# Network Efficacy Evaluation Based on AHP for Network Security Situation Assessment

Zhichao Yuan[1, a], Shan Yao[2, b], Chunhe Xia[3, c] and Shuang Xiang[3, d]

[1]Library, Beihang University, Beijing 100191, China;

[2]National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China;

[3]Beijing Key Laboratory of Network Technology, Beihang University, Beijing 100191, China.

[a]ieyuanzc@163.com, [b]yaoshan@cert.org.cn, [c]xch@buaa.edu.cn, [d]805051394@qq.com

**Keywords:** network security situation assessment, network efficacy evaluation.

**Abstract.** How to accurately find the risk existing in the network in time and rapidly put forward response plans put forward becomes a core issue in the new era of network security. Real-time quantitative assessment of network security situation due to its real-time problem discovery and reference value of assessment result has become an effective means to solve this problem. In this paper, according to the principles of real-time network security situation assessment technology we present a method of network efficacy evaluation based on Analytic Hierarchy Process to offer help to network security situation assessment. Our experiments show the proposed method can effectively improve the accuracy of the network situation assessment.

## 1. Introduction

Network security situation is an overall comprehensive concept, which can be understood as the current state and the future trend of the entire network. The so-called network security situation assessment is to full access, infer, vividly display the various security-related elements in network security situation, in order to logically analyze these kinds of information to predict what changes development might occur in the future of network security situation. The perception of network security situation has played an irreplaceable important role in the field of network security.

Tim Bass et al in 1999 proposed the concept of network situation to reflect the current status of the entire network [1]. Pew believes the security situation should include environment, goals, systems, available physical and human resources and other factors [2]. Shanmugavadivu designed a system to identify the invasion of activities based on fuzzy logic [3]. Årnes et al proposed to use hidden Markov models for real-time network situation assessment [4, 5].

Network efficacy evaluation is an important part of network security situation assessment. In this paper, according to the principles of real-time network security situation assessment technology we present a method of network efficacy evaluation based on Analytic Hierarchy Process to offer help to network security situation assessment.

## 2. Network Efficacy Evaluation

### 2.1 Indicators of Network Efficacy.

Network efficacy reflects the fact that network defense devices (IPS, firewalls, etc.) and network infrastructure devices (switches, routers, etc.) cannot provide adequate defense capability or services due to their high load, suffered attacks or some other destruction of the availability.

In order to evaluate network efficacy, considering the relevant network security data that can be obtained in actual network, we selected following indicators: connection number, bandwidth usage, CPU usage, memory usage.

- *Connection number*: connection number is to measure the maximum capacity of network security devices handling peer to peer connections. It directly reflects the access control ability of the network security devices for multiple connections. This indicator reflects the ability of the system to effectively deliver services.

- *Bandwidth usage*: bandwidth usage is to measure data transmission capability of network. If the bandwidth usage of network security devices is too high, it will affect the performance of the network and will further affect the normal activities of other network devices.
- *CPU usage*: CPU usage refers to the CPU average utilization of network security devices or hosts in a certain period. The higher CPU usage of the device is, the less its idle resources are and the more difficult it would complete other tasks.
- *Memory usage*: memory usage is similar to the CPU usage. It refers to the memory average utilization of network security devices or hosts in a certain period of time. The higher memory utilization of the device is, the less its idle resources are and the more difficult it would complete other tasks.

**2.2 Calculation of Overall Network Efficacy Indices.**

Depending on the target network status we can determine the weight of each indicator based on Analytic Hierarchy Process. The process is as follow:

1. Establish the hierarchy

By analyzing the relationship between network efficacy and CPU usage, memory usage, network bandwidth usage, connection number, we can create a two-layer structure as Fig. 1 shown below.

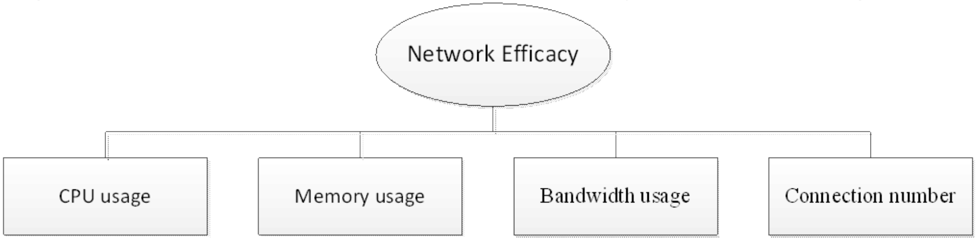

Fig. 1 Hierarchy of network efficacy

2. Construction and assignment of judgment matrix

Here we assume that memory usage is as important as CPU usage and that bandwidth usage and network connections are equally important. Since the main task of the network services is to provide services outside, network bandwidth usage and connection number are relatively more important than CPU usage and memory usage. Therefore, we establish the following judgment matrix.

Table 1 Judgment matrix of network efficacy

| | Connection number | Bandwidth usage | Memory usage | CPU usage |
|---|---|---|---|---|
| Connection number | 1 | 1 | 3 | 3 |
| Bandwidth usage | 1 | 1 | 3 | 3 |
| Memory usage | 1/3 | 1/3 | 1 | 1 |
| CPU usage | 1/3 | 1/3 | 1 | 1 |

3. Overall sort (calculate weight vector) and consistency check

According to AHP we use formula (1) to calculate the weight of each indicator.

$$W_i = \frac{1}{n}\sum_{j=1}^{n}\frac{a_{ij}}{\sum_{k=1}^{n} a_{kl}} . \qquad (1)$$

Consistency index is then calculated. After looking up the table, we can get R.I. = 0.89, and $C.I. = \frac{\lambda_{\max} - n}{n-1} = 0$, then $C.R. = \frac{C.I.}{R.I.} = 0 < 0.1$, so the consistency of judgment matrix is acceptable.

So we can get the weights of each indicator below:

Table 2 Weights of indicators in network

| CPU usage | Memory usage | Bandwidth usage | Connection number |
|---|---|---|---|
| 0.125 | 0.125 | 0.375 | 0.375 |

Next we can calculate the overall network efficacy indices according to formula (2):

$$E_t = \sum e_t^i w_i . \qquad (2)$$

## 3. Experiment

Our experimental environment is the production network of a certain department. The network connected to the Internet through a router. Firewall (FW), Intrusion Prevention System (IPS) and other security protection systems are deployed. Experimental data are set security event alert log and performance Indices running log of FW, IPS, and server hosts.

We import IPS data, server host data and other data into the database. Our test takes intervals of 5 minutes, and obtains the date for each piece of 40 intervals in order. Then we extract the main efficacy indicators of firewall, IPS, and hosts during that period. CPU usage, memory usage, bandwidth usage and connection number are shown separately below.

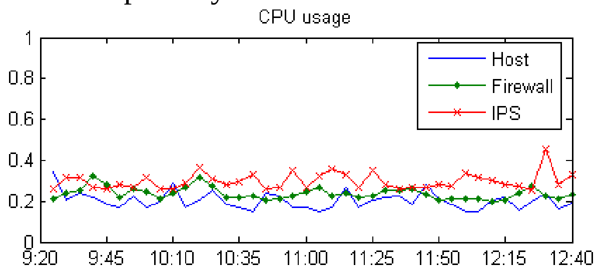

Fig. 3 CPU usage sequence

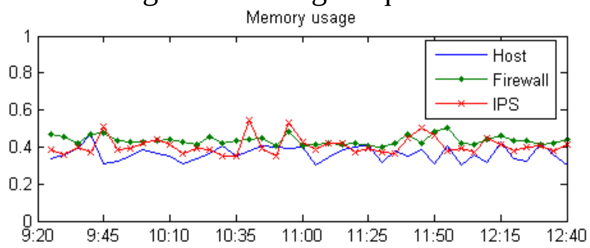

Fig. 4 Memory usage sequence

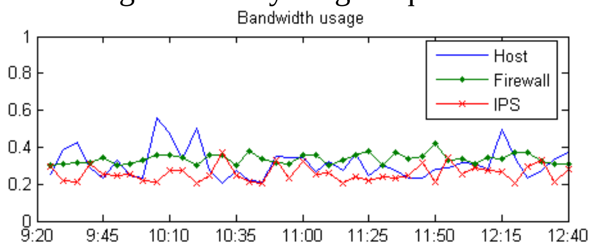

Fig. 5 Bandwidth usage sequence

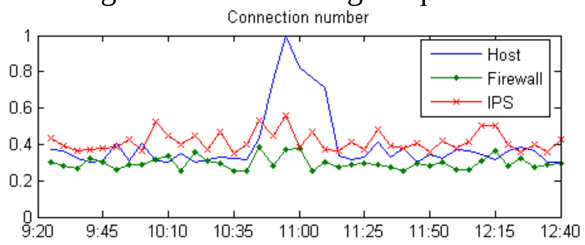

Fig. 6 Connection number sequence

We try to analyze the weight of each parameter through AHP. In addition, we observed that the network department does not provide large flow rate operation, but there will be large number of people online access at the same time. As a result, the importance of connection number is slightly larger than bandwidth usage. We give the following final modified judgment matrix:

Table 3 Modified judgment matrix

| | Connection number | Bandwidth usage | Memory usage | CPU usage |
|---|---|---|---|---|
| Connection number | 1 | 3 | 5 | 5 |
| Bandwidth usage | 1/3 | 1 | 3 | 3 |
| Memory usage | 1/5 | 1/3 | 1 | 1 |
| CPU usage | 1/5 | 1/3 | 1 | 1 |

With the program we get C.R. =0.0489<0.1, where it passed the consistency check. The weights of each indicator are as follow:

Table 4 Weights of indicators

| CPU usage | Memory usage | Bandwidth usage | Connection number |
|---|---|---|---|
| 0.5549 | 0.2516 | 0.0967 | 0.0967 |

At last, substituting these parameters we obtain the final network efficacy curve:

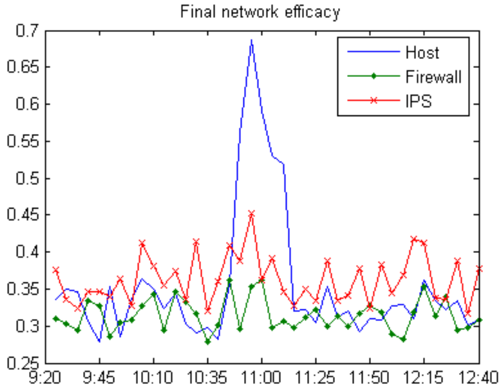

Fig. 7 Final network efficacy curve

Compared with the alert logs we can find it is at about 10:58 when the serious attacks occur. In our network efficacy curve we can also observe the network efficacy indicators abnormal. Especially the connection number approaches saturated, so the hosted services no longer have the ability to provide services outside, which means the network is under compromised state in actual. It is illustrated that the result of network efficacy evaluation technique we presented is in line with expectation.

## 4. Summary

In this paper, we propose a method of network efficacy evaluation for network security situation assessment. First, we analyze and select four reasonable indicators of network efficacy. Then, we based on AHP calculate network efficacy indices of the target network, which considers the actual network service situation. After executing the process, it will find the overall network efficacy. Based on the experimental verification for our method, the result is in line with expectation in the true environment. For future work, in order to improve our method, the network indicators of network efficacy may be more various. Also the next step we can embed our method into other different kinds of network security situation assessment model to improve the evaluation effect.

## 5. Acknowledgement

This work is supported by the project of AVIC under Grant No.CXY2011BH07.

## References

[1]. T. Bass. Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems. Proceedings of the IRIS National Symposium on Sensor and Data Fusion. 1999, p. 24-27.

[2]. R. Pew. The state of situation awareness measurement: Heading toward the next century. Situation awareness analysis and measurement, 2000, p. 33-50.

[3]. R. Shanmugavadivu, Dr N. Nagarajan. Learning of Intrusion Detector in Conceptual Approach of Fuzzy Towards Intrusion Methodology. International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2 (2012) No. 5, p. 246-250

[4]. A. Årnes, K. Sallhammar, K. Haslumet, et al. Real-time risk assessment with network sensors and intrusion detection systems. Computational Intelligence and Security. 2005, p. 388-397.

[5]. A. Årnes, F. Valeur, G. Vignaet, et al. Using Hidden Markov Models to Evaluate the Risks of Intrusions. Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2006, p. 145-164.