Construction of Quantitative Model for Network Security Situation Assessment Based on Intelligent Immunity

Guowei Suo1,a, Jiawei Du1, Ying Zhou1 and Ronghua Guo1
1 LEETC, Zhoushan Road 17#, Luoyang City, Henan Province, China
E-mail:441953136@qq.com

Abstract. The purpose of this paper is to deeply study the quantitative model of network security situation assessment and establish a quantitative model of network security situation assessment based on intelligent immune. First, we introduce the related theory of network security situation awareness, grasp the algorithm framework of intelligent immune and the relevant knowledge of grey prediction model. On this basis, we design the quantitative process of network security situation assessment and the evolutionary process of intelligent immune detector, and finally realize the quantitative evaluation hierarchical structure and frame model of network security situation based on intelligent immunity.

1. Introduction
Since the security mechanism of the network is not perfect enough, the protection function of the existing network security products is limited, the original data of the network security is often from a single data source, which leads to the difficult judgment and control of the overall security of the network, so it is necessary to use new technology to evaluate the overall situation of the network more effectively.

The network security situation assessment technology[1] can perceive and obtain the related elements from time and space, quantize and analyze the data information of the original network event data, extract the information of time correlation and key features, give the current status of the network, integrate a variety of security factors, and use a specific mathematical prediction model[2]. Prior knowledge can predict the trend of development, enhance network security and prevent risks. The goal is to inform the decision-maker of the current state of the network and the possible risks in the future.

The research of situation assessment model should focus on operability, flexibility and accuracy. At present, the research work on network security situation assessment and quantification at home is just starting. There is no established standard in theory and technology, so research on this field has important theoretical and practical significance.

2. The Related Theory of NETWORK Security Situation Assessment

2.1. Network Security Situation Assessment
The network security situation assessment is having the ability to aware when the attack occurs. After the attack, the threat information is collected, the information is merged, the redundant information is removed, and the extent of the attack and the extent of the damage are evaluated[3]. The specific contents include the following parts.

2.1.1. The process of network security situation assessment
(1) Alarm data acquisition
Network security devices collect network traffic and data, merge them, remove redundant information and preprocess, and prepare for the next step of association analysis.

(2) Security events association
On the basis of data acquisition, the preprocessed original data are related to security events, and the security events data server is used to find and match the related security event feature information.

(3) Assessment of the degree of network security
Using appropriate assessment techniques, we integrate the prior knowledge and data of various security events to assess the overall extent of the hazards.

(4) Forecast of the trend of network development
The current security status of the network is analyzed, and the development and changes of the subsequent network state are summarized by using the results of the evaluation and the history network security incident information.

2.1.2. Network security situation assessment methods
There are many existing network security situation assessment methods.

(1) Classification according to the perspective of evaluation
According to the emphasis of evaluation, it is divided into risk assessment and threat assessment, and it is divided into static and dynamic evaluation according to the real time evaluation. According to the theoretical evaluation basis, it is divided into three categories based on mathematical model, knowledge reasoning and model.

(2) Theory based evaluation methods
The evaluation methods based on data model include analytic hierarchy process, fuzzy comprehensive evaluation method and multi-attribute utility function distance deviation method. Knowledge reasoning includes fuzzy reasoning, Bayesian network, Markov process, D-S evidence theory and so on. Pattern based assessment methods include clustering analysis, grey relational analysis, neural network and so on.

2.2. The Basic Theory of Intelligent Immunity

2.2.1. Overview
In biology, immunity refers to the immediate measures to ensure that the organisms are invading themselves from foreign invasion, and to clear the invaders through a variety of special self-protection mechanisms, immune systems and defense. Its core elements can be summarized as self identification and exclusion. Specifically, immune revelation is a special physiological reflection of organisms.

Intelligent immunity is an adaptive network system, which introduces the specific ability of the immunity, and establishes a model to solve the specific problems of network security situation assessment.

2.2.2. The algorithm derivation framework for intelligent immunity
At present, research on Intelligent immunity is no longer associated with immunology. Researchers have not yet proposed effective immunization mechanisms. Stepney S[4] set up an algorithm framework based on biologic guidance. The overall framework is shown in Figure 1.

![Figure 1. The framework structure of the algorithm for intelligent immunity](image-url)
The framework uses various disciplines to integrate the practical intelligent immune processing algorithms, identify the processing methods in the acquisition of immunology, through the in-depth analysis of biological analysis, and find the regularity results, after the experiment is verified, it can inspire new algorithm design thinking. The framework is an iterative cycle, whether it is to observe, test, analyze and study the biological system, or to simplify, abstract and represent the results, until the final model process is established. The framework algorithm can enlighten a better application class design algorithm.

2.2.3. Grey prediction model
Grey prediction belongs to the quantitative forecast analysis in network security situation prediction methods[5]. There are grey GM (1, 1) and Verhulst models.

The grey GM (1, 1) model is a first order differential equation. The equation contains single variable, and the single variable can be used to predict the future situation value. Here is a brief introduction to the main steps of GM (1, 1).

The first step is to set the initial data sequence of the network security situation value:

\[ x^{(0)}(t) = \{x^{(0)}(1), x^{(0)}(2), x^{(0)}(3), \ldots, x^{(0)}(n)\} \]  

If \( x^{(i)}(t) = \sum_{i=1}^{n} x^{(i)}(i), t = 1, 2, \ldots, n \), the initial sequence is processed by AGO, and the following new data sequence can be obtained:

\[ x^{(1)}(t) = \{x^{(1)}(1), x^{(1)}(2), x^{(1)}(3), \ldots, x^{(1)}(n)\} \]  

The GM (1, 1) model can be described by the equation shown in (3).

\[ \mu = \alpha x^{(1)}(i) + \frac{dx^{(1)}}{dt} \]  

In this equation, \( \alpha \) and \( \mu \) are undetermined parameters, and their values are calculated through the following formula:

\[ (\alpha, \mu)^T \approx (B^T B)^{-1} B^T y \]  

The B and y calculation methods in equation (4) are:

\[ B = \begin{bmatrix} -1/2[x^{(2)}(2) + x^{(0)}(1)] & 1 \\ \vdots & \vdots \\ -1/2[x^{(n)}(n) + x^{(0)}(n-1)] & 1 \end{bmatrix} \]  

\[ y = \begin{bmatrix} x^{(0)}(2), x^{(0)}(3), \ldots, x^{(0)}(n) \end{bmatrix} \]  

The cumulative values calculated by the prediction are as follows:

\[ \hat{X}^{(i)}(t+1) = \left[ x^{(0)}(1) - \frac{\mu}{\alpha} \right] e^{\alpha t} + \frac{\mu}{\alpha} \]  

Finally, the accumulated sequence values are restored and the prediction results are as follows:

\[ \hat{X}^{(0)}(t+1) = \hat{X}^{(i)}(t+1) - \hat{X}^{(i)}(t) \]  

The grey prediction model algorithm is simple and convenient, and the result can also reflect the development of the situation smoothly. It is suitable for a single change situation. It can not reflect the periodicity and randomness, and the prediction results often have error.

The Verhulst model introduces dynamic development constraints and uses nonlinear Malthus model representation[6].
\[ rp(t) - p^2(t)u = \frac{dp(t)}{dt} \]  

(9)

Among them, \( r \) and \( u \) are specific parameters of the model.

\[ p(t) = \frac{r}{u \text{e}^{-r(t-t_0)} - [1 + \frac{r}{u}]} \]  

(10)

In equation (9), \( t_0 \) is the starting time, \( p(t_0) \) is the initial value in the sequence.

Set the original data sequence as:

\[ x^{(0)} = \{x^{(0)}(1), x^{(0)}(2), x^{(0)}(3), \ldots, x^{(0)}(n)\} \]  

(11)

Completing a weighted generation operation (Accumulated Generating Operation, AGO), Get:

\[ x^{(i)} = \{x^{(i)}(1), x^{(i)}(2), x^{(i)}(3), \ldots, x^{(i)}(n)\} \]  

(12)

Among them:

\[ x^{(i)}(k) = \sum_{i=1}^{k} x^{(i)}(i) \geq 0, k = 1, 2, 3, \ldots, n \]  

(13)

\( x^{(i)} \) is a weighted generation operation of \( x^{(0)} \), and \( x^{(0)} \) can also be represented by \( x^{(i)} \):

\[ x^{(0)}(k) = \begin{cases} x^{(i)}(k) - x^{(i)}(k-1) & k \neq 1 \\ x^{(i)}(k) & k = 1 \end{cases} \]  

(14)

In equation (14), \( x^{(0)}(k) \in x^{(i)} \), the operation is also called the first order inverse accumulative generation operation.

The Verhulst model can weaken the randomness in the original sequence, and easily discover the rules in the sequence, so that the prediction can be more accurate, with higher accuracy and wider adaptability.

3. Construction of Quantitative Model for Network Security Situation Assessment Based on Intelligent Immunity

3.1. Quantitative Process of Network Security Situation Assessment

In order to evaluate the situation effectively, this section puts forward the network security situation quantitative model based on the intelligent immunity theory. According to the perception of the situation elements, the situation assessment model is used to quantify the security situation of the network[7]. In this way, network administrators can get effective network security information from massive network data packets by this process, so as to fully and effectively grasp the situation of the security situation in the network environment. The antigen extraction is to filter and extract the massive network data packets received from the network and hosts, and the sensor can monitor the external threat in time and effectively. The detailed quantification process of network security situation assessment is shown in Figure 2.

In Figure 2, Network security situation assessment quantitative process has been divided into three parts: situation understanding, situation assessment and situation prediction. Situation understanding consists of two sub-parts: network data acquisition, filtering & preprocessing. Situation assessment consists of three sub-parts: antigen extraction, antigen monitoring and quantitative assessment. Situation prediction is composed of grey prediction model to achieve accurate prediction of the situation.
3.2. Evolutionary Process of Detector Based on Intelligent Immunity

The detector based on Intelligent immunity is similar to the detector in the intrusion detection system[8]. The detector is introduced into the intelligent immunity. The antibody $ab$ is defined as a detector $d$, which is used to match the antigen $ag$. The three types of immune cells that correspond to the immature, mature and memory types have three kinds of immature, mature and memory detectors, which are named as non mature detection respectively. The Immature Detector (IMAD), the mature detector (Mature Detector, MAD) and the memory detector (Memory Detector, MED), the antigen is monitored by two detectors of MAD and MED, and the increase of network attacks will result in the increase of the number of detectors cloned. In MED, the concentration of antibody is quantitative, and it can reflect the intensity of the current network attack and the security situation of the network in real time.

The detector has two evolutionary mechanisms: self tolerance and cloned mutation. When the IMAD tolerance value reaches the tolerance limit $\alpha$, it evolves into MAD; when the number of antigens of the corresponding antibody of MAD reaches the activation threshold $\beta$, it clones itself and evolves to MED; the denier antigen is identified by the antibody of MAD, and the detector cloned by it is merged into the MAD or MAD set.

3.2.1. Self tolerance

In the process of self tolerance, the immune tolerance of the IMAD is successful if MAD does not match the self concentration of any element within the tolerance cycle $a$; otherwise, it will be cleared. The Hamming distance matching algorithm is used to calculate the affinity between detector and self set or antigen.

The following equation (15) describes how any IMAD $y$ is identified by the self element $x$. The result is that $0/1$ indicates whether IMAD matches $x$, which is the length of detector $d$, indicating the affinity between $x$ and $y$, and $r (0 \leq r \leq 1)$ indicates affinity threshold.

$$f_a(x, y) = \begin{cases} 0, & \text{Other} \\ 1, & \frac{f_a}{I_a} > \gamma \end{cases}$$

(15)

$f_i$ indicates whether $y$ can tolerate element $x$. The result of $x$ is 1, which is intolerance; otherwise it is intolerance.

$$f_i(x, y) = \begin{cases} 0, & \text{Other} \\ 1, & \exists x_i, y_i: f_a(x, y) = 1 \end{cases}$$

(16)

Finally, when $t \geq \alpha$, the cumulative IMAD was evolved to MAD. The concrete calculation method is as follows:
3.2.2. Cloned mutation

Clonal mutation mechanism is related to clonal selection and mutation. Clonal selection includes clone of mature detector and memory detector. Let $\zeta$ be a clone constant. $n$ represents the sum of the mature detector and memory detector (the total antigen obtained by the detector). $n_c$ represents the number of detectors similar to the antibodies of the $d$, $T_{Mn}$ and $M_{Tn}$ represent the clonal selection of the mature detector and the memory detector, and all the cloned detectors are merged into the MAD set. The following can be expressed as follows:

- \[
T_n = T_d \cup y, I_d = I_d - y \quad y \in I_d, yd \geq \alpha
\]
- \[
yt = yt + 1 \quad yt < \alpha \land f(x, y) = 1
\]

\[f_c(c) = \left[\frac{\zeta(1 - n_c / n)}{n}\right]
\]

\[T_c = M_{Mn} \cup T_d \cup T_{Mn} - \{d | d \in T_{Mn}\}
\]

3.3. A Network Security Situation Assessment Model Based on Intelligent Immunity

3.3.1. Hierarchical structure of network security situation assessment model

The network security situation assessment model based on intelligent immunity comprehensively analyzes multi index data related to security situation and extracts different historical data from various data sources as the input information of situation assessment[9], from network host node situation, network comprehensive situation, theory security threat, network node weight value importance and so on. In addition, the grey model is used to conduct quantitative evaluation, and finally visualize the quantitative assessment results of network security situation. The hierarchical structure diagram of the network security situation assessment model is shown in Figure 3.

![Figure 3](image)

**Figure 3.** The hierarchical structure of network security situation assessment model

The main purpose of network security situation assessment is to provide the overall security situation of network and to the knowledge of network security situation. The decision-makers can make the corresponding decision according to the results of the situation assessment. The network described in Figure 3 represents the universal network type. All kinds of security equipments, hosts and servers in the network are used as the input of the model. The input information mainly includes...
all kinds of node state information, vulnerability information, log information and so on, and then extracts indexes from these inputs for situation assessment.

3.3.2. Network security situation assessment model

The network security situation assessment model based on Intelligent immunity is a distributed model, which contains a series of host nodes, each host node has multiple detectors. The host node is a minimal independent immune function node. The main functions involved in the model include antigen recognition (matching), antibody diversity (diversity of detectors), regulation (detector regulation), self tolerance (autologous tolerance of detector), cell life cycle (detector's life cycle), and other advanced mechanisms. The framework of the model is shown in Figure 4.

![Diagram](image)

**Figure 4.** Framework of network security situation assessment model based on intelligent immunity

4. Conclusion

In this paper, the relevant theories and key technologies of network security situation assessment and intelligent immunity are studied. The relevant methods of grey prediction model are analyzed, and the quantitative model of network security situation assessment based on intelligent immunity is put forward, and the hierarchical structure and model framework of network security situation assessment model are constructed, which have better dynamic adaptability, stability and prediction accuracy. It provides new ideas and new methods for the research of network security situation. However, there are still some problems to be further improved, and the following work needs to be further studied.

1. The quantitative model of network security situation assessment based on intelligent immunity is only a quantitative evaluation method, which has many unique advantages, such as strong adaptability, good real-time and high accuracy in medium and small scale network environment. However, when evaluating large-scale networks, the computational complexity will be very large. Massive data processing will cause the real-time performance of the model to be affected. In future research, we will further resolve it.

2. In future studies, we will further study and analyze the multimodal situation changes and forecast complex situation changes.
5. References

[1] Wei Y, Lian Y F, Feng D G. “A network security situational awareness model based on information fusion”[J]. Journal of Computer Research and Development, 2009, 46(3): 353-362.

[2] Stepney S, S. R., Timmis J, Tyrrell A, Neal M, Hone A, “Conceptual frameworks for artificial immunity”[J]. Int J Unconventional Comput, 2006.1 (3):315-338.

[3] R. Rapuzzi, M. Repetto. “Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model”[J]. Future Generation Computer Systems, 2018.

[4] Stepney S, S. R, Timmis J, Tyrrell AM. “Towards a conceptual framework for artificial immunity”[C]. in Proceedings of the 3rd International Conference on Artificial Immunity (ICARIS2004). 2004: Springer, Berlin.

[5] Songqian HUANG, Weimin WANG, Cong ZENG, Shuang HAO, Xiaojuan CAO. “Application of Gray Metabolic GM (1, 1) Model in Prediction of Annual Total Yields of Chinese Aquatic Products”[J]. Asian Agricultural Research, 2013, 5(03): 21-25.

[6] Yong Shao. “Gray Prediction of Air Pollutants in Beijing Based on Improved Residual GM (1,1) Model”[A]. International society for information and engineering. Proceedings of 2016 4th International Conference on Machinery, Materials and Information Technology Applications (ICMMITA 2016) [C]. International society for information and engineering, 2016: 7.

[7] Yunhu Jin. “The Model of Network Security Situation Assessment Based on Random Forest”[A]. The Institute of Electrical and Electronics Engineers, IEEE Beijing Section. Proceedings of 2016 IEEE 7th International Conference on Software Engineering and Service Science(ICSESS 2016)[C]. The Institute of Electrical and Electronics Engineers, IEEE Beijing Section:, 2016:4.

[8] Lina Qin. “Network security situation prediction based on artificial immune algorithm”[J]. Journal of Changchun Institute of Technology (NATURAL SCIENCE EDITION), 2018, 19 (01): 103-106.

[9] Meiyu Ren, Jianchang Fu. “Network security situation assessment and prediction key technology research”[J]. network security technology and application, 2015 (11): 124-125.