Construction and Security Measurement of Cybersecurity Metrics Framework Based on Network Behavior

Xiaolin Zhao, Jingjing Zhao, Xiaoyi Jiang, Xiaoyu Zhang and Wentai Zhang

School of Computer Science & Technology, Beijing Institute of Technology, 5 South Zhong Guan Cun Street, Haidian District Beijing 100081, China
Email: zhaoxl@bit.edu.cn
Email: 531379963@qq.com
Email: jxy.e@qq.com
Email: zxy_officemail@163.com
Email: 3120181098@bit.edu.cn

Abstract. Cyberspace security involves national security, enterprise security, personal privacy security and so on, which has been paid more and more attention by the state. Cyberspace security measurement is an important step to protect any network. The important premise is to establish a reasonable and universal security measurement framework for network systems. But the network is very complex, and the network security state is changing all the time. Existing information security models lack the description of network behavior. Aiming at this problem, in this paper, the existing information security models at home and abroad are compared and analysed, and their advantages and disadvantages are summarized. Based on PDR (Protection, Detection, Response) model, this paper adds management functions, and optimizes the original concept of PDR model. On this basis, we add characteristic measurement, efficiency measurement and impact measurement to form 12 indicators to dynamically reveal the evolution mechanism of security characteristics measurement indicators. AHP is used to distribute the weight of each dimension, and the network is evaluated quantitatively from four dimensions: detection, protection, response and management. The framework of the proposed metric framework is verified by experiments.

1. Introduction

With the development of the times, the information technology revolution is changing with each passing day and flourishing, which has a profound impact on the development of international politics, economy, culture, society, military and other fields. Internet has been integrated into all aspects of people's lives. People's life is more and more inseparable from Internet products, which brings convenience to people, but also brings many hidden dangers of cyberspace security. Network attacks emerge in endlessly, causing great losses to the state, enterprises and individuals. Cyberspace security is a major strategic issue concerning national security, national development and the work and life of the broad masses of the people.

Cyberspace security measurement is an important step to protect any network. Accurate and effective network measurement can help cyberspace security researchers to judge the security status of the current system, so as to design security countermeasures and take better emergency measures. At the same time, it gradually strengthens the robustness and integrity of cyberspace security, and reduces the occurrence of cyberspace security accidents. But the network system is very complex, the network threats are more and more diverse, and the state of the network is changing at any time. Therefore, it is
necessary to establish an metric framework that can reflect the dynamic evolution mechanism of network and measure the network.

2. Researches of Metric Framework for Measuring Cyberspace Security

This section mainly describes the basic concepts of Cyberspace Security assessment. The existing cyberspace security measurement framework is compared and analysed.

2.1. Concepts of Metric Framework for Cyberspace Security Measurement

The network system is very large and complex, and it is dynamic. To evaluate cyberspace security, we should not only take into account the dynamic changes in the network, but also take into account the security of network hardware and equipment, technical personnel management and other factors. Therefore, first of all, we should have a comprehensive metric framework. This requires the framework to include not only dynamic changes in the network system indicators, but also static indicators such as personnel management, host hardware conditions and so on. Most of the existing security models at home and abroad take these factors into account and are very comprehensive. On the one hand, most of them are qualitative standards and requirements. There is no more detailed description of cyberspace security metrics. Because it is very difficult to collect more detailed cyberspace security metrics, and it is difficult to quantify. This is also a major challenge for cyberspace security assessment.

Most of the existing cyberspace security assessment models classify the security level of the network system. However, in order to measure the network system accurately, it is necessary to have the precise values of various indicators to make a comprehensive evaluation of the network system. Cyberspace security measurement is not a unilateral measurement. Consideration should be given to the dynamic changes in practical applications, including changes in the cyberspace security environment, changes in response strategies, and so on. There is also a correlation between the indicators. So it's very complicated and difficult to measure.

2.2. Comparative Analysis of Network Information Security Framework

There are also some static and qualitative evaluation criteria for network information security measurement at home and abroad. The International Organization for Standards (ISO) proposed the OSI security architecture [1]. At the beginning of this model, it mainly focused on the research of information security technology and model. It is not suitable for dynamic network. It is designated for stand-alone system and cannot reflect the distributed and dynamic cyberspace security problems. NIST Cyberspace security Framework was first released by the National Institute of Standards and Technology in 2014 to help companies, especially key infrastructure departments, manage cyberspace security risks [2]. There is a great subjectivity in the implementation process. Quantitative evaluation of indicators has not been achieved. IATF is a guidance document formulated by the National Security Agency (NSA) to describe its information security [3]. Based on the information security standards of TCSEC, ITSEC in Europe, CCTEC in Canada and FC in the United States, the Common Criteria for Information Security Technology Evaluation was proposed by seven parties from six countries (National Security Agency and National Institute of Technical Standards, Canada, Britain, France, Germany and the Netherlands). CC) is short for CC standard. However, due to the complexity and time-consuming of the certification process, many companies do not participate in CC certification [4].

The "Information System Security Level Protection" series of criteria refers to the hierarchical security protection of information systems that store, transmit and process information [5]. The security products used in the information system are managed according to the level, and the information security incidents occurring in the information system are dealt with according to the level. On May 13, 2019, version 2.0 of Cyberspace security Level Protection (hereinafter referred to as Equal Guarantee 2.0) was officially released.

It can be seen that in recent years, the cyberspace security model has been gradually optimized from static model to dynamic model. Some network models do not consider such factors as personnel management and equipment management. The main focus is on the evaluation of information security. And most of the evaluation bases are qualitative indicators, which are difficult to quantify. From the
perspective of information security alone, the dynamic evolution process of network cannot be reflected.

2.3. Overview of PDR Model
ISS (American Internet Security System) company has proposed PDR (Protection Detection Response), PPDR (Policy Protection Detection Response) and other models [6]. PDRR (Protection Detection Reaction Recovery) model has been proposed by the U.S. Department of Defense. WPDRRRC (Warning Protection Detection Reaction Recovery Counterattack) was proposed by the "863" Information Security Expert Group of China [7]. The core of these models is a loop based on protection, detection and response.

In the PDR model, a loop is composed of protection, detection and response. PPDR model adds security policy on the basis of PDR model. PDRR model adds recovery function on the basis of PDR model. Both analyse the movement of the network, but lack the description of the network behavior. WPDRRRC model includes Warning Protection Detection Reaction Recovery Counterattack, which is more comprehensive. Protection is the preventive measures adopted according to the security problems that may arise in the system. When the attacker penetrates the protection system, detection will play a role. At the same time, the response system starts to work, and processes the response and recovery. Other models add functions on the basis of PDR, which makes the whole model more reasonable and comprehensive.

In terms of cyberspace security measurement, PDR class models are time-based provable security models. Definition: Protection time Pt (the time when hackers initiate an attack to protect the system from being broken), detection time Dt (the time from initiating an attack to detecting an attack) and response time Rt (the time from discovering an attack to making an effective response). When Pt > Dt + Rt, that is to say, the system is safe. That is to say, if the hacker discovers and stops the hacker's behavior before he breaks down the system, the system is safe.

The basic model of PDR is a dynamic protection system, but its cyberspace security measurement method is relatively single. It cannot evaluate the security of the whole network system from many aspects, nor can it reflect the dynamic evolution mechanism of network measurement index. Based on the above model, management elements are added to the PDR model to form the PDRM (Protection, Detection, Response, and Management) security protection system. In terms of network measurement, from 12 aspects, we select quantifiable indicators and use AHP to analyse the weight of indicators. Finally, we get the overall score of cyberspace security.

2.4. Research on Cyberspace Security Metrics
At present, the common cyberspace security measurement methods are cyberspace security measurement method based on attack graph [8]. In the past, expert assessment method is one of cyberspace security evaluation methods [9]. Combining attack graph and Bayesian network CVSS score to measure the overall cyberspace security [10]. PagePank algorithm [11] is also used in some security assessment models. TOPSIS method can be used to measure the criticality of network assets [12]. In addition, the grey relational degree algorithm can be applied to cyberspace security measurement [13]. Fuzzy comprehensive evaluation method is often used for cyberspace security risk assessment [14]. AHP Analytic Hierarchy Process is usually used to analyse the weights of indicators in the network system [15]. Delphi method is a method of consulting experts to evaluate, summarize and converge back to back with letters [16]. Hatizivasilis et al.[17] gave a method to measure software security, privacy, and dependency. Rahman et al. [18] proposed a formal approach for network security management based on qualitative risk analysis. Doynikova et al. [19] proposed a CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection. [19]. Doynikova et al. [20] proposed Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks. Simon et al.[21] proposed a systematic evaluation of cyber security metrics for dynamic networks. Jin et al.[22] proposed dynamic security metrics for measuring the effectiveness of moving target defense techniques. Teresa et al.[23] proposed security metrics to evaluate organizational IT security. Qazi et al. [24] proposed to use multirate delphi to secure
multirate ad hoc networks against wormhole attacks. Gharib et al. [25] proposed an evaluation framework for intrusion detection dataset.

2.5. A Brief Introduction to Analytic Hierarchy Process (AHP)

The following table shows the current situation. See Table 1. Comparison of network security assessment methods.

Table 1. Comparison of network security assessment methods

| Method name                      | Advantages                                      | Disadvantages                                                                 |
|----------------------------------|-------------------------------------------------|-------------------------------------------------------------------------------|
| Delphi method                    | simple operation, expert knowledge can be used, | strong subjectivity, difficult to converge conclusions when evaluating by many |
|                                  | and the conclusion is easy to use.             | people                                                                         |
| measure method                   | describe all possible attacks in the network    | low efficiency, long construction cycle, high demand for users' knowledge and |
| based on attack graph            |                                                 | skills, and possible to cause path explosion                                  |
| relational matrix analysis       | high reliability and small error                | the factors of the evaluation object cannot be multiple (generally no more than 9). |
| fuzzy comprehensive evaluation   | overcome the disadvantage of 'unique solution'  | cannot solve the problem of information duplication among evaluation indexes,  |
|                                  | in traditional mathematical method.             | membership function, fuzzy correlation matrix and other determination methods  |
|                                  | According to different possibilities, the solution| need to be further researched                                                 |
|                                  | of multiple levels of problems is obtained.    |                                                                                |

Analytical Hierarchy Process (AHP) refers to the decision-making method that divides the elements that are always related to decision-making into objectives, criteria, schemes and other levels, on which qualitative and quantitative analysis can be carried out. In the AHP analysis of indicators, first of all, the hierarchical structure model should be established, and the factors of evaluating cyberspace security should be considered as comprehensively as possible. Then the judgment matrix is constructed, and then the two indexes involved are compared with each other. The constructed judgment matrix is normalized and its maximum eigenvalue is obtained for consistency checking. AHP weight analysis method is relatively simple and easy to operate, and more objective than other weight analysis methods. It is a static, expert-dependent weight analysis method. It is also a more general method of weight analysis. Compared with the various methods in the Table 1. Comparison of network security assessment methods, analytic hierarchy process is preferable. Therefore, this paper uses this weight analysis method.

3. Construction of Metric Framework Model

From the angle of attack-defense confrontation and combining the advantages of the above model, this paper establishes a cyberspace security measurement metric framework model based on 12 index points. CEI-PDRM (Characteristic, Efficiency, Influence, Protection, Detection, Response, Management).

3.1. PDRM Framework

This paper proposes a PDRM model based on PDR model. On the basis of PDR model, management function is added. Some optimization and improvement have been made on the original concept. The PDRM model includes four aspects: Protection, Detection, Response, Management.
1) Protection: Before the attack, the network system is protected by data encryption, identity authentication, firewall and so on.

2) Detection: When the attack penetrates the defense system, the detection function plays a role. In practice, the defender does not know when the attack occurs. Only through real-time observation system can it be possible to judge the attack occurring time. Once an attack is detected, the detection system generates data continuously and provides it to the response layer and the management layer. So as to formulate strategies

3) Response: Once an attack is detected, the response system starts to work and process the event., which including emergency response and recovery processing. At the same time, new management strategies are constantly acquired from management. Then adjust the response behavior.

4) Management: Management is the core of the model. All protection, detection and response are implemented according to security policy. At the same time, all protection, detection and response are also fed back to the management system for policy adjustment in real time. Thus a dynamic attack-defense ring system is formed.

These four aspects dynamically describe the network movement from the perspective of the defensive side. The PDRM framework takes management as its core and describes the defense, detection and response states in the network. It is a dynamic and complete network movement cycle.

3.2. OODA(Observe, Orient, Decide, Act)Modeling

OODA cycle theory is Boyd's classical battle model, which is used to describe and study the command and control process in the battle process by analyzing his battle experience for many years. In addition to its application in the field of war strategy, this model is also widely used in business, political and other fields. OODA cycle theory consists of four steps: observe, orient, decide, act. In the whole process, the four steps mentioned above are feedback to each other. The purpose of observation is to detect the evolving external environment, continuously provide information for the "judgment" link, and provide guidance and basis for judgment. Decision-making is to formulate a reasonable and feasible operational plan at the macro level of enemy information obtained from observation and judgment. Action is the concrete implementation of decision-making.

3.3. OODA Circle Based on Network Behavior

Every object can be regarded as consisting of the object itself and its own motion attributes. The composition of things and the characteristics of their space-time structure can be used as the identification characteristics to describe this object. The efficiency attributes formed by the movement of things can be seen as the efficiency effects on describing the object. Identification characteristics can be represented by characteristic metrics (CM). Efficiency impact can be expressed by efficiency metrics (EM) and impact metrics (IM). These three metrics can accurately describe the behavior process of the network. The network behavior is represented by CM, EM and IM from three aspects: before attack, during attack and after attack. In this way, the attack and defense process of the network system can be described comprehensively.

Based on the above theory, CM, EM and IM are applied to the measurement framework of cyberspace security system.

1) CM: Measurements of network system security characteristics, identification characteristics of things composition and their temporal and spatial structure, which are used to characterize network characteristics before attacks occur.

2) EM: It is a efficiency measurement of cyberspace security behavior, the efficiency attributes formed by the movement of things, are used to characterize the characteristics of the network in the process of attack and defense.

3) IM: Measuring the impact of cyberspace security behavior, task function and capability efficiency, used to characterize the impact of attacks on the network.

From the perspective of attack-defense confrontation, this paper combines CM, EM, IM and OODA cycle theory to form a new dynamic attack-defense system. It includes the loop of safety measurement, safety judgment, safety decision and behavior feedback. As is shown in Figure 1. OODA circle based on network behavior.
Safety measurement: Before the attack occurs, the network system environment is observed and detected. The static characteristics of the network environment are detected and represented by CM. Dynamic efficiency characteristics of network environment are detected and expressed by EM. When an attack occurs, the corresponding EM must change and record it at this time. After the attack, the attack has a certain impact on the current network environment. IM is used to characterize the impact of the attack on the network.

Safety analysis: Preliminary safety analysis is carried out by using EM and IM detected by safety measurement. Information is provided to decision makers and feedback is given to the first step of observation activities.

Security Decision-making: Integrate the information from security analysis and security judgment, and make a cyberspace security defense plan and make a decision based on the network system environment CM.

Safety Action: To implement the scheme of safety decision-making. In the process of implementation, real-time feedback information is provided for the first three steps to form a dynamic OODA cycle with real-time regulation function.

3.4. Metric Framework Model of Cyber Security Measurement

From the angle of attack-defense confrontation, this paper combines the advantages of the above model. PDRM model is regarded as the first dimension of network security measurement model. PDRM model dynamically describes the network movement from the perspective of the defender. The PDRM framework takes management as its core and describes the defense, detection and response states in the network. It is a dynamic and complete network movement cycle. Therefore, taking PDRM as the first dimension of network security evaluation model is comprehensive and reasonable. CM, EM and IM are considered as the second dimension in the framework of PDRM. These three metrics can accurately describe the behavior process of the network. The network behavior is represented by CM, EM and IM from three aspects: before attack, during attack and after attack. In this way, the attack and defense process of the network system can be described comprehensively. Therefore, it is reasonable to regard CM, EM and IM as the second dimension in the framework of PDRM. A network security measurement index system model based on 12 index points is established. That is, CEIPDRM (Characteristic, Efficiency, Impact-Protection, Detection, Response, Management) is shown in the framework diagram of the indicator system as shown in Figure 2. Metric framework.

Figure 1. OODA circle based on network behavior

Figure 2. Metric framework
### 3.5. Detailed Description of 12 Measurement Points

In CEI-PDRM model, 12 First level index points include: protective characteristic metrics, protective efficiency metrics, protective impact metrics, detection characteristic metrics, detection efficiency metrics, detection impact metrics, response characteristic metrics, response efficiency metrics, response impact metrics, management characteristic metrics, Management efficiency metrics and management impact metrics. There are several intermediate indicators describing network behavior under 12 metrics. There are corresponding meta-indicators under each intermediate index. There are more than 30 secondary indicators and nearly 100 tertiary indicators. **Table 2.** 12 Measurement points shows some of the indicators.

| Level 1 Indicators | Level 2 Indicators | Level 3 Indicators |
|--------------------|--------------------|--------------------|
| protective strength | number of firewalls | protective strength |
| protective strength | network architecture | network protection policy strength |
| network and communication security | border protection | host protection policy strength |
| vulnerability threat metrics | network intrusion prevention | event detection delay |
| protection strategy strength | network node malicious code prevention | vulnerability measure |
| event detection delay | number of vulnerabilities | collection software vulnerability severity |
| attack graph class | vulnerability level | number of attack paths |
| probability indicator of the attack graph | minimum attack path length | |
| host status | attack graph achievement | |
| CPU usage | |
| disk usage | |
| memory usage | |
| Open port number index | |
| peak flow | |
| average flow | |
| bandwidth utilization | |
| number of viruses | |
| virus intrusion duration | |

**Table 2.** 12 Measurement points
3.6. CEI-PDRM Framework

The CEI-PDRM two-dimensional model has the following advantages:

1) Dynamics: From the perspective of attack-defense confrontation, constantly monitor the changes of relevant indicators in the network environment, pay attention to the dynamic evolution of system security over time, and make security decisions.

2) Comprehensive: The defense process is divided into four aspects: protection, detection, response and management. It not only measures the state change index of the network system in the process of attack and defense, but also measures some indicators of hardware and personnel operation. It covers a series of relevant indicators before, during and after the attack.

3) Quantifiable: In the past, most of the index measurement models used to analyze and evaluate the cyberspace security status from a qualitative perspective, and roughly classify the security level. The metric framework of security metrics proposed in this paper provides quantitative calculation, which makes the evaluation results more accurate.

4) Dynamic Indicators: This model is applicable to quantifiable indicators, and reveals the evolution mechanism of safety characteristics measurement indicators. Compared with the traditional security model, it can better reflect the dynamic evolution of the network.

In this paper, CEI-PDRM two-dimensional model has the following disadvantages:

Although the framework proposed in this paper cover a comprehensive range, it can also be used for quantitative calculation of indicators. However, there is a certain subjectivity in the selection of indicators. If the indicators are not selected properly, it will have a great impact on the security evaluation of the entire network system. Moreover, the network system is very complex, and there are many interacting indicators. How to calculate and deal with the correlation between indicators is also a challenging issue.

4. Experimental Process and Results

This paper uses the following experiments to analyze and calculate to verify the rationality of the proposed cyber security metrics framework of cyber security measurement. This paper constructs two network environments. One is the normal network environment, the other is the network environment attacked by DoS. The index values under these two network environments are measured, and the weights of these index values are calculated by analytic hierarchy process, and then the network is
scored comprehensively. By comparing the network score under normal condition and the network score after DoS attack, we can prove that the framework proposed in this paper is effective. In order to prove the rationality and feasibility of this framework, an experiment is designed according to Figure 3. Flow chart of experiment.

![Flow chart of experiment](image)

**Figure 3.** Flow chart of experiment

4.1. Experimental Process
The network consists of one router, one switch and several hosts. In the experiment, the DDOS attack method was used to attack the target network, and various tools such as perfmon and Nessus were used to record the changes of the selected indicators in the network system and the indicators were dimensionless. The weights of the indicators in the network are assigned, and finally the security values of the network system are comprehensively calculated.

1) Indicator acquisition: The network without DoS attack is first collected. Monitor and collect traffic class metrics by using Perfmon tools. Nessus is used to scan the network for vulnerabilities and get the information of vulnerabilities, so as to calculate the response indicators. Use system commands to obtain open port information in the network, etc.

2) Attacking: Attacking the target in the network by using XOIC tools. Select the host whose IP is 192.168.1.103 in the network, and choose the 137 port of UDP to attack DoS. Continue to use the above tools to collect indicators in the network.

3) Index processing: Firstly, each sub-index is quantified. Using analytic hierarchy process (AHP) to distribute weights, 12 intermediate indicators were scored. The four dimensions of
protection, detection, response and management were scored respectively. Finally, four dimensions are synthesized to evaluate the security of the network system. As shown in the figure.

4.2. Experimental Environment
The target network can be determined according to the actual situation. This evaluation object builds a real small network environment for itself.

Using virtual mechanism to build network environment. The network consists of a router, a switch and several hosts. Routers are responsible for network connectivity. Switches connect several hosts in the network. The network topology of this experiment is shown in the following Figure 4. Experimental topology

![Figure 4. Experimental topology](image)

4.3. Indicator Selection
The protective strength index is adopted as the characteristic index of protective class. The protection strength includes the number and strength of firewalls, which are mainly obtained by evaluating the incoming and outgoing information. The protective utility index is vulnerability threat index. The vulnerability threat index is quantified by the number and level of vulnerabilities. The impact index is expressed by the strength of protection strategy. Quantitative value of comprehensive protection strategy strength obtained from the protection intensity of integrated network and host protection strategy.

The characteristic indicators of the detection class are host state, including CPU occupancy index, memory occupancy index, disk occupancy index and open port index. The above four three-level indicators are obtained through experiments. After normalization, the weights are obtained by AHP analytic hierarchy process. Calculate the host state value. Utility indicators are network state index, including peak traffic index, average traffic index and bandwidth utilization index. The values of three traffic indicators are obtained by experiments, and the network state values are obtained by analytic hierarchy process (AHP). Influencing indicators select virus hazard detection, including the number of viruses and the length of virus invasion. The value of virus hazard detection is obtained by quantifying the two indicators.

In response class, blacklist response time index is selected as feature index. Record the time from detecting malicious entities to blacklisting each time, and then add up the time when each malicious entity was blacklisted. This index cannot be detected in this experiment, so it is set to be empty. Utility index chooses intrusion response time. The average first intrusion time is used to quantify. The backup
management indicators are selected for impact indicators. If the network system has a backup, the value is 1, and if there is no backup, the value is 0.

Table 3. Indicator values of experimental results

| First dimension | Second dimension | Indicator name                      | Pre-attack indicators | Indicator value after DDOS attack |
|-----------------|------------------|-------------------------------------|-----------------------|----------------------------------|
| Protection      | CM               | Protective strength                 | 0.829                 | 0.829                            |
|                 | EM               | Vulnerability threat index          | 0.761                 | 0.791                            |
|                 | IM               | Protection strategy strength        | 0.560                 | 0.465                            |
| Detection       | CM               | Host Status                         | 0.822                 | 0.535                            |
|                 | EM               | Flow change                         | 0.421                 | 0.410                            |
|                 | IM               | Hazard metric                       | 0.715                 | 0.635                            |
| Response        | CM               | Blacklist response time index       | null                  | null                             |
|                 | EM               | Intrusion response time             | null                  | null                             |
|                 | IM               | Recovery plan                       | 1                     | 1                                |
| Management      | CM               | Key equipment health index          | 1                     | 0.820                            |
|                 | EM               | Safety asset importance             | 0.642                 | 0.568                            |
|                 | IM               | Vulnerability prevention cost score | 0.699                 | 0.678                            |

In the management indicators, the characteristic indicators are expressed by the key equipment health index. It includes router health index and switch health index. Finally, the comprehensive score is obtained by analytic hierarchy process. Utility indicators are represented by security event management. The value of security event management is obtained by measuring the effectiveness of security event strategy and emergency plan. The impact class index is expressed by the cost of vulnerability prevention. The cost of vulnerability prevention includes the number of vulnerabilities, the level of vulnerabilities, and whether there are repair schemes for vulnerabilities.

Indicator values directly collected in the experimental process need to be undetectable in the advanced experimental process, which is expressed by null. See Table 3.

4.4. Experimental Result
The analytic hierarchy process is used to assign weights to the CM, EM, and IM index points under the four levels of protection, detection, response, and management. Calculate the network system security assessment score for each layer. Finally, the results of each layer are combined to arrive at the final cyber security assessment value. See Table 4. Cyber security Score.

Table 4. Cyber security Score

| Network Type       | Protection | Detection | Response | Management | Final score |
|--------------------|------------|-----------|----------|------------|-------------|
| Standard network   | 0.722      | 0.626     | 1        | 0.701      | 0.735       |
| Experimental network | 0.717   | 0.554     | 1        | 0.633      | 0.710       |

From this table, we can see that the network security score of each layer after DoS attack is lower than that of the network without DoS attack, which is consistent with the actual situation. It shows that the measurement framework of the index system proposed in this paper is reasonable. Although the framework of the index system is reasonable, there are still difficulties in the collection of indicators. In large complex networks, more indicators need to be collected in order to better reflect the network security status.
5. Conclusion
This paper proposes a PDRM model based on the PDR model and adds CM EM IM to the PDRM model. From the perspective of offensive and defensive confrontation, the dynamic evolution process of the network system is described by quantifiable indicators. This is innovative. After collecting the relevant indicator values, the security of the network system is scored by using the analytic hierarchy process. And the experimental results have obtained reasonable results. Explain the rationality of this framework.

But this framework also has shortcomings. In the face of complicated network environment, the collection of indicators is not comprehensive. Therefore, the evaluation results also have certain limitations. This is also a challenge in the current field of network security assessment. The collection of indicators and the quantification of indicators are all difficult. In addition, there is a certain correlation between indicators. Subsequent research can use machine learning to assign weights to a large number of network security metrics.

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

7. References
[1]. Stergiou T, Leeson M S and Green R. J 2004 An alternative architectural framework to the osi security model. J Computers & Security, 23(2), pp137-153.
[2]. Belalcazar A, Ron M , Diaz J and Molinari L 2017 Towards a Strategic Resilience of Applications through the NIST Cybersecurity Framework and the Strategic Alignment Model (SAM). International Conference on Information Systems & Computer Science. IEEE Computer Society.
[3]. Liu F and Liu M. 2014 American ficic framework and its influence analysis. J Information Security in China (12), PP109-112.
[4]. Ekelhart A , Fenz S and Goluch G 2007 Ontological mapping of common criteria’s security assurance requirements. New Approaches for Security, Privacy and Trust in Complex Environments. Springer US.
[5]. Zhang Y M, Huang R, Liu A C, Zhong S and Yu L 2017. Safety Protection Measures of Level 3 Information Security Protection Standard. Cyberspace security Technology and Application (6), PP16-17..
[6]. Yang X M 2010 Defense Architecture of Key Application Information System Based on PPDR Model. Computer and Applied Chemistry 27(8).
[7]. Yuan M X and Wang Z 2016 Research on security evaluation of hospital information system based on wpdrrc model. Electronic Design Engineering.
[8]. Zhang Y, Zhang Q, Wei W U and Shi Z 2018 Security analysis and evaluation of representational state transfer based on attack graph. J Journal of Computer Applications.
[9]. Christie R D and Talukdar S N 1988 Expert systems for on line security assessment-a preliminary design. IEEE Transactions on Power Systems, 3(2), pp654-659.
[10]. Frigault M, Wang L, Jajodia S, and Singhal A 2017 Measuring the Overall Cyberspace security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks. Cyberspace security Metrics.
[11]. Qin Z Q, Kai-Bin L I and Ming-Chu L I. 2010 Webpage security evaluation model based on pagerank and system calls. Journal of Chinese Computer Systems, 31(10), pp2068-2072.
[12]. Kim A, Kang H 2011 Determining Asset Criticality for Cyber Defense[J]. Determining Asset Criticality for Cyber Defense
[13]. Ye X and Li C 2013 The improved grey relation degree and its application in cyberspace security diagnosis. Control & Decision Conference.
[14]. Zhang K W 2013 Risk assessment of smart grid cyber security based on multi-level fuzzy comprehensive evaluation method. Advanced Materials Research, 605-607, pp2311-2317.
[15]. Ji X and Pattinson C 2010 AHP Implemented Security Assessment and Security Weight Verification. IEEE Second International Conference on Social Computing. (London: Chapman and Hall) chapter 6 pp173–214
[16]. Qazi S, Raad R, Mu Y and Susilo W 2018 Multirate delphi to secure multirate ad hoc networks against wormhole attacks. Journal of Information Security and Applications, 39, pp31-40.
[17]. Hatzivasilis G, Papaefstathiou I and Manifavas C 2016 Software security, privacy, and dependability: metrics and measurement. IEEE Software, 33(4), pp46-54.
[18]. Rahman, Mohammad Ashiqur, Al-Shaer, Elhab. A formal approach for network security management based on qualitative risk analysis. Proceedings of the 2013 IFIP/IEEE International Symposium on Integrated Network Management, p 244-251, 2013.
[19]. Doynikova, E and Kotenko I. 2017 CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection. In 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP) (pp. 346-353). IEEE.
[20]. Ghanshyam S. Bopche, Babu M. Mehtre 2017 Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks, Computers & Security, Volume 64, pp16-43, ISSN 0167-4048.
[21]. Simon Yusuf Enoch, Mengmeng Ge, Jin B. Hong, Hani Alzaid, Dong Seong Kim, A systematic evaluation of cybersecurity metrics for dynamic networks, Computer Networks, Volume 144, 2018, Pages 216-229, ISSN pp1389-1286.
[22]. Jin B. Hong, Simon Yusuf Enoch, Dong Seong Kim, Armstrong Nhlabatsi, Noora Fetais, Khaled M. Khan, Dynamic security metrics for measuring the effectiveness of moving target defense Techniques, Computers & Security, Volume 79, 2018, pp33-52, ISSN 0167-4048
[23]. Teresa Pereira and Henrique Santos. 2014 Security metrics to evaluate organizational IT security. In Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance (ICEGOV’14). ACM, New York, NY, USA, pp500-501.
[24]. Qazi S, Raad R, Mu Y and Susilo W 2018 Multirate delphi to secure multirate ad hoc networks against wormhole attacks. Journal of Information Security and Applications, 39, pp31-40.
[25]. A. Gharib, I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “An evaluation framework for intrusion detection dataset,” in 2016 International Conference on Information Science and Security (ICISS). IEEE, 2016, pp. 1–6
[26]. J. Mirkovic and P. Reiher, “A taxonomy of ddos attack and ddos defense mechanisms,” ACM Sigcomm Computer Communication Review, vol. 34, no. 2, pp. 39–53, 2004.