Quantifiable Network Security Measurement: A Study Based on an Index System

Guoquan Li[1], Yulong Fu[1](✉), Zheng Yan[1], and Weilin Hao[2]

[1] School of Cyber Engineering, Xidian University, Xi'an, China
ylfu@xidian.edu.cn

[2] School of Electronic Engineering and Computer Science, Peking University, Beijing, China

Abstract. Security Metrics help network administrators master the security status and strengthen security management for many years. Recently, with the usages of many new techniques and network structures, the cyber attacks become complex and the security measurement has received more and more attentions. However, existing methods usually focus on one aspect of security and the indicators used are usually difficult to quantify, which makes it difficult to understand network security status in some real circumstance. In this paper, we consider the network system security from the perspective of attack and defense and the changes of external security environment to propose a comprehensive and quantifiable index system for network security measurement. We illustrate the corresponding theories and the usages of each selected indicators and we also complete the real-time security measurement in various attacks and defenses by using NS3 simulator. The simulation results verify the correctness and rationality of the proposed Security Measurement Index System.

Keywords: Security metric · Index system · Attack and defense confrontation · NS3 simulation

1 Introduction

The rapid growth of information technology promoted the development and the quality of computer networks, and also bring cyber attacks to users. Increasing cyber threats and hacker activities made the network environment become serious and became the headache of modern networks system. In order to relieve user's safety anxiety and accelerate the development and use of modern network technologies, a security measurement to the network is necessary. However,

National Key R&D Program of China (grant 2016YFB0800700), NSFC (grants 61602359 and 11571281), Fundamental Research Funds for the Central Universities (JB150115) and the 111 project (grant B16037).

X. Chen et al. (Eds.): ML4CS 2019, LNCS 11806, pp. 47–62, 2019.
https://doi.org/10.1007/978-3-030-30619-9_5

existed rule-based or machine learning-based security measurement methods are passive, single-assist mitigations for specific security issues. These measures lack of systematic considerations, which may blindly add protective equipment, waste manpower and material resources, and can no longer meet the current network security needs [1]. In order to fully understand the network security status and effectively strengthen network security, network security metric has become a hot and difficult issue. Although some security metric standard have been established, many of them have some limitations and may lead to some issues.

Existed network security metric models, such as the National Institute of Standards and Technology (NIST) cyber security framework, the Common Criteria for Information Technology Security Assessment (CC), the Information Security Technology Framework (IATF) and the information security protection level (ISPL) are define the security measurement with standards or frameworks. These security standards or frameworks tend to focus on product or management, and indicators in them are not quantified. In addition, there are also some researchers conduct network risk assessments from the vulnerabilities [3]. Common methods include probability-based attack graph model, system evolution of Markov chain random representation, fault tree analysis and attack tree, etc. [4]. However, these existed methods only focus on the possible risks, they does not consider the changes of the network system's own detection and defense capability and the indicators used are usually difficult to quantify. In order to solve the problems mentioned above, in this paper, we propose a complete, dynamic, quantifiable and comparable index system for security measurement. Through the real-time measurement and calculation of security indicators, the dynamic changes of network status can be accurately described, and the internal causes of network status changes can be deeply reflected, so that security-enhanced decision support can be provided to security management.

The main contributions of this paper are listed as follows:

1. We propose a comprehensive, dynamic, quantifiable and comparable index system from the perspective of offense and defense for network security measurement.
2. We implement the multiple attack and defense modules in NS3 simulator.
3. We use the NS3 simulator to measure the network security status in real time, verify the rationality and correctness of the proposed index system.

The remainder of this article is organized as follows. Section 2 introduces the background knowledge and related work of security metric. A security index system is proposed and the weights were determined in Sect. 3. Section 4 completes the real-time measurement of the network status and verify the correctness and rationality of the index system based on NS3 simulator. Section 5 summarizes the whole article and points out the directions of future work.

2 Related Work

Security Measurement is important and many existed works has been done in the literature. Some authoritative and relatively new security standards, including Common Criteria for Information Technology Security Assessment (CC), Classified Protection of Information Security (CPIS), Network and Information Security Directive (NIS), National Institute of Standards and Technology (NIST) and Information Assurance Technical Framework (IATF) have defined their indicators for security evaluation. We strictly reviewed these indicators, and compare them against comprehensiveness, dynamics, quantification, objectivity, and comparability. The results of the comparison are shown in Table 1.

Table 1. Index system comparison

Standard	Comprehensiveness	Dynamics	Quantification	Objectivity	Comparability
CC	No	No	No	No	Yes
CPIS	Yes	No	Yes	No	Yes
NIS	Yes	Yes	No	No	Yes
NIST	Yes	Yes	No	No	Yes
IATF	Yes	Yes	No	No	Yes

Besides those published standards, private research on this problem are also contributed. In [6], the authors discuss the importance of network metric and believes that security metric should be characterized by certainty, simplicity, objectivity and repeatability. Then several commonly used metric method are introduced and the security metric work is introduced from the policy and economic aspects. However, this article only introduces the basic knowledge of network metric, and does not propose a specific metric scheme. Literature [7] proposes a hierarchical security threat metric model, including three levels of service, host and network, and quantifies the evolution of security risks of these levels based on IDS alarm and network bandwidth occupancy. The article proposes some threat risk calculation formulas, which can quantify the risk index of service, host and network in real time, and verify the correctness of risk index quantification through experiments. However, the article only considers the attack risks, and does not consider the changes in the network's own defense capabilities. In [8], the authors believe that the core of security metric is the result of an attacker using vulnerability to launch attacks and interact with defense. From the perspective of attack and defense confrontation, the metrics are divided into four categories: vulnerability indicator, defense indicator, attack indicator and status indicator. The index system proposed in the paper is relatively comprehensive, but just introduce the meaning of these indicators and lack quantitative calculation formulas.

Although the researches on security metric are plenty, but the existed results are single aspect, static and subjective, a comprehensiveness, dynamics and quantifiability security metric are always required.

3 Security Metric Index System

Building a quantifiable and relatively complete index system is the main purpose of our work. In order to solve the shortcomings of the existing index system, we propose a quantifiable, comprehensive, dynamic and universal index system from the perspective of offensive and defensive confrontation. As shown in Fig. 1, we consider network's own defense capability and threats caused by attack, vulnerability. In addition, the network performance anomaly index is proposed from the perspective of overall network communication performance. We describe the definition of all indicators in the proposed index system, and then the calculation and quantization formula of indicators will be given and the calculation results are normalized.

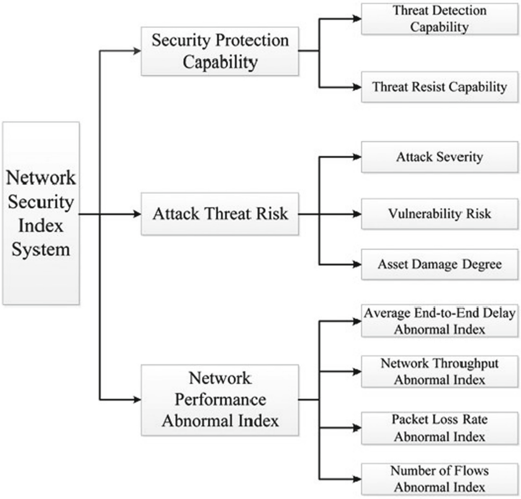
Network Security Index System
Security Protection Capability
Threat Detection Capability
Threat Resist Capability
Attack Threat Risk
Attack Severity
Vulnerability Risk
Asset Damage Degree
Network Performance Abnormal Index
Average End-to-End Delay Abnormal Index
Network Throughput Abnormal Index
Packet Loss Rate Abnormal Index
Number of Flows Abnormal Index

Fig. 1. Network security index system

3.1 Security Protection Capability

Threat Detection Capability. Threat Detection Capability (TDC) is a metric that measures the detection and monitoring efforts of devices such as IDS or monitoring audit system for cyber attack. Threat detection capability is related to threat detection intensity level (TDIL) and intrusion detection classification performance. These two indicators are described below.

Threat Detection Intensity Level. It describes the scope and effectiveness of attack detection by threat detection device. To best of our knowledge, mainstream attacks account for the majority of all attacks, such as DDoS, XSS, buffer overflow, etc. Therefore, successful detection of mainstream attacks contributes a lot to network security [9]. We use interval data to describe different levels of threat detection capability, as shown in Table 2.

Table 2. Hierarchical definition of threat detection intensity

Level	Capability	Threat detection intensity description
1	0	No threat detection device, no threats can be detected
2	0.3	Can only detect a few threats, the detection effect is poor
3	0.8	Can detect mainstream threats, the detection effect is good
4	1.0	Can detect most threats, the detection effect is very good

Intrusion Detection Classification Index. IDS is a network behavior classifier and its role is to identify threat behaviors [10]. Therefore, we can use traditional classification evaluation indicators in statistical learning to measure intrusion detection capability. The commonly used classification performance indicators include recall, precision and etc. Precision (P) indicates the correct proportion of the prediction in the positive samples, and recall (R) indicates the proportion of the true positive samples that are predicted as positive samples. P and R reflect the classification performance from different aspects, but sometimes there are conflicts [11]. To deal with this problem, we use F-Measure (F1) as the intrusion detection performance indicator. The formula for F1 is as follows.

$$F1 = \frac{2 * P * R}{P + R} \tag{1}$$

Threat Detection Capability Calculation. The value of TDC is equal to the product of TDL and F1. The calculation formula is as follows.

$$TDC = TDL * F1 \tag{2}$$

Where F1 is calculated based on the historical detection data of IDS. The TDC has no dimension and the value ranges from 0 to 1, so it is not necessary to normalize.

Threat Resist Capability. Threat Resist Capability (TRC) is a measure of the ability to block or mitigate threats. It can defend against cyber attacks, and prevent malicious behavior detected in time to ensure the network security. The devices with threat resistance mainly include firewall, anti-virus software, intrusion prevention system, and active defense technology [12]. TRC is related to the threat resist intensity level and the blocking ratio. And these indicators are described below.

Threat Resist Intensity Level. TRL measures the range and effect of security protection and preventing threat. To best of our knowledge, mainstream attacks occupy a large proportion, so the ability to defend against mainstream attacks is important for network defense capabilities. We use interval data to describe the ability of different threat level, and Table 3 gives the definition of threat strength level.

Table 3. Hierarchical definition of threat resist intensity

Level	Capability	Threat resist intensity description
1	0	No security measures to reach and prevent threats
2	0.3	Can only defend against few threats, the protection effect is poor
3	0.8	Can defend against mainstream threats, the protection effect is good
4	1.0	Can protect most threats, the protection effect is very good

Blocking Ratio. Blocking ratio (BR) is the ratio of the number of successful defending attacks to the number of hosts that are attacked. It can measure the efficiency of defense equipment. The formula is as follows.

$$BR = \sum_{n}^{i=1} \frac{Blk(i)}{En(n)} * 100\%, Blk(i) \in [0, 1] \tag{3}$$

Where n is the number of network device, Blk(i) is the degree to which the i-th device successfully blocked the attack, ranging from 0 to 1, and En(n) indicates the number of devices being attacked.

Threat Resist Capability Calculation. The value of TRC is equal to the product of BR and TRL. The calculation formula is as follows.

$$TRC = TRL * (BR_b * m_{br1} + BR_t * m_{br2}), m_{br1} + m_{br2} = 1 \tag{4}$$

Where BR_b is calculated according to historical data of the defense device, and BR_t is calculated in the current security metric period T. In order to prevent the security metric calculation error caused by the zero-day attack, the value of BR is the weighted sum of BR_b and BR_t. For real-time measurement of network status, we need to pay more attention to the current measurement period, so that $m_{br1} = 0.2$ and $m_{br2} = 0.8$. TRC has no dimension and the range of values is between 0 and 1, so it is not necessary to normalize.

3.2 Attack Threat Risk

Attack Severity. The Attack Severity (AS) measures the extent to which an attack is harmful to network. Traditional cyber risks involve three elements, namely threat, asset, and vulnerability [13]. The attack severity defined here fuse threat and asset, which can more comprehensively and accurately measure the degree of harm caused by attack to network resources. The calculation of the severity of the attack involves the attack severity level and the target asset importance level (TAIL). Their definitions are described below.

Attack Severity Level. Attack Severity Level (ASL) ranks the severity of an attack and visually shows the difference between different attacks. We determine the severity of the attack according to the attack classification and prioritization in the snort user manual. The snort manual divides the attack into three levels, namely high, medium, and low. In this paper, we use 3, 2, 1 to represent these three levels. The snort user manual already contains most of the attacks. For some attacks that are not involved, we give them the same severity level as the same type of attack.

Target Asset Importance Level. Successful implementation of a cyber attack must be done through the target of the attack. Different device or service may become target of intruder, such as router, firewall, and user data. The target asset importance level (TAIL) is determined by the target type. We classify TAIL into there levels, namely high, medium and low, represented by 3, 2 and 1.

Attack Severity Calculation. The severity of the attack is related to the type and the number of attack, and the importance of the target assets. The calculation formula is as follows.

$$AS = \sum_{m}^{i=1} (1 + k_i * cf_i) * r * 10^{ASL_i} * N_i * TAIL_i \tag{5}$$

Where m is the number of attack category, ASL_i is the severity level of the i-th attack, N_i is the number of occurrences of the i-th attack, and $TAIL_i$ is the asset importance level of the i-th attack's target. We use 10^{ASL_i} instead of ASL_i according to the literature [7]. In order to more accurately reflect the impact of attack and defense interaction on the network, we add the resist factor r to indicate that attacks are successfully resisted by defense. The value of r is 0.1 indicating that the attack is only 10% of the original when the attack is resisted. We divide attack into independent attack and coordinated attack, and their severity calculation methods are slightly different. Implementing an coordinated attack scenario requires multiple attack steps in sequence. And the attack that occurs later is more threatening, so we propose the attack correlation factor cf to more accurately describe the impact of attack. k_i is the number of attack steps before the i-th attack, and cf_i is the attack-related factor, indicating the degree of the collaborative attack threat increasing, the value of cf_i is 0.1.

Max-min and z-score normalization are not applicable because it is difficult to determine the maximum number of attacks based on historical statistics. To solve this problem, we choose the negative exponential function e^{-a*x} as the mapping function. It maps the indicator to between 0, 1 and is very close to the max-min mapping. Based on experience and historical data analysis, we take a equal to 0.005, a can be adjusted according to the actual size and status of network, so the formula of AS is normalized as follows.

$$AS' = e^{-a*AS} \tag{6}$$

Vulnerability Risk. The execution of the attack is inseparable from the exploitation of the vulnerability. These vulnerabilities and efforts to compromise these vulnerabilities are the most commonly collected data for understanding network security. Many researchers have conducted network risk assessment and analysis from the perspective of vulnerability analysis and have achieved many results. The risk caused by the vulnerability is a potential energy that can affect the network. Therefore, based on previous vulnerability risk assessment, we propose vulnerability risk (VR) indicator. VR is related to the vulnerability severity score and TAIL. The latter has been quantitatively analyzed in the previous section. Below we describe the vulnerability severity score.

Vulnerability Severity Score. CVSS is often used to measure the severity of vulnerabilities and help people determine their priority. It is mainly based on measurements in different dimensions, namely basic, temporal, and environmental measure. In CVSS, the vulnerability score is between 0 and 10 and the high score represents a very serious risk. Our vulnerability severity score (VSS) is based on the CVSS.

Vulnerability Risk Calculation. The value of VR is the product of VSS and TAIL. The calculation formula is as follows.

$$VR = \sum_{n}^{i=1} VSS_i * TAIL_i \tag{7}$$

Where n is the number of vulnerabilities, VSSi is the severity score of vulnerability i, and $TAIL_i$ is the asset importance of the device with vulnerabilities i. We use the negative exponential function e^{-b*x} as a mapping function to normalize the vulnerability risk. Based on the analysis of historical risk data, we take c equal to 0.005. The normalized formula for VR is as follows.

$$VR' = e^{-b*VR} \tag{8}$$

Asset Damage Degree. Intruders break the network and cause damages to the network, such as server crash, database leak, and router outage. Network damage directly affects network security and we propose the asset damage degree (ADD) to measure the degree of asset damage. The value of ADD is determined by TAIL, and the calculation formula is as follows.

$$ADD = \sum_{n}^{i=1} TAIL_i \tag{9}$$

Where i represents the i-th damaged target, and $TAIL_i$ is the severity of the damaged target. We use the exponential function e^{-c*x} as a mapping function to normalize. Based on the analysis of historical NDD data, we take c equal to 0.2. The normalization formula is as follows.

$$ADD' = e^{-c*ADD} \tag{10}$$

Network Performance Anomaly Index. In order to measure the network security status more accurately, we provide an overall research perspective by detecting abnormal changes in network communication performance. When applying the metric system to the actual network, we may encounter some unknown attacks. The metrics of attack and defense indicators will be deviated, and the network performance metric can slightly alleviate this deviation. We propose 4 indicators, including average end-to-end delay abnormal index (AEEDAI), network throughput abnormal index (NTPAI), packet loss rate abnormal index (PLRAI) and number of flows abnormal index (NFAI), which are described in detail below.

Average End-to-End Delay Abnormal Index. End-to-end delay refers to the time it takes for a packet to be sent from being received. Some attacks can be reflected in end-to-end delay changes, such as the router's routing table failure and server resource exhaustion. Average End-to-End Delay (AEED) refers to the average of all communication link delays across the network. AEEDAI indicates the extent to which AEED deviates from the normal range. The calculation formula is as follows.

$$\begin{aligned} AEEDAI &= \frac{\|AEED - AEED_{norm}\|}{AEED_{max} - AEED_{norm}} \\ \|AEED - AEED_{norm}\| &= \begin{cases} AEED - AEED_{norm}, other \\ 0, AEED - AEED_{norm} < 0 \end{cases} \end{aligned} \tag{11}$$

Where $AEED_{norm}$ is the average threshold of AEED, and $AEED_{max}$ is the maximum threshold. We normalize AEEDAI using the exponential function e^{-d*x} as a mapping function. Based on the historical AEED data, we take the value of d as 0.005. The normalization formula for AEEDAI is as follows.

$$AEED' = e^{-d*AEDD} \tag{12}$$

Network Throughput Abnormal Index. Network throughput represents the actual maximum data transmission rate, mainly related to network congestion, storage mechanism and processor performance. The Network Throughput Abnormal Index (NTPAI) indicates the extent to which the network throughput deviates from the normal range. The calculation formula is as follows.

$$NTPAI = \frac{\|NTP_{norm} - NTP\|}{NTP_{norm} - NTP_{min}} \tag{13}$$

Where NTP_{norm} is the maximum throughput of the network, and NTP_{min} is the minimum threshold of NTP. We use max-min method to normalize NTPAI as shown below.

$$NTPAI' = \frac{NTPAI_{max} - NTPAI}{NTPAI_{max} - NTPAI_{min}} \tag{14}$$

Packet Loss Rate Abnormal Index. The packet loss rate (PLR) refers to the ratio of lost data packets to transmitted data packets. Many attacks can increase the packet loss rate, such as routing attacks and virus attacks. PLRAI is an indicator that we propose to measure the extent to which PLR deviates from the normal range. The calculation formula is as follows.

$$PLRAI = \frac{PLR - PLR_{norm}}{PLR_{max} - PLR_{norm}} \tag{15}$$

Where PLR_{norm} is the normal threshold of PLR, and PLR_{max} is the maximum threshold. We normalize PLRAI using the min-man rule as shown in Eq. 16.

$$PLRAI' = \frac{PLRAI_{max} - PLRAI}{PLRAI_{max} - PLRAI_{min}} \tag{16}$$

Number of Flows Abnormal Index. A flow is a classification of packet characteristic. In general, source destination IP, source destination port and protocol with the same data packet form a stream. The number of flow will fall within a normal range. If the number of flow changes greatly, it indicates that the network status changes. Therefore, we propose NFAI to measure the extent to which the number of flow deviates from the normal range. The calculation formula is as follows.

$$NFAI = \frac{\|NF - NF_{norm}\|}{NF_{max} - NF_{norm}} \tag{17}$$

Where NF_{norm} is the average number of flow, and NF_{max} is the maximum number of flow. We use the exponential function e^{-g*x} as a mapping function to normalize NFAI. Based on the historical data, we take g equal to 0.005. The normalized formula is as follows.

$$NFAI' = e^{-g*NFAI} \tag{18}$$

We propose four indicators based on commonly used network performance parameters to describe the degree of network performance anomalies. And these indicators can mitigate attack and defense metric errors caused by zero-day attacks. The threshold of the network performance indicators in this paper is determined by 30 experimental statistics.

Indicator Weight Calculating. There are many methods for determining indicator weights, such as Delphi, AHP, principal component analysis and entropy weight. The first two are subjective, but can can rely on expert experience. The latter two are relatively objective, but they are not applicable here, because different network configurations and changing network environments can result in unreliable statistics. In this paper, we use the AHP method to calculate the weight of all indicators.

4 Security Metric Simulation Implementation

In order to verify the rationality and correctness of the proposed index system, we use the NS3 simulator to achieve real-time measurement of network status. First, we need to build an enterprise network and configure network resources and vulnerability information. Then implement different attack and defense modules and build different network scenarios. Finally, the security indicators are collected and calculated in different scenarios, and the real-time network status value is obtained, and the rationality of the index system is judged according to the actual network status.

4.1 Build Network Scenario

Simulation Environment. We use the simulator NS3.25 to build the enterprise network. We use 101 nodes to simulate the equipment of the intranet, and 125 nodes are used to simulate the external network. Different subnets are connected through routers. The simulated network topology is shown in Fig. 2. We configure the resources in the enterprise network and list the vulnerability information as shown in Table 4.

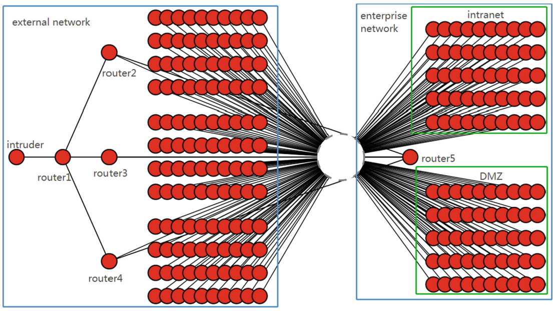

Fig. 2. Simulation network topology

4.2 Offense and Defense Module

In order to measure the impact of offense and defense on network, we add different strengths of attack and defense to the network scenarios in NS3. As NS3 simulator does not involve any security function, the implementation of the attack module is to use the attack principle to embed the attack function code in NS3. NS3 is more flexible than the actual network attack tools, and there is no limitation of system permission [14], so we can modify the kernel source code as needed. We implemented the attacks listed in Table 5, and also implemented different defense modules in NS3 to defense the attacks, including IDS and firewall, etc.

Table 4. Implemented defense module

Asset	TAIL	Quantity	System type	Vulnerability number	CVSS score
Router	3	1	MikroTik	CVE-2018-10070	7.8/10
switcher	3	2	Cisco IOS XE	CVE-2018-0165	6.1/10
				CVE-2018-0090	5.0/10
Database server	2	4	Windows	CVE-2018-2775	4.0/10
				CVE-2018-2769	4.0/10
Web server	2	1	Linux	CVE-2005-1110	7.5/10
Mail server	2	1	Windows	CVE-2004-2168	5.0/10
TFTP server	2	1	Windows	CVE-2001-1097	5.0/10
User host	1	10	Windows	CVE-2011-0514	5.0/10
User host	1	35	Windows	CVE-2013-1451	4.0/10
User host	1	6	Linux	CVE-2017-8779	7.8/10
User host	1	40	Linux	CVE-2008-5183	4.3/10

Table 5. Implemented attack module

Attack type	Dependent protocol
TCP-SYN, UDP, ICMP flood attack	TCP, UDP, ICMP
TCP-SYN, UDP port scan	TCP, UDP
IP scanning	ICMP
TCP-SYN, UDP-Echo, ICMP-Echo reflection amplification attack	TCP, UDP, ICMP
Botnet	Irc
IP spoofing	IP
Blackhole attack	AODV
Wormhole attack	AODV

4.3 Security Metirc Experiment Analysis

We designed two sets of experiments to analyze the network state changes in attack and defense confrontation. The attack strength level in the experiment refers to the snort user manual [15], and the defense strength level is determined by the number of defense device. Table 6 lists the attack severity levels and attack targets. Table 7 shows the defense equipment and defense strength. The security metric experiment is detailed below.

The Impact of Attack on Network Security. In order to measure the impact of attacks on network security, we need to fix the defense strength and then adjust the different attack strength. We first determined that the defense device is CRT-RS-IDS, blacklist and ACL, and then set up four different attacks. Table 8 lists five different offensive and defensive scenarios. "/" means no attacks occur.

Figure 3 show the changes in comprehensive indicators. In subgraph 1, we can find that the network status value exceeds 0.8 when the attack did not occur because the strength level of the defense is 3. When an attack occurs, the security status values in scenario 1 and 3 are drastically reduced because the protection

Table 6. Attack information used in the experiment

Attack type	Severity level	Attack target
IP spoofing	1	Combined with DDoS attack
UDP DDoS	3	TFTP server
UDP DoS	2	TFTP server
UDP port scanning	1	DMZ area server
TCP-SYN DoS	2	Mail server
IP scanning	1	Enterprise network equipment
TCP-SYN port scanning	1	DMZ area server

Table 7. Defense strength information used in the experiment

Defense	Defense strength level	Threat detection intensity level	F-measure
CRT-RS-IDS, blacklist, ACL	3	3	0.99
CRT-RS-IDS, BF-ICMP-DEFEND-DDoS, blacklist, ACL	3	3	0.99
CRT-RS-IDS, blacklist, ACL, IP-MAC binding	3	3	0.99
CRT-RS-IDS, BF-ICMP-DEFEND-DDoS	3	3	0.99
CRT-RS-IDS, blacklist	2	3	0.99

device cannot defend against DDoS or DoS attacks. The attacks in scenario 2 and 4 can be detected by CRT-RS-IDS and blocked by blacklist or ACL, so the security status value is slightly reduced. Subgraph 2 shows the impact of the attack on security capabilities. When no attack occurs, multiple defense devices make the network highly resistant. If the attack breaks through the defense, such as scenario 1 and 3, then the network will be damaged and security protection ability will decline. If the attack is successfully defended, the security protection capability is basically unaffected. Subgraph 3 shows the impact of an attack on the attack threat capability. The attack threat capability is less than 1 when no attack occurs, because the vulnerabilities cause the network to have a threat risk. We can find that the attack strength is directly proportional to the attack threat

Table 8. Implemented defense module

Defense	0–20 s	20–40 s	40–60 s	60–80 s	80–100 s
1	/	/	IP spoofing, UDP DDoS(A1)	/	/
2	/	/	UDP DDoS(A2)	/	/
3	/	/	IP spoofing, UDP DoS(A3)	/	/
4	/	/	UDP port scanning(A4)	/	/
5	/	/	/	/	/

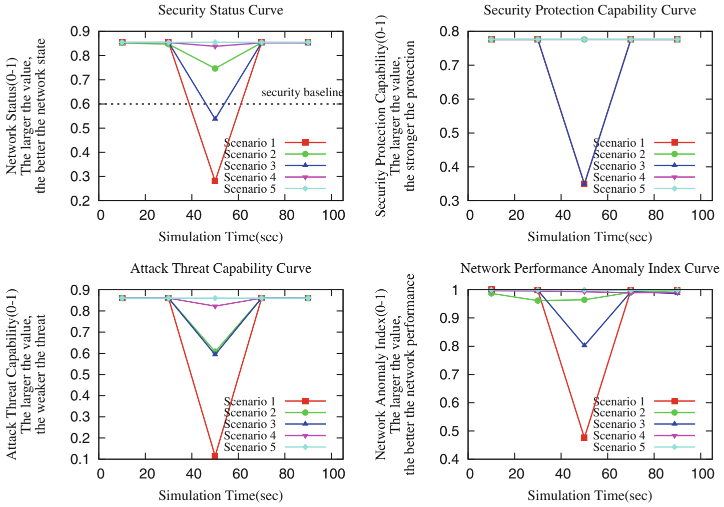

Fig. 3. The impact of attacks on network comprehensive indicators

capability from scenario 1, 2, 3 and 4. Subgraph 4 depicts the impact of attacks on network performance. When no attack occurs, the network performance anomaly index is very low, so the network communication performance is good. When an attack occurs, the attack that breaks through the defense has a large impact on the network performance, such as scenario 1 and 3, because the large amount of data generated in a short time causes the communication link and bandwidth to be occupied, resulting in an increase in network delay and PLR. When the attack is successfully blocked by the defense, the network communication performance is almost unaffected. In general, the measurement results can accurately reflect the real-time impact of different attacks on network status.

The Impact of Defense on Network Security. Figure 4 describes the impact of different defense strengths on comprehensive indicators. In subgraph 1, the network status value increases as the security level increases without attack. When there is no protection, such as scenario 5, the network security status is lower than the security baseline due to the risk of vulnerabilities. When an attack occurs, attacks can be successfully blocked by BF-ICMP-DEFEND-DDoS in scenarios 1 and 3, so network status value is not greatly affected. In other cases, the network is not effective against DDoS attacks with IP spoofing, and the network status value is below the security baseline. From subgraph 2, we can find that the security protection capability is directly related to the security defense strength. If the network defense can defend against the attack, the defense ability will not be affected, otherwise it will be seriously degraded, such as scenario 2 and scenario 4. In scenario 5, when there is no defense, the value of security protection capability is zero. Subgraph 3 shows that the attack threat capability depends not only on the strength of the attack, but also on the outcome of the attack and

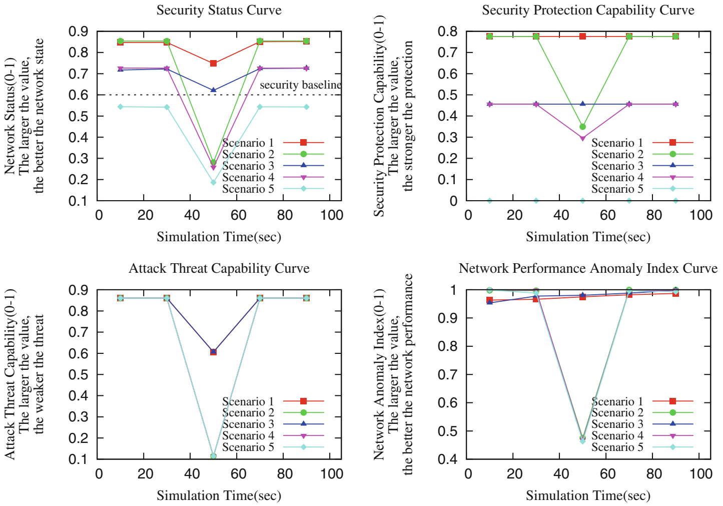

Fig. 4. The impact of defense on network comprehensive indicators

defense interaction. Subgraph 4 shows the impact of defense strength on network performance. Whether network performance is seriously affected depends on whether the current attack breaks through the defense, such as scenario 2 and 3. In general, the measurement results can accurately reflect the real-time impact process of different defenses on network status.

Combining the above analysis to compare the real state of the network with the values of the various comprehensive indicators, the accuracy and rationality of the indicator system can be verified.

5 Conclusion and Future Works

This paper describes the importance and necessity of security metric, and points out the deficiencies of metrics by analyzing and comparing existing security standards. In order to solve the problem that the existing index system cannot be quantified, we propose a quantifiable, comprehensive, dynamic and comparable network security index system through the perspective of attack and defense confrontation and calculate the index weight through AHP. The index system considers both the threat brought by the attack and the defense capability of the network itself. AHP can use the data collected in real time to ensure the reliability and accuracy of the measurement results, and reduce the computational difficulty and complexity. We also used NS3 simulator to test the proposed methods, the simulation results show the quantitability and dynamics of the indicator system, but also verify that the index system is accurate and comprehensive.

In the future, we need to take a more objective and appropriate weight calculation method to measure the network security status more accurately. More types of attacks, such as XSS, SQL injection and buffer overflows, and other types of network metrics, such as adhoc, should also be studied in our future work.

References

1. Hayden, L.: IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw Hill, New York (2010)
2. Ahmed, M.S., AI-Shaer, E., Khan, L.: A novel quantitative approach for measuring network security. In: The 27th IEEE Conference on Computer Communications, pp. 1957–1965. IEEE Communication Security, Phoenix (2008)
3. AI-Shaer, E., Khan, L., Ahmed, M.S.: A comprehensive objective network security metric framework for proactive security configuration. In: The 4th Cyber Security and Information Intelligence Research Workshop, Association for Computing Machinery, New York (2008). https://doi.org/10.1145/1413140.1413189
4. Liu, G., Yan, Z., Pedryczc, W.: Data collection for attack detection and security measurement in mobile Ad Hoc networks: a survey. J. Netw. Comput. Appl. **105**, 105–122 (2018)
5. Li, G.Q., Yan, Z., Fu, Y.L.: Data fusion for network intrusion detection: a review. Secur. Commun. Netw. **2018**, 1–16 (2018)
6. Atzeni, A., Lioy, A.: Why to adopt a security metric? a brief survey. In: Gollmann, D., Massacci, F., Yautsiukhin, A. (eds.) Quality of Protection. ADIS, vol. 23. Springer, Boston (2006)
7. Chen, X.Z., Zheng, Q.H., Guan, X.H.: Quantitative hierarchical threat evaluation model for network security. J. Softw. **17**(4), 885–897 (2006)
8. Pendleton, M., Garcia-lebron, R., Cho, J.H.: A survey on systems security metrics. ACM Comput. Surv. **49**(4), 62–96 (2016)
9. Jing, X.Y., Yan, Z., Pedryczc, W.: Security data collection and data analytics in the internet: a survey. IEEE Commun. Surv. Tutorials **21**(1), 586–618 (2018)
10. Lin, H.Q., Yan, Z., Zhang, L.: A survey on network security-related data collection technologies 2018, p. 1 (2018)
11. Jing, X.Y., Yan, Z., Pedrycz, W.: Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch (2018)
12. Hong, J.B., Yusuf, E.S., Seong, K.D.: Dynamic security metrics for measuring the effectiveness of moving target defense techniques. Comput. Secur. **79**, 33–52 (2018)
13. Abraham, S., Nair, S.: A stochastic model for security quantification using absorbing Markov chains. J. Commun. **9**, 899–907 (2014)
14. Li, G.Q., Yan, Z., Fu, Y.L.: A study and simulation research of blackhole attack on mobile AdHoc network. In: 2018 IEEE Conference on Communications and Network Security, pp. 1–6. IEEE Communication Security, Phoenix (2018)
15. Snort users manual. http://manual-snort-org.s3-website-us-east-1.amazonaws.com/snort_manual.html. Accessed 2018