Multi-layer Network Attack and Defense Model Based on Entropy Method to Measure Network Security

Xiaolin Zhao, Jiong Guo, Xiaoyi Jiang, Jingjing Zhao and Hao Xu

School of Computer Science & Technology, Beijing Institute of Technology, 5 South Zhong Guan Cun Street, Hai Dian District Beijing 100081, China
Email: zhaoxl@bit.edu.cn
Email: jiong-guo@qq.com
Email: jxy.e@qq.com
Email: 531379963@qq.com
Email: xhao0403@163.com

Abstract. Network security is also facing major challenges. On the one hand, network security assessment can dynamically reflect the state of network security and reveal potential threats. On the other hand, network security assessment is the basis of network security management, it is also the prerequisite for building a reliable and secure network. This paper proposes a multi-level network security measurement model, which divides the network into a network environment layer and a network attack and defense layer. The network environment layer considers the network hardware security and the reliability of a network topology. The network attack and defense layer mainly examines the security status of the network from the perspective of network attack and defense. The model comprehensively evaluates and measures the network from different layers of the network, and conducts experiments. The result of experiment proves that the model can effectively assess the security of the network.

1. Introduction

The network security problems are being paid more attention to. The assessment of network security is the starting point to strengthen network security construction. The assessment of network security can not only judge the security of the network, but also find the problems to improve the security of the network. Therefore, it is very significant to propose an effective model of the network security.

At present, a series of methods for network security have been proposed at home and abroad [1]. Abasi pays attention to network security situation assessment, which can reflect on the dynamic security state. So Abasi proposed a new security situation assessment by comprehensively taking various network security factors [2]. Vulnerabilities are the weakness in the network and have pose serious threats, Suh-Lee et.al proposed a novel way to quantify the risk of vulnerability in the network [3]. Noel S et.al considers attack graph [4]. In addition, Elizabeth LeMay et.al proposed the adversary view security evaluation method to measure the strength of the network security [5]. By analyzing network attack graph, they evaluated the network security successfully. Zhang et.al proposed a new algebraic approach and a uniform algorithm to model and computing the Nash equilibria strategies on the model [6]. For enhancing the applicability of network security risk analysis, Liao et.al suggested a hierarchical fuzzy risk assessment method [7]. In his study, a fuzzy weighted average method was proposed to evaluate the fuzzy risk value. Zhang et.al considered network situation value, used the grey neural network to evaluate effectiveness of network situation security [8]. In addition, the US Infrastructure Advisory Board proposed Common Vulnerability Scoring System (CVSS) [9], which is a
measurement of individual vulnerabilities subjectivity but does not provide a good assessment of network security and potential attacks. In February 1994, China issued the "Regulations on the Security Protection of Computer Information Systems" [10]. Since then, it has been continuously improved, risk assessment methods are proposed for the environment, communication, equipment and data of the network.

2. Related Research

Most of the previous network metrics used qualitative assessment or attack graph-based method. The qualitative assessment does not use mathematical methods, but draws conclusion by the evaluator directly. Also, qualitative assessment generally assesses network security based on expert knowledge and experience, which is lack of objectivity [11]. Thus, human factors have a significant impact on final results. The risk analysis of network is a significant process. A declarative model for qualitative risk analysis is proposed to assess the risk of network [12]. Clark et.al proposed quantitative and qualitative techniques to assess vulnerability risk [13].

Compared to qualitative assessment, attack graph-based assessment is the mainstream method of quantitative measurement. In the network, there are always vulnerabilities and there is a certain relationship between these vulnerabilities. Specially, when the vulnerability is successfully exploited, another one may be used on this condition to threaten the network security. Therefore, the main idea of the attack graph is to use the vulnerability to gradually attack the network and finally attack aims. The attack graph-based assessment method is to use the attack graph to generate possible attack paths of the network, analyze them, and evaluate network security under different configurations. H. Kim used Bayesian network to model the uncertainty of network attacks [14]. Kaynar et.al explored taxonomy of attack graph generation and usage. And then using attack graph technology to evaluate the network security [15]. Liu proposed an attack graph generation method to improve efficiency. Then this model can be used to make a comprehensive analysis on network security [16].

Table 1 is the qualitative assessment and attack graph-based method comparison.

| Method                          | Comprehensiveness          | Objectivity   | Applicability       | Complexity        |
|---------------------------------|-----------------------------|---------------|---------------------|-------------------|
| Qualitative assessment          | Far from comprehensive     | subjectivity  | infrastructural construction | simplicity       |
| attack graph-based method       | focusing on the vulnerability| Comparatively objective | Vulnerability assessment | Generation are complex |

In summary, qualitative assessment has certain advantages. It can evaluate the unquantifiable network infrastructure and network security construction. However, it also has some limitations [17]. For example, it is impossible for qualitative assessment to quantify the assessment results. Also, the result is easy to be inaccurate and subjective due to the evaluator’s own reasons. The attack graph-based method mainly measures the security performance of the network in the view of network attackers, barely caring about the change of the security state in the network attack and defense. More importantly, the cost of constructing and processing the attack graph is bigger as the network scale increases. Only the vulnerability in the network is analyzed, which means the attack graph-based method is not comprehensive and has considerable flaws [18]. The multi-layer network attack and defense model proposed in this paper hopes to solve these problems. By stratifying the network and selecting a series of measurable and computable indicators, the model can quantitatively evaluate and measure the security of the network.

3. Multi-layer Network Attack and Defense Model Based on Entropy Method

3.1 Model Introduction

This paper proposes a multi-layer network attack and defense model to measure network security. The network is divided into a network environment layer and a network attack and defense layer. Network
environment layer considers the security situation of hardware and topology environment. Network attack and defense layer takes into account the security state during the network attack and defense process. In addition, it evaluates network’s ability whether the network can dynamically resist external attacks. Figure 1 shows architecture of the whole model.

![Figure 1. Model architecture](image)

The network environment layer considers the security of network from hardware and topology. The hardware security is the basis of network system security, so hardware security considers the installation and security strength of the hardware equipment. It mainly evaluates the hardware and network security status from the physical level. Topology also directly affects the security of the network system. Topology security emphasizes the network structure and vulnerability. From the perspective of physical connectivity, vulnerability threat and vulnerability prevention are considered to evaluate the reliability of the network.

On the one hand, the network attack and defense layer starts from the perspective of network attack and defense. Network normal state, attack process and attack result are described by characteristics metric (CM), effectiveness metric (EM) and impact metric (IM) respectively. On the other hand, the network attack and defense layer examines detection, protection, response, and management capabilities. To be specific, detection is an effective ways to discover possible vulnerabilities or attacks and monitor network state. Protection measures important assets and information in the network, ensuring availability and privacy through data encryption, access control and so on. Response, which can further protect network security, is a process that reacts rapidly and recover timely. Management is the centralized control of assets, data and security events in the network. In addition, management aims to ensure network security in the view of network operation and maintenance.

### 3.2 Entropy Method

Entropy can be used to measure ordering level of the whole complex system [19]. With the increase of entropy, it is obvious that the indeterminacy and information of a system decrease, and vice versa. According to this characteristic, we can judge the degree of dispersion of the index by the magnitude of entropy. Specifically, index’s dispersion and impact on the final evaluation result increase with the decrease of entropy. Therefore, entropy method can determine the index weight and provide a basis for evaluating the importance of the index.

To determine the weight, indicators need to be collected from the network repeatedly. Assume that j-th result of i-th indicator can be defined as $s^j_i$. After obtaining a series of data, because the units of measurement are different, it is primary to use range transformation to process these different index values. These original values finally convert to evaluable values so that different dimension cannot affect the subsequent process. Depending on their nature, the indicators are divided into positive parts and negative parts. For positive indicators, bigger values indicate better performance. However, bigger
values manifest more terrible performance for negative ones. Therefore, the two parts are processed in
different ways:

For positive indicator:

$$s_i' = \frac{s_i - s_i^{\min}}{s_i^{\max} - s_i^{\min}}$$  \hspace{1cm} (1)

For negative indicator:

$$s_i' = \frac{s_i^{\max} - s_i}{s_i^{\max} - s_i^{\min}}$$  \hspace{1cm} (2)

In formula (1) and (2),

$$s_i^{\max} = \max(s_i^1, s_i^2, ... s_i^n)$$  \hspace{1cm} (3)

$$s_i^{\min} = \min(s_i^1, s_i^2, ... s_i^n)$$  \hspace{1cm} (4)

Next, the probability distribution of indicators and entropy value can be calculated [20]. For discrete
distributed variable, information entropy can be defined as:

$$h_i = -\sum_{x \in \chi} p(x) \log(p(x))$$  \hspace{1cm} (5)

$\chi$ represents the sets of events while $p(x)$ is the probability of events. As for continuous random
variable, its cumulative distribution function $F(x)$ must be continuous. So when the derivative of
$F(x)$ exists, if $f(x) = F'(x)$ and $\int_{-\infty}^{+\infty} f(x) = 1$. Then $f(x)$ is the probability density function of
this continuous random variable. Therefore, its differential entropy can be defined as:

$$h = -\int f(x) \log(f(x))dx$$  \hspace{1cm} (6)

The indicators collected in the network have both discrete and continuous indicators. For
calculating entropy value conveniently, several common probability distributions for calculating
information entropy are as follows:

For Bernoulli distribution:

$$h = -(p \log p + (1-p) \log(1-p))$$  \hspace{1cm} (7)

For uniform distribution:

$$h = -\int_0^a \frac{1}{a} \log\left(\frac{1}{a}\right)dx = \log a$$  \hspace{1cm} (8)

For normal distribution:

$$h = -\int \phi \log\phi = \frac{1}{2} \log(2\pi e \sigma^2)$$  \hspace{1cm} (9)

Smaller entropy means the impact of indicator is bigger, which also means this indicator is more
important. Therefore, entropy value and indicator’s weight should be negatively correlated. Here, let
$g_i = 1 - h_i$, which indicate utility value of the indicator. Then i-th indicator’s weight can be defined as:

$$w_i = \frac{g_i}{\sum g_i}$$  \hspace{1cm} (10)
It can be seen that utility value and weight are increasing with the decrease of entropy. In other words, the more information the indicator provides to evaluate system, the more important the indicator is. Different from the ways of weighting subjectively such as AHP, entropy method determines weight by the degree of index value’s dispersion and tries to avoid the influence of human factors. In addition, entropy method reflects the amount of useful information provided by the evaluation object’s indicator. Also, it is a description of the influence on the indicator and can better distinguish the importance among the indicators.

3.3 Evaluation Process
In this paper, a multi-layer network attack and defense model based on entropy method is proposed. Respectively, environment layer and attack and defense layer are quantitatively modeled and measured. Then, a network security value can be calculated to evaluate and analyze the network security according to this value.

The first step to evaluate the network security is to choose appropriate indicators. The model divides the network into a network environment layer and a network attack and defense layer. Then each layer is divided into different dimensions. In each dimension, several indicators should be selected to measure network security quantificationally. Be aware that indicators should be different according to different network. Next, these indicators should be recorded repeatedly. Some values can be found directly in the system log while some may be obtained by some tools. In addition, there are several indicators can only be measured qualitatively, so these indicators are obtained through big data analytics.

The dimensions of these indicators we selected are different. So if we use them to evaluate directly, it is very possible that the evaluation results are uncertain. What is more, the results are totally wrong, thus losing the meaning of the evaluation. Therefore, it is necessary to properly process these data of the evaluation indicators before evaluating the network security. We should convert the actual value of the indicators into the values that can be using to calculate the security value. The most common methods is nondimensionalizing and normalizing these indicators. After that, we should calculate the probability distribution of each indicator. Then entropy method is used to determine and assign weight for each indicator in the entire model. Finally, we can obtain a security evaluation value and analyze the state of network security. The whole evaluation process is shown in Figure 2.

Figure 2. Evaluation process
4. Experiment

In order to test the validity of the proposed model, an experimental network platform environment is designed. Figure 3 shows the whole network which includes a router, a switch and some hosts. Supposed that the normal condition of the network, that is, the network has not been attacked, is the standard state. The network is the metric state when network is attacked by the Dos attack. Firstly, a security value under the standard state can be calculated. Then a Dos attack is performed to the network, and another network security value of the metric state network could be obtained. Finally, by comparing these two scores, we could draw the conclusion.

![Network topology graph](image)

**Figure 3.** Network topology graph

4.1 Experimental Process.

The first step is to select appropriate indicators for this experimental network. Hardware dimension chooses host state and network state. Host state measures CPU utilization, disk usage, memory usage, while network state measures peak flow and bandwidth utilization. Meanwhile, topology dimension selects vulnerability threat and cost of vulnerability prevention. Vulnerability threat evaluates the number of vulnerabilities and vulnerabilities strength while cost of vulnerability prevention is an effort to repair detected vulnerabilities. Through spotlight on windows, CPU utilization, disk usage and so on can be monitored before and after the Dos attack. Meanwhile a large amount of data is obtained for subsequent calculation and comparison. The number of vulnerabilities in the network and their threat level could be obtained by Nessus and then we could get threat score of vulnerabilities by comparing CVSS.

In the network attack and defense layer, CM measures static characteristics before attacked. Therefore, connectivity factor, number and strength of firewall, defense strategy, and emergency plan are selected in terms of detection, protection, response and management. EM measures the cost and effect of network attack and defense. Important of network assets, average flow, availability and safety technology management are chosen respectively. To be specific, availability measures completion degree of data transmission. Finally, IM measures security status and efficiency after the attack. In terms of four capacities, data encryption method, invulnerability, transmission delay, backup management are selected. Specially, management index values can be obtained through corresponding settings and security protection system in the network. Data flow, invulnerability and other similar indicators could be obtained by jmeter and spotlight on windows. In addition, no technical indicators are obtained through big data analytics, which has certain reference significance.

After obtaining these indicators, data of standard state can be calculated by some tools. Then we could get each standard value. Then a Dos attack is performed to the network. In this process, data are obtained and processed. Next, entropy method is used to calculate weight of each indicator. Finally, metric value of the state of metric network could be calculated. Table 2 shows selected indicators and their standard and metric values.
### Table 2. Indicator values of experimental results

| Layer                           | Dimension | Indicator                               | Standard value | Metric value |
|---------------------------------|-----------|-----------------------------------------|----------------|--------------|
| Network environment layer       | Hardware  | Host state                              | 0.8949         | 0.3599       |
|                                 | Topology  | Network state                           | 0.3850         | 0.1464       |
|                                 | Topology  | Vulnerability threat                    | 0.7633         | 0.7627       |
|                                 | CM        | Cost of vulnerability prevention        | 0.6960         | 0.6790       |
|                                 | Protection| Connectivity factor,                    | 0.2867         | 0.1670       |
|                                 | Response  | Number and strength of firewall         | 0.8300         | 0.8300       |
|                                 | Management| Defense strategy                        | 0.5630         | 0.4670       |
|                                 | EM        | Emergency plan                          | 1.0000         | 1.0000       |
|                                 | CM        | Important of network assets             | 0.6420         | 0.5680       |
| Network attack and defense layer| Protection| Average flow                            | 0.4593         | 0.2517       |
|                                 | Response  | Availability                            | 0.9163         | 0.4520       |
|                                 | Management| Safety technology management            | 1.0000         | 1.0000       |
|                                 | Detection | Data encryption method                  | 0.072          | 0.072        |
|                                 | EM        | Invulnerability                         | 0.6260         | 0.6000       |
|                                 | IM        | Transmission delay                      | 1.0000         | 0.8900       |
|                                 | Management| Backup management                       | 1.0000         | 1.0000       |

### 4.2 Experimental Results

First, in the standard network environment, conventional data can be obtained to calculate a standard security value. Secondly, by performing a Dos attack on the network, tools such as spotlight on windows are used to record changes in CPU utilization, network flow and so on. After obtaining the value of each indicator, the given model can be used to obtain a final metric security value. The experimental results are shown in Table 3.

### Table 3. Comparison of experimental results

| Network         | Network environment layer value | Network attack and defense layer value | Network security value |
|-----------------|---------------------------------|---------------------------------------|------------------------|
| Standard network| 0.6934                          | 0.7146                                | 0.7093                 |
| Metric network  | 0.4908                          | 0.6243                                | 0.5909                 |

### 5. Conclusion

The multi-layer network attack and defense model proposed in this paper not only evaluates network environmental security, but also pays more attention to dynamic evolution during network attack and defense process. More important is choosing some static and dynamic indicators before and after the attack from the aspects of detection, protection, response and management, which evaluates the security of the network dynamically and roundly. Particularly, weight of the indicator is calculated by entropy method, which decreases the interference of human factors to the maximum extent. Finally, the model is verified by experiment that shows metric security value obtained after the Dos attack is smaller than standard security value. This result is consistent with actual situation of the network security state. Therefore, the model proposed in this paper is effective.

However, this paper also has some shortcomings. On the one hand, because there is no scientific selection method to choose network indicators, there are some subjective understandings during selection and allocation of indicators in the network attack and defense layer. On the other hand, using entropy method to evaluate the weights of a large number of indicators has a problem that the computation complexity is great. Hence, the focus of the next step study is to solve the problem that how to select indicators more convincing and calculate the weights of a large number of indicators more efficient.
6. **Acknowledgement**

This work was supported by National Key R&D Program of China (Grant No.2 2016YFB0800700).

7. **Reference**

[1] Kumar S N. Review on Network Security and Cryptography 2015. *J. International Transaction of Electrical and Computer Engineers System*.

[2] Abasi. A study on network security situation evaluation model 2014. *Applied Mechanics and Materials*, v 556-562, 5312-15

[3] Suh-Lee, C, Juyeon Jo. Quantifying security risk by measuring network risk conditions. 2015 *IEEE/ACIS 14th International Conference on Computer and Information Science*. 9-14.

[4] Noel S, Jajodia S. Metrics suite for network attack graph analytics 2014. *Proceedings of the 9th annual Cyber and Information Security Research Conference*. ACM, 5-8.

[5] LeMay E, Unkenholz W, Parks D, Muchrce C, Keefe K, and Sanders W H. Adversary-driven state-based system security evaluation 2010. *In Proceedings of the 6th International Workshop on Security Measurements and Metrics (MetriSec ’10)*. ACM, New York, NY, USA, Article 5, 9 pages.

[6] Zhang Q, Jiang Y. Modelling and analysis of network security: an algebraic approach 2016. *2016 IEEE Trustcom / BigdataSE / ISPA*, 308-15.

[7] Liao Y T, Ma C B, Zhang C. A new fuzzy risk assessment method for the network security based on fuzzy similarity measure 2006. *Sixth World Congress on Intelligent Control and Automation*, 5pp.

[8] Zhang S B, Shen Y J. Network security situation prediction model based on multi-swarm chaotic particle optimization and optimized grey neural network 2018. *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS). Proceedings*, 426-9.

[9] MELL P. The common vulnerability scoring system (CVSS) and its applicability to federal agency system 2007 R, [S.I.]: NIST.

[10] GB/T22239-2008. Information Security Technology – Basic Requirements for Security Protection of Computer Information Systems S 2008. Beijing: China Standard Press.

[11] Vadim S L. How to measure qualitative data. Fuzzy Information Processing Society 2015. *IEEE*, 1-4.

[12] Rahman, Mohammad Ashiqur, Al-Shaer, Ehab. A formal approach for network security management based on qualitative risk analysis 2013. *Proceedings of the 2013 IFIP/IEEE International Symposium on Integrated Network Management*, p 244-251.

[13] Clark, K. Tyree, S. Dawkins, J. Hale, J. Qualitative and quantitative analytical techniques for network security assessment 2004. *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop (IEEE Cat. No.04EX879)*, 321-8.

[14] Kim H, Reich J, Gupta J, Shahbaz M and Feamster N. “Kinetic: verifiable dynamic network control” 2015. *Usenix NSDI*.

[15] Kaynar K. A taxonomy for attack graph generation and usage in network security 2016. *Journal of Information Security & Applications*, 29(C):27-56.

[16] Liu Z M. Li S. Complex network security analysis based on attack graph model 2012. *Proceeding of the 2012 2nd International Conference on Instrumentation and Measurement*.

[17] Liu X. Information security risk assessment model based on dynamic threat value and fault tree 2014 D. Lanzhou: Lanzhou University.

[18] Xie L X, Qiu X R, Li X F. Research on network security risk assessment based on attack graph model 2014. *Microelectronics and Computers*, 7: 77-83.

[19] Callegari C, Giordano S, and Pagano M. Entropy – based network anomaly detection 2017. *In 2017 International Conference on Computing Networking and Communications. (ICNC’2017)*.

[20] Chen S B and Wang X F. Feature Selection Algorithm for Incomplete data based on information entropy 2014. *PR & AI*. 27(12): 1131-1137.