm{num}_{\mathrm{attack}}^{\tau}$ was increased or str^{τ} increased, according to $\sigma_\tau = 1 - 2e^{-\sqrt{10\mathrm{num}_{\mathrm{attack}}^{\tau} + 10^{\mathrm{str}^{\tau}}}}$, σ_τ was increased and because when $\mathrm{num}_{\mathrm{attack}}^{\tau}$ was increased or str^{τ} increased, the activated mature detectors and memory detectors were also rising, then $C_{\mathrm{ab}}^{s\tau}(t)$ was increased and $\delta_\tau C_{\mathrm{ab}}^{s\tau}(t)$ was also increased, so $\sum_{\tau=q}^{q_n} \delta_\tau C_{\mathrm{ab}}^{s\tau}(t)$ was also increased. □

Definition 8. When μ_s is the importance of the host s in the network, t moment, all hosts s_n under q attack of antibody concentration formula are defined as

$$C_{\mathrm{ab}}^{q}(t) = \frac{1}{s_n} \sum_{s=1}^{s_n} \mu_s C_{\mathrm{ab}}^{sq}(t), \tag{18}$$

where $\mu_s = 1 - 2e^{-\sqrt{\alpha_s + \beta_s}}$, α_s manifests the price of the host s, and β_s refers to the memory of the host s.

Definition 9. All hosts s_n (i.e., entire network) under all of the attacks of antibody concentration formula are defined as

$$C_{\mathrm{ab}}(t) = \frac{1}{s_n} \sum_{s=1}^{s_n} \mu_s \sum_{\tau=q}^{q_n} \delta_\tau C_{\mathrm{ab}}^{s\tau}(t). \tag{19}$$

3.7. Body Temperature Assessment Model. According to the mechanism of the biological immune system, the body temperature rises in the face of external viruses and other harmful substances (fever phenomenon), indicating that the invasion of harmful substances alters the physiological regulation of equilibrium. Network is subject to risks caused by external attacks with which they have the same purpose. Therefore, in order to more conveniently and intuitively distinguish network degree of risk, using the way of body temperature to assess network risk, the body temperature will be divided into different stages and defined with different colors; depending on the different colors the danger zone can quickly be determined.

The host s under q attack of body temperature calculation formula is as follows:

$$T_{sq}(t) = 3\left(1 - \ln\left(1 + e^{-\sqrt{\delta_q C_{\mathrm{ab}}^{sq}(t)}}\right)\right) - 1. \tag{20}$$

Through the fusion of risk for the host of all attacks, the host s under all of the attacks of body temperature calculation formula is as follows:

$$T_s(t) = 3\left(1 - \ln\left(1 + e^{-\sqrt{C_{\mathrm{ab}}^{s}(t)}}\right)\right) - 1 = 3\left(1 - \ln\left(1 + e^{-\sqrt{(1/q_n)\sum_{\tau=q}^{q_n} \delta_\tau C_{\mathrm{ab}}^{s\tau}(t)}}\right)\right) - 1. \tag{21}$$

Through the fusion of risk for all hosts with a kind of attack, all hosts under q attack of body temperature calculation formula are as follows:

$$T_q(t) = 3\left(1 - \ln\left(1 + e^{-\sqrt{C_{\mathrm{ab}}^{q}(t)}}\right)\right) - 1 = 3\left(1 - \ln\left(1 + e^{-\sqrt{(1/s_n)\sum_{s=1}^{s_n} \mu_s C_{\mathrm{ab}}^{sq}(t)}}\right)\right) - 1. \tag{22}$$

Through the fusion of risk for all hosts and attacks, all hosts under all of the attacks of body temperature calculation formula are as follows:

$$T(t) = 3\left(1 - \ln\left(1 + e^{-\sqrt{C_{ab}(t)}}\right)\right) - 1 = 3\left(1 - \ln\left(1 + e^{-\sqrt{(1/q_n s_n)\sum_{s=1}^{s_n}\mu_s\sum_{\tau=q}^{q_n}\delta_\tau C_{ab}^{s\tau}(t)}}\right)\right) - 1. \quad (23)$$

Because the body temperature range of 0 to 1 and the defined body temperature range are different, the body temperature T needs to adopt deviation standardization of the inverse function, standardize to T^* [7], that is, $T^* = T(\max - \min) + \min = 5T + 1$. The standardized body temperature range is 1 to 6. The function of network body temperature is defined as $T' = 34 + T^*$.

4. Simulation Experiments and Analysis

This model uses r-contiguous bits nonconstant matching rate algorithm in the stage of invasion, select artificial immune algorithm (AIA), where $r \in [2, 10]$. It is proved that the matching algorithm can improve the detection rate of the nonself and reduce the false detection rate of self, which is shown in Figures 1 and 2.

In order to verify the feasibility and effectiveness of the method described in this paper, this paper uses the typical types of attacks (such as SYN Flood, Land, and Smurf attacks) of simulation experiment to test it. The structure of the experimental environment is shown in Figure 3. The experimental network is composed of twenty hosts, and the hosts s_1, s_2, and so on are monitored. In this experiment, the selected parameters are as follows: initial antibody concentration is 0.015; the hosts s_1 and s_2 prices are, respectively, 0.3 and 0.6 thousand yuan; hosts memory is, respectively, 2 G and 4 G; that is, the importance of hosts is, respectively, 0.56 and 0.77; the intensity of the attacks of SYN Flood, Land, and Smurf attack is, respectively, 0.5, 0.8, and 0.1; the number of attacks is, respectively, 0.2, 0.1, and 0.15; that is, the threat of attack types is, respectively, 0.79, 0.87, and 0.62.

The host s_1 of antibody concentration curve is illustrated in Figure 4 as the number of different attack types; as you can see from Figure 3, once the attack occurred, the antibody concentration will be increased. In three different states, in the moments of 24 to 76, the host s_1 relatively suffered no significant strengthening attack, so the trend of overall change in antibody concentration is relatively stable. In the moments of 18–24, the host suffered SYN Flood attack; with the increase of attacks, antibody concentration significantly increased. As can be seen from the whole, the antibody concentration of the host s was strengthened with the increase of categories of attacks and threat.

The antibody concentration and attack power curve is illustrated in Figure 5. As you can see from Figure 5, in the moments of 32–40, with the significant increase of attack times, antibody concentration is also rapidly increasing; antibody concentration is positively correlated with the attack times. In the moment of 25, antibody concentration reaches

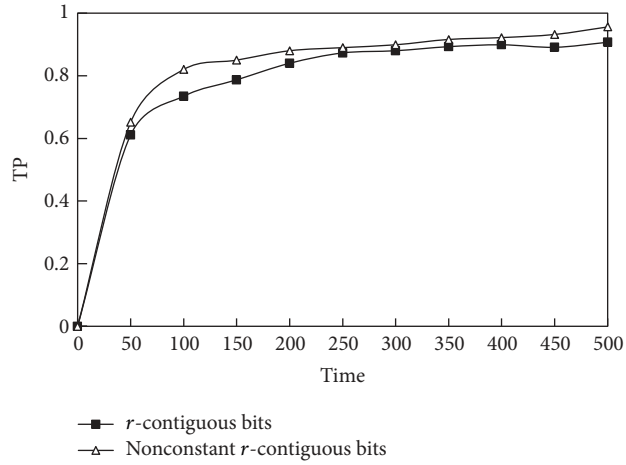

Figure 1: The nonself detection rate of two matching algorithms.

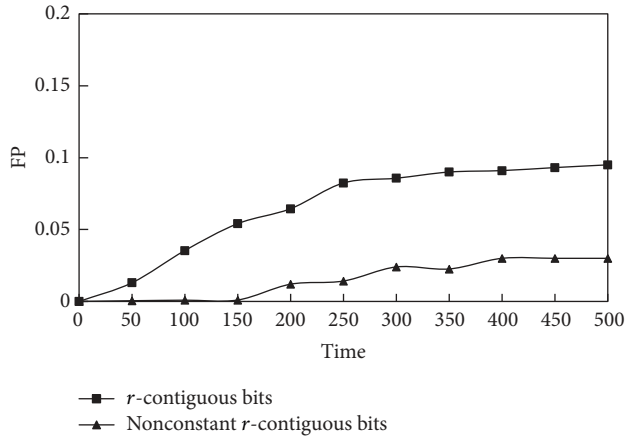

Figure 2: The self-false detection rate of two matching algorithms.

the first peak and it has higher vigilance about attack; attacks occur within a short time; in the moment of 40, the antibody concentration reaches the highest value; when attacks are weakened, the antibody concentration decrease delays; in the moments of 40–50, antibody concentration basically remains unchanged; after the moment of 50, it began to fall. In the moments of 50 and 70, the system takes appropriate measures and the falling speed is relatively fast. At other times, it does not take measures, and the magnitude of the threat of attack is relatively small and the antibody concentration change is relatively stable. As can be seen from the whole, due to the presence of IDS, at the beginning, the increase of antibody concentration is slow; IDS orders the firewall to prevent a part of the attacks. The overall increase of antibody concentration is smaller than that of no IDS. The effect of initial different antibody concentration for risk values is shown in Figure 6. As can be seen from the bar chart, when c is equal to 0.015, the value of risk is more satisfactory.

The host s_1 of attacks and antibody concentration increase factor curve is illustrated in Figure 7. The host s_1 of antibody concentration and temperature evaluation is illustrated in

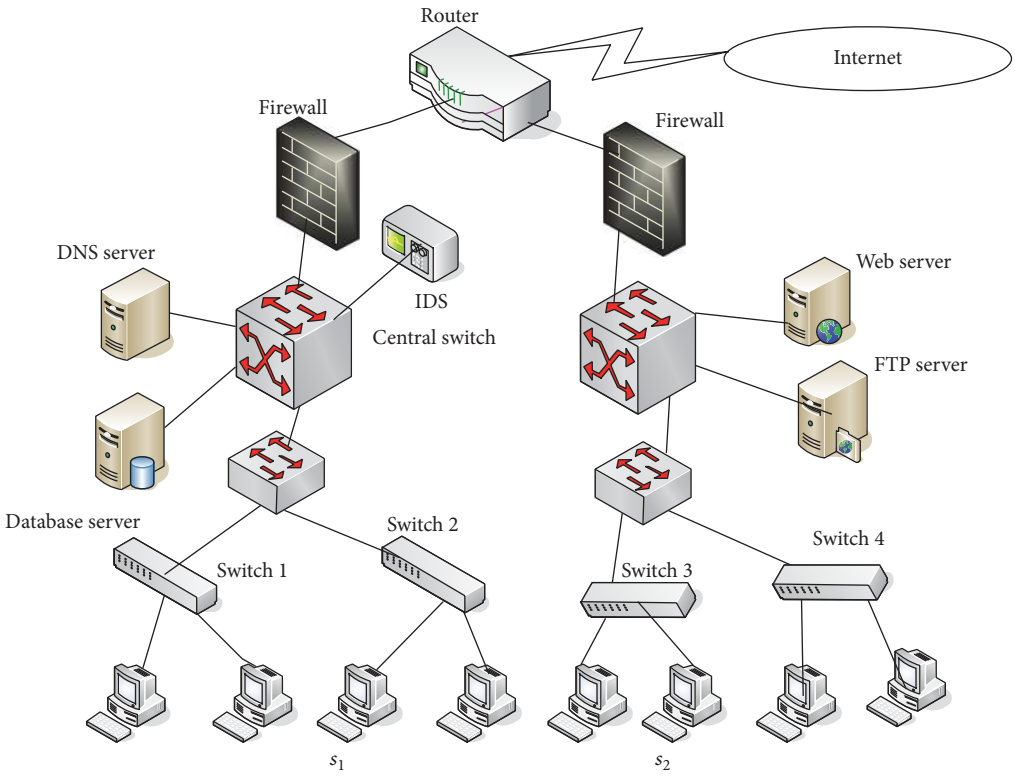

Figure 3: The experimental environment structure diagram.

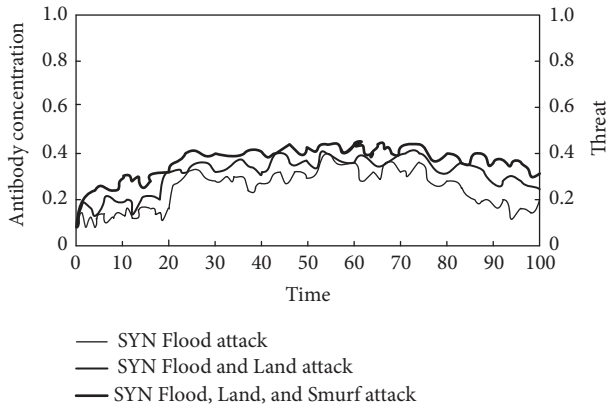

Figure 4: Host s_1 antibody concentration on the condition of the number of different attack types.

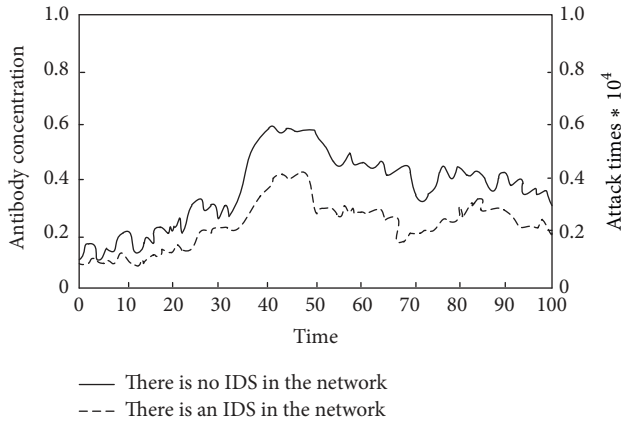

Figure 5: Under conditions with IDS and without IDS, the host s_2 of antibody concentration and attack times diagram.

Figure 8. As you can see from Figure 7, the antibody concentration increase factor k and the number of attacks change trend has good consistency: with the increase of the number of attacks, the corresponding k value will rapidly rise and vice versa. As you can see from Figure 8, the antibody concentration and temperature change trend has good consistency. Compared with Figure 7, it shows that if the number of attacks increases, the antibody concentration and temperature will increase, but if the number of attacks decreased, antibody concentration and temperature will slowly decline. Due to recurrence of similar attacks in a short time in the real network environment, the network has higher vigilance. Therefore, in Figure 8, in the moments of 35 to 45 and in the moments of 48 to 57, the change of antibody concentration and temperature is smooth.

The temperature value is divided into five parts, namely, the definition of $[0, 0.2]$ is very safe, $(0.2, 0.4)$ is security, $[0.4, 0.6)$ is low risk, $[0.6, 0.8)$ is moderate risk, and $[0.8, 1]$ is high risk. By the mapping function body temperature is mapped to $[35, 36]$, $(36, 37)$, $[37, 38)$, $[38, 39)$, and $[39, 40]$; those areas are, respectively, represented by green, blue, yellow, orange, and red.

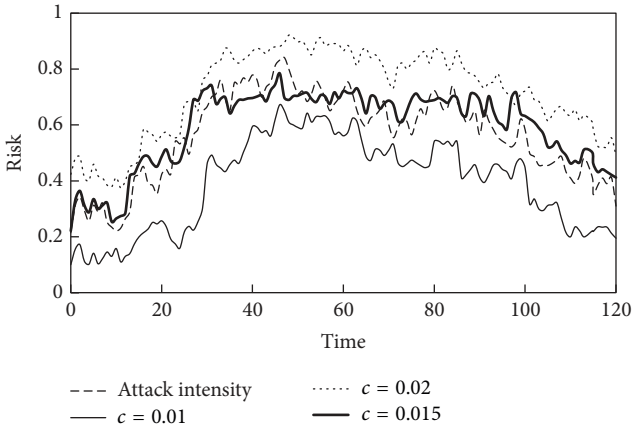

Figure 6: The effect of different initial antibody concentrations for risk values.

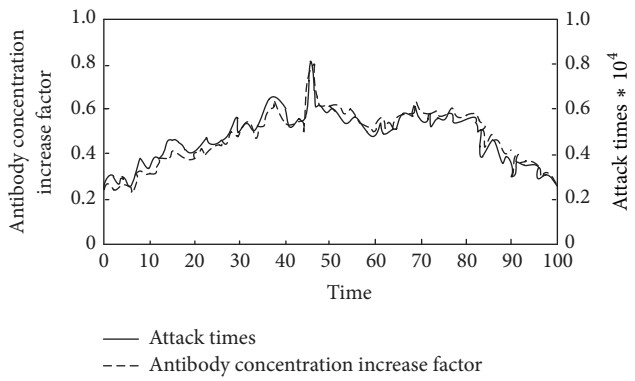

Figure 7: Host s_1 of attacks and antibody concentration increase factor.

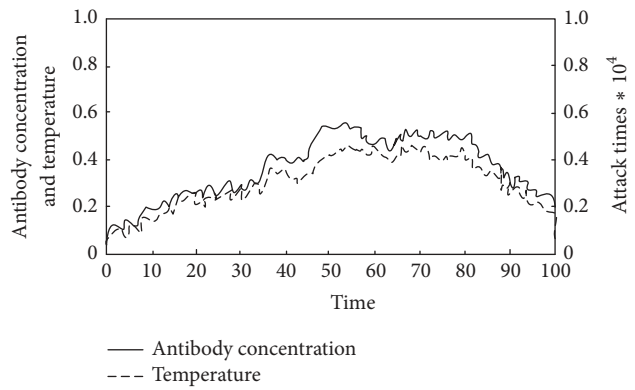

Figure 8: Host s_1 of antibody concentration and temperature evaluation factor.

The body temperature evaluation of the entire network is illustrated in Figure 9. In the moments of 0 to 100, the corresponding color of 0–60-moment body temperature characterization is shown in Figure 10. As you can see from Figure 9, in the moment of 40, the body temperature significantly increased, and the body temperature value was at a low risk stage. In the moments of 50 to 60, the body

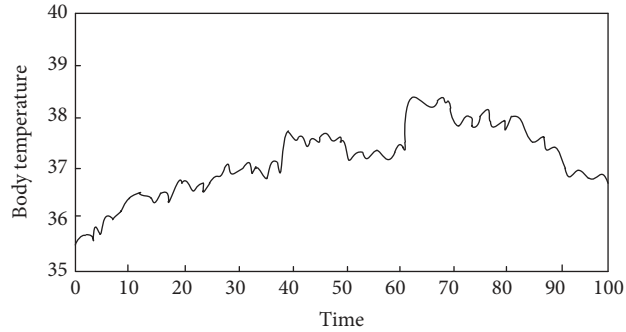

Figure 9: The temperature evaluation of the entire network.

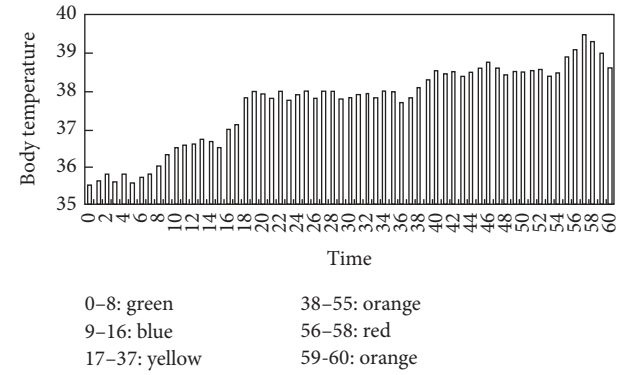

Figure 10: The corresponding color of 0–60-moment temperature characterization.

temperature was slowly falling, and it was still at a low risk stage; because the system does not take measures, the decreased body temperature explains the reason why the system did not suffer new attacks in a certain period of time; a part of the mature detectors was death. In the moment of 70, the temperature increased, and the temperature value was at a moderate risk stage. But in the moment of 80, the temperature value was decreased to a low risk stage, during this period, indicating that the system takes the corresponding measures.

The scope of attack power will be mapped to the range of temperature which is defined in this paper and compared with network temperature. As you can see from Figures 11 and 12, the model of literature [14] and the proposed model in this paper all can represent the real time network risk, experimental result, and the change of attack power that keeps basic consistency. However, the proposed model is more close to the actual attack strength, and the network risk evaluation is more effective and accurate.

5. Conclusion

This paper references the mechanism of body temperature change caused by biological immune system imbalance, analyzes antibody concentrations change caused by the change process of various types of detectors in computer immune system, and proposes a quantitative risk evaluation model for network security based on body temperature (QREM-BT). The model established the evaluation equation

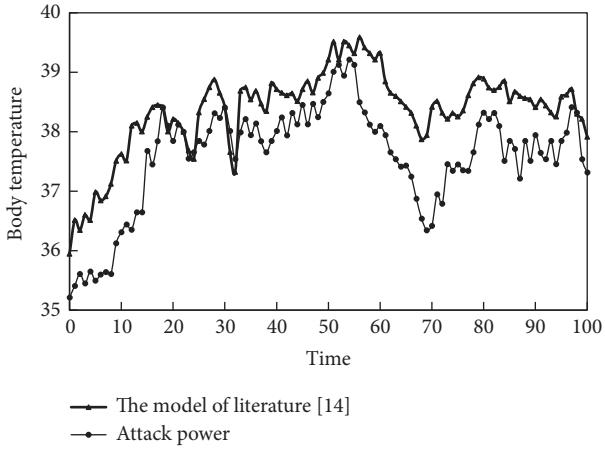

Figure 11: The change curve of the measured body temperature and the actual attack intensity with the model of literature [14].

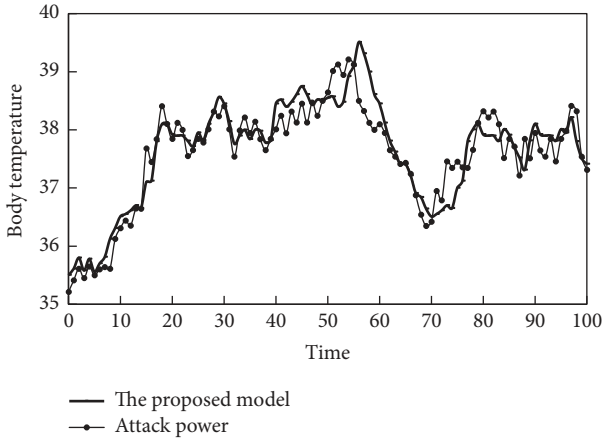

Figure 12: The change curve of the measured body temperature and the actual attack intensity with the proposed model.

of antibody concentration and body temperature in this paper, and body temperature values are mapped to be more easily convenient and intuitive judgment dangerous levels of body temperature range, making it more in line with the mechanism of biological immune system and more practical significance. Simulation results show that the model can be on the basis of the body temperature value and the color of the corresponding is relatively more effective, in real time, and intuitive to assess network security risk.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

The authors are grateful to the National Natural Science Foundation (no. 61272038), Henan Science and Technology Agency-Funded Science and Technology Research Projects (no. 0624220084), Henan Province Department of Education Program (no. 2010A520044), and Henan Science and Technology Department of Basic and Cutting-Edge Technology Projects (no. 122300410255).

References

[1] B. Tim, "Intrusion detection systems and multi-sensor data fusion creating cyberspace situational awareness," *Proceedings of the ACM*, vol. 43, no. 4, pp. 99–105, 2000.

[2] M. Li and M. Bardi, "A risk assessment method of cloud computing based on multi-level fuzzy comprehensive evaluation," in *Proceedings of the International Conference on Cyberspace Technology (CCT '14)*, pp. 1–4, Beijing, China, November 2014.

[3] A. Sotoodeh Gohar, M. Khanzadi, M. Parchami Jalal, and A. A. Shirzadi Javid, "Construction projects risk assessment based on fuzzy AHP," in *Proceedings of the IEEE Student Conference on Research and Development (SCOReD '09)*, pp. 570–573, November 2009.

[4] M. Alhomidi and M. Reed, "Risk assessment and analysis through population-based attack graph modelling," in *Proceedings of the World Congress on Internet Security (WorldCIS '13)*, pp. 19–24, IEEE, London, UK, December 2013.

[5] M. Keramati and A. Akbari, "An attack graph based metric for security evaluation of computer networks," in *Proceedings of the 6th International Symposium on Telecommunications (IST '12)*, pp. 1094–1098, IEEE, Tehran, Iran, November 2012.

[6] J. J. P. Sipayung and J. Sembiring, "Risk assessment model of application development using Bayesian Network and Boehm's Software Risk Principles," in *Proceedings of the International Conference on Information Technology Systems and Innovation (ICITSI '15)*, pp. 1–5, IEEE, Bandung, Indonesia, November 2015.

[7] M. Naderpour, J. Lu, and G. Zhang, "A fuzzy dynamic bayesian network-based situation assessment approach," in *Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ '13)*, pp. 1–8, IEEE, Hyderabad, India, July 2013.

[8] F.-W. Li, S. Sun, J. Zhu, and S.-C. Yang, "Situation assessment method based on hidden Markov model," *Computer Engineering and Design*, vol. 36, no. 7, pp. 1706–1711, 2015.

[9] R. R. Xi, X. C. Yun, Y. Z. Zhang, and Z. Y. Hao, "An improved quantitative evaluation method for network security," *Chinese Journal of Computers*, vol. 38, no. 4, pp. 749–758, 2015.

[10] Y.-F. Wang, T. Li, X.-Q. Hu, and C. Song, "A real-time method of risk evaluation based on artificial immune system for network security," *Chinese Journal of Electronics*, vol. 33, no. 5, pp. 945–949, 2005.

[11] N. Liu, S.-J. Liu, Y. Liu, and H. Zhao, "Method of network security situation awareness based on artificial immunity system," *Journal of Computer Science*, vol. 37, no. 1, pp. 126–129, 2010.

[12] Z. Gao and X. Hu, "Design and implementation of real-time network risk control system based on antibody concentration," *Journal of Computer Applications*, vol. 33, no. 10, pp. 2842–2845, 2013.

[13] I. Kotenko and A. Chechulin, "A cyber attack modeling and impact assessment framework," in *Proceedings of the 5th International Conference on Cyber Conflict*, pp. 1–24, Tallinn, Estonia, June 2013.

[14] M. Khosravi-Farmad, R. Rezaee, and A. G. Bafghi, "Considering temporal and environmental characteristics of vulnerabilities in network security risk assessment," in *Proceedings of the 11th International ISC Conference on Information Security*

and Cryptology (ISCISC '14), pp. 186–191, IEEE, Tehran, Iran, September 2014.

[15] M. G. Ionita and V. V. Patriciu, "Biologically inspired risk assessment in cyber security using neural networks," in *Proceedings of the 10th International Conference on Communications (COMM '14)*, pp. 1–4, Bucharest, Romania, May 2014.

[16] M. Rezvani, V. Sekulic, A. Ignjatovic, E. Bertino, and S. Jha, "Interdependent security risk analysis of hosts and flows," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2325–2339, 2015.

[17] A. Hemanidhi, S. Chimmanee, and C. Kimpan, "Cyber risk evaluation framework based on risk environment of military operation," in *Proceedings of the 1st Asian Conference on Defence Technology (ACDT '15)*, pp. 42–47, April 2015.

[18] D. Wu, Y.-F. Lian, K. Chen, and Y. L. Liu, "A security threats identification and analysis method based on attack graph," *Chinese Journal of Computers*, vol. 35, no. 9, pp. 1938–1950, 2012.

[19] Y.-L. Chen, G.-M. Tang, and Y.-F. Sun, "Assessment of network security situation based on immune danger theory," *Journal of Computer Science*, vol. 42, no. 6, pp. 167–170, 2015.

[20] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Transactions on Industrial Electronics*, 2016.

[21] S. C. Mukhopadhyay, "Wearable sensors for human activity monitoring: a review," *IEEE Sensors Journal*, vol. 15, no. 3, pp. 1321–1330, 2015.

[22] P. Gope and T. Hwang, "BSN-care: a secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, no. 5, pp. 1368–1376, 2016.

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

[24] X. Feng, M.-Y. Ma, T.-L. Zhao, and H.-Q. Yu, "Intrusion detection system based on hybrid immune algorithm," *Journal of Computer Science*, vol. 41, no. 12, pp. 43–47, 2014.