Network security prediction method based on kubernetes

Zhengping Ruan*  
1 Aostar information Technologies Co., Ltd., Chengdu, Sichuan, 610000, PRC  
*Corresponding author’s e-mail: ruanzhengping@sgitg.sgcc.com.cn

Abstract. In order to improve the stability and security of network operation, a network security prediction method based on kubernetes is proposed. CPU resources are managed by kubernetes. Based on this, terminal data and resources are converged, and network extension is standardized according to the final situation value. Combined with POS algorithm, starting from the group theory, through the cooperation and competition between different particles in the network, a particle swarm optimization model of "network running speed network communication" is established. Through the relationship of particle swarm optimization in the network, the SVR parameters are optimized. The network security is predicted by extracting the characteristics of network load. Through the application of the design method, it is proved that this method can realize the effective prediction of network operation security.

1. Introduction
People's various behaviors in the network belong to a kind of behavior that can be monitored for the terminal. Because of this, some personal identity information or privacy files of network users are maliciously stolen when abnormal interference occurs in the network. This kind of problem has become the core problem of network users' normal use of the network. Therefore, it is necessary to design a prediction method for network security, which can sense the change trend of the network in real time, so that the network users can sense the fluctuation of the network in operation in time, and provide the decision-making basis for the operator whether to continue the operation in this way [1]. However, when the network development technology units deeply study this problem, it is found that the process of predicting network security is a nonlinear and time-varying fusion problem. Only according to the traditional network time sequence arrangement, it can not reflect the dynamic fluctuation of the network in real time, let alone effectively predict the operation of the network. Therefore, in this study, kubernetes technology is proposed, which is referred to as "k8s". K8s is an open source container choreography tool of Google company, and it is also the de facto container choreography standard today. Using k8s can efficiently deploy applications and expand or shrink their capacity. The purpose of introducing kubernetes is to improve the succinct and efficient operation of the terminal deployment information data container, so as to achieve the purpose of planning, updating and maintaining the network terminal. Although k8s has been widely used in public cloud and private cloud as the basic component of PAAS platform, most of its security research and application are still in the initial stage, and there are few extensive and effective cases. Therefore, based on the application of kubernetes, this paper designs the network security prediction method, and uses the related characteristics of k8s' reconciling and scheduling to realize the effective decoupling of different network information, so as to provide a more powerful tool for network security supervision.
2. Network security prediction method based on kubernetes

2.1. Network data extension based on kubernetes

In order to realize the effective prediction of network security, kubernetes is introduced in this paper to realize the extension of network data through the effective management of network resources [2]. In this process, considering that in the process of network security prediction, the situation change of terminal CPU is more significant, and the overall span value is higher. In order to avoid the influence of various factors of the terminal on this step behavior, kubernetes can be used for CPU resource management, and the terminal data and resources can be converged according to the final situation value, The network extension is standardized. Assuming that the situation value data set is expressed as $X_i$, then $x = [x_1, X_2, ..., x_n]$, where $x$ belongs to $R$ and $R$ is the extension dimension of network data. In this process, the formula for standardizing the extreme value of situation data can be expressed as follows.

$$x_i = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}}, i = 1, 2, ..., n$$  \hspace{1cm} (1)

In formula (1): $x_i$ is the extreme value of network security situation data after standardized processing; $x_{\min}$ is the minimum value of network security situation; $x_{\max}$ is the maximum value of network security situation. Based on the above formula, the security threshold range of kubernetes can be defined as $[x_{\min}, x_{\max}]$. In order to predict the network data more accurately, we need to delay and expand the deployment of $X$ in the network [3]. It should be considered that there is a certain decoupling relationship between the machine files in kubernetes. Therefore, a container image can be generated by packing the network data to occupy the network capacity, and the first-order network data can be expanded to the second-order network data by stack combination. In this way, the network can be expanded layer by layer, and the safe operation of the network can be finally determined, Its extension dimension should be expressed as M. In the process proposed above, the multi-dimensional extension process of the network can be represented in Table 1 below.

| Serial number | The sample is entered on the Kubernetes container side | Expected output value |
|---------------|-------------------------------------------------------|-----------------------|
| (1)           | $x_1, x_2, \ldots, x_{n-1}$                         | $x_n$                 |
| (2)           | $x_1, x_2, \ldots, x_{n-1}$                         | $x_{n+1}$             |
| (3)           | \ldots                                              | \ldots                |
| (4)           | $x_{n-1}, x_{n-2}, \ldots, x_n$                     | $x_n$                 |

According to the above way, a reorganized network operation situation data can be output to complete the extension processing of network data.

2.2. Selection and optimization of network SVR parameters

Considering the prediction of network security, the selection and use of any parameter will affect the prediction results to some extent, so it is necessary to optimize the network SVR parameters to ensure that the selected prediction parameters have real expression ability [4]. In the process of optimization, a particle swarm optimization model of "network running speed network communication" can be established through the POS algorithm, starting from the group theory, and through the cooperation and competition between different particles in the network. The SVR parameters can be described through the relationship of particle swarm in the network.

In the above content, it can be assumed that the network particle swarm is composed of Y particles, each particle is in the position of communication or information transmission node in the network, and only by constantly adjusting its own position can the stable transmission of information in the network be ensured. Therefore, the process of searching terminal location can be described as the process of...
finding the optimal solution. At this time, the position of the particle can be defined as the network node P, and the corresponding security transmission speed of P is s. Through real-time monitoring of the priority, the end-user behavior can be integrated, that is, the user can directly retrieve or locate the information transmission efficiency on the computer at this time. This process is also known as network security operation visualization.

After mastering the above information, we can know whether the particles pass through a node by calling the resource configuration of a node P. This method can not only avoid the tedious calculation, but also avoid the user's wrong behavior of node selection to a certain extent. Based on the above analysis, the method of continuously calling particle node P is adopted to locate a channel for information transmission or communication in the network, and the intermediate node is selected as the SVR parameter to output the parameter value, so as to realize the optimization of capacity node parameters.

2.3. Prediction of network operation security based on network operation load characteristics

After the completion of the above research, the network security operation can be comprehensively analyzed by the way of network operation load evaluation. In this way, the network operation load characteristics can be output to achieve the final prediction of network security [5]. The prediction process is shown in Figure 1.

![Network security operation load forecasting process](image)

Figure 1. Network security operation load forecasting process

After the output of network security operation load prediction results, the network communication port and network operation data are connected, and the resource usage input by the computer front end is sequenced. On this basis, the stability of the operation of the resource sequence is evaluated, that is, whether the sequence value meets the conditions of network security and stable operation is analyzed. If the conditions are met, the average value of the network operation resources needs to be processed. If
the conditions are not met, the sequence processing process should be returned. According to the above content, the average value of resources is processed as the basis of prediction. Assuming that the input value of the front end is greater than the average value, the network operation is considered to have security risk, otherwise, there is no security risk. To sum up, the design of network security prediction method based on kubernetes is completed.

3. Application analysis

Considering that the kubernetes capacity version used in this paper only supports the dynamic adjustment of CPU and memory resources, in this experiment, we need to build a kubernetes data cluster first, and configure the parameters of the terminal virtual machine equipment in the experiment process, as shown in Table 2 below.

| Serial number | Configured resources       | Parameters and specifications |
|---------------|---------------------------|------------------------------|
| (1)           | Kubernetes cluster        | Version 1.20.1               |
| (2)           | Master Node*1             | CPU: 2C Mem: 4G              |
| (3)           | Work Node*2               | CPU: 2C Mem: 8G              |
| (4)           | operating system          | CentOS 7.6                   |

After setting the parameters of the experiment, the average value of the resources is calculated, and the communication network is connected with the communication signal of the terminal virtual machine to keep the normal running state of the network. At this time, the virtual machine will predict the network security situation according to the calculated average resource load, and convert the predicted signal into the electronic signal that can be directly displayed by the computer. The fluctuation of the electronic signal is used as the basis to evaluate whether the network security prediction method is effective. If there is sudden and violent fluctuation in the electronic signal identified by the terminal, it can be considered that the network resources transmitted by the front end may affect the network security. On the contrary, if there is no significant fluctuation in the electronic signal identified by the terminal, it is considered that this method can not effectively evaluate the network security. On this basis, the comparative experiment is carried out, and some network security operation situation diagrams in the terminal display screen are intercepted. As shown in Figure 2 below.

![Figure 2. Partial situation diagram of network security operation](image)

According to the experimental results shown in Figure 2 above, there are three violent fluctuations in the continuous operation of the network. Therefore, it can be considered that the method designed in this paper has three network security operation risks after prediction. Based on this experiment, the final conclusion is that the network security prediction method based on kubernetes can effectively predict...
the network operation security, which can provide decision support for improving the stability of network operation.

4. Conclusion
Nowadays, the continuous development of high-tech, to a certain extent, provides more convenient conditions for people's daily life, whether it is work or buying products and other life behaviors, can be implemented on the basis of the network. But the network has strong development and freedom, which leads to frequent network terminal security problems. In order to solve this problem and achieve effective supervision of the network, this paper designs a prediction method for network security based on the application of kubernetes. After completing the design of the method, it is proved that this method can effectively predict the fluctuation of network operation through the application of an example.

References
[1] Nie Hua Wei, Deng Jie, Liao Xiao Mei. Research on road traffic safety prediction model based on RBF neural network [J]. Science and technology innovation, 2020 (27): 132-133
[2] Wan bin, Xu Ming. A network security prediction method based on Apriori algorithm [J]. Power information and communication technology, 2019,17 (01): 133-138
[3] Li Wentao. Eight network security predictions proposed by the company [J]. Software and integrated circuits, 2019 (z1): 37-39
[4] Qin Lina. Network security prediction based on Kalman filter [J]. Journal of Xiangnan University, 2019,40 (02): 22-25
[5] Jin Fang, long Juan. An elastic network traffic management method for kubernetes cluster [J]. Journal of Beijing Jiaotong University, 2020,44 (05): 77-86