Hindawi
Security and Communication Networks
Volume 2020, Article ID 6679304, 11 pages
https://doi.org/10.1155/2020/6679304

Research Article

Defending Application Layer DDoS Attacks via Multidimensional Parallelotope

Xiaolin Zhao,[1] **Hui Peng**,[1] **Xiang Li**,[2] **Yue Li**,[1] **Jingfeng Xue**,[1] **Yaoyuan Liang**,[1] **and Mingzhe Pei**[1]

[1]*Beijing Institute of Technology, Beijing 100081, China*
[2]*National Key Laboratory of Science and Technology on Information System Security, Beijing 100101, China*

Correspondence should be addressed to Xiang Li; lixiangxts@163.com and Jingfeng Xue; xuejf@bit.edu.cn

Received 31 October 2020; Revised 17 November 2020; Accepted 18 December 2020; Published 30 December 2020

Academic Editor: Zhe-Li Liu

The Internet is more and more integrated into people's life; because of the complexity and fragility of the network environment, network attack presents a more and more serious trend. Application Layer DDoS (AL-DDoS) attack is the most complex form of DDoS attack, which is hindering the availability for the legitimate users by taking up a large number of requests of web server. The paper introduced the concept of behavior utility to portray the network. The concept of attack and defense utility was defined by a specific property which was the manifestation of the network risk after the offset of attack and defense. In the utility model, traffic metrics were mapped to the multidimensional parallelotope in the Euclidean space to express as a diagonal matrix. To determine the threshold status, the defense strategies of load balancing and limiting the maximum number of connections were used with different attack scales. Finally, the attack and defense utility value was calculated to evaluate the network risk level. The proposed method can master the capacity of network system against each attack means and the defense capability of network system. Its availability and accuracy are verified by comparing with the relevant works.

1. Introduction

With the rapid development of network technology, the field of network security is facing hacker attacks. The intensity of attacks is gradually increasing, and illegal attackers achieve improper goals. DDoS attacks are the main means. AL-DDoS attacks are different from traditional network layer DDoS attacks. It mainly uses existing protocol loopholes, such as HTTP and SMTP, and consumes existing network resources, so that the target server cannot provide conventional services. The intensity and accuracy of this attack are higher, and the threat to security is also greater. The number of attackers and the required attack traffic are much lower than traditional AL-DDoS attacks, which also means that AL-DDoS attacks are easier to launch, and attackers can accurately attack specific applications, so the attack threat is great.

The measurement of network system security by most of today's methods cannot reach the stage of quantitative calculation. Most security measurement methods rely on a certain technology while relying on the human experience of experts to measure whether it is safe. These methods are not accurate and objective enough, so people are always looking for a method that can quantitatively, dynamically, and objectively measure network security. Although the network is static, it is always changing. In order to measure attacks more accurately, a network security measurement method that can dynamically describe and warn attacks is needed. Boyer et al. [1] propose a network security evaluation framework based on D-S evidence theory, but this method has some problems such as large calculation. Ramaki et al. [2] propose a network security risk assessment method based on Bayesian network. Although this method has a strong capacity to process a large amount of data, it is inevitably affected by some subjective factors, so the method must be properly trained to obtain relevant parameter. In the paper of Mukherjee et al. [3], a new security metric based on attack graph, namely, attack difficulty, has been proposed

which includes the position factor. Wen et al. [4] propose a network security situation prediction method based on the hidden Markov model. The change rules and trend changes were analyzed by describing the dependence of security conditions in different periods. Wang et al. [5] propose an improved base metric algorithm based on dependency relationship graph and CVSS, aiming at the problem that the existing network security measurement based on CVSS could not accurately measure the probability and the impact of network attack at the same time.

In order to find a way that can dynamically measure network security and does not rely on expert experience, this paper attempts to find performance metrics that can describe AL-DDoS attacks. This paper analyzes the principles of attack and defense types, summarizes the characteristics of attack and defense targets, and proposes metrics for measurement. In order to evaluate the impact of AL-DDoS attacks, the parameters and calculation methods used in various technologies are analyzed to find better performance metrics to describe the impact of the attack. The main contributions are as follows:

(1) This paper puts forward the definition of AL-DDoS attack and defense utility combined with the definition of related concepts from the perspective of sociology and network. It is the first time that the concept of utility combines with attack and defense to measure network security.

(2) This paper selects 6 metrics and conducts a large number of simulation experiments combining type and intensity changes. The selected metrics can be used to do various experiments with different attack and defense effect.

(3) This paper proposes a calculation model that uses the concept of hyperparallel to construct multidimensional space for utility calculation. The model can accurately represent the impact of the attack and quantitatively determine the impact value of the attack and defense utility. This paper verifies the credibility and accuracy of the calculation model.

2. Related Research

2.1. DDOS Attack and Detection Technology. DDoS attacks evolved from DoS attacks and are divided into network layer DDoS attacks and AL-DDoS attacks. The traditional network layer DDoS attack means that hackers invade and control a large number of puppet machines through various loopholes and then use puppet machines to attack the target server. AL-DDoS attack refers to the attacker sending a large number of requests from the victim computer to the database to disable the server [6]. AL-DDoS attacks are usually divided into two types: flooding attacks and slow attacks [7].

Currently, DDoS attacks occur frequently, so it is necessary to detect attacks in time. AL-DDoS attacks generate a large amount of request data in a short period of time. This attack method is similar to the behavior of a large number of users suddenly and normally accessing. Therefore, this condition needs to be distinguished from normal access by a large number of users. The purpose of the AL-DDoS attack is to make the applications on the server unable to provide normal services to legitimate users and deny their access [8]. Intrusion Detection System (IDS) is one of the most effective detection and defense mechanisms for DDoS attacks [9]. IDS is an application-type system that monitors suspicious events in the network, generates reports, and forwards them to administrators for action. There are many traditional IDS/IPS technologies, such as feature-based detection methods and abnormal behavior-based detection methods [10].

2.2. AL-DDOS Attack Assessment Method. Among current researches on DDoS attacks, most of them are based on the network layer, but there are few researches on the impact of AL-DDoS attacks [11]. The paper of Pallavi et al. [12] finds that over 45% of these applications do not implement measures to protect BLE data, and that cryptography is sometimes applied incorrectly in those that do. Application layer data is extremely vulnerable. The paper of Wei Zhou et al. [13] finds that smart home devices are vulnerable to attacks by network traffic interception. While bringing unprecedented convenience and accessibility, they also introduce various security hazards to users.

Kumar et al. [14] propose a method to measure the impact of AL-DDoS attacks on web server performance. The authors modify the Webtraf module in NS-2 to generate attack traffic to simulate legitimate user behavior. They analyze the impact of different server processing strategies and queue lengths on the attack. In this method, Wang et al. [15] have developed a prototype of SkyShield and evaluated its effectiveness using real attack data collected from large web clusters. Experimental results show that SkyShield can quickly reduce malicious requests while having limited impact on legitimate users. In the method of Sahoo et al. [16], an information distance-based flow discriminator framework has been discussed, which can discriminate DDoS traffic during flash events in a software-defined network (SDN) environment, that is, legitimate traffic that looks similar. The information distance metric is used to describe the variations of traffic behavior of such events. The simulation results show that the information distance metric can effectively identify the DDoS traffic [17]. The paper of Jiahao Cao et al. [18] systematically studies the impacts of attack on various network applications in a real SDN test bed. Experiments show that the attack significantly degrades the performance of existing network applications and causes serious network anomalies, e.g., routing black hole, flow table resetting, and even network-wide DoS.

Procopiou et al. [19] propose ForChaos, a lightweight detection algorithm for IoT devices, which is based on forecasting and chaos theory to identify flooding and DDoS attacks. In NS-3, the detection algorithm is evaluated through a series of experiments in flooding and slow-rate DDoS attacks. Sardana et al. [20] propose an integrated honeypot framework for active detection, characterization, and redirection of DDoS attacks at the ISP level. The authors evaluate the impact of DDoS flood attack on effective throughput, average transaction failure interval time, and

average response time as parameters under different operation modes and use the framework to defend against high-rate DDoS attack by referring to impact value.

Most of the relevant studies rely on subjective empirical judgment and lack of objectivity and use fewer metrics, so the conclusions may be biased. In this paper, a measurement method of AL-DDoS attack and defense utility is proposed to calculate the effects of AL-DDoS attack. By comparing the simulation experiment data with the related technical data, the effectiveness, objectivity, and accuracy of the method are verified.

3. AL-DDOS Attack and Defense Utility and Calculation Model

Attack and defense behaviors are defined in the network: from the perspective of network objects and their interconnection, attack or defense behavior refers to a series of state changes caused by attacks or defense methods in the network. The network status change caused by the attack process can be described as an attack behavior. The weakening of the attack effect caused by the defensive means leading to the change of the network state can be defined as defensive behavior. The attack behavior is composed of five basic elements, among which the behavior subject is the attack initiator, that is, the hacker. The object of behavior is the target of attack, namely, the network system. The behavior environment is the network environment where the attack process is located. The behavior means are the resources used in the network when the attack is launched. The behavior result is the agreement degree between the expected attack result and the actual attack result during the attack. By analogy, the basic elements of defensive behavior are as follows. The behavior subject is the defensive measure. The behavior object is the target of defense, that is, the source of attack. The behavior environment refers to the network environment in the process of defense. The behavior means is the resource in the network when the defense measures are launched. The behavior result is the agreement degree between the expected defense result and the actual defense result after the attack process [21].

Based on the analysis of sociology and network behavior, attack and defense behavior have the following features: (1) Purpose: the occurrence of attack and defense behavior must be accompanied by purpose, in which the attack behavior will not affect the network for no reason, and the defense behavior will not work without being attacked. (2) Persistence: attack and defense behaviors each point to their own goals. Generally, attack and defense behavior will not terminate until the goal is completed. When attack and defense behaviors are in effect, they may change their behaviors due to the difficulty of achieving the goal, but attack and defense behaviors are persistent. (3) Variability: the mode of attack and defense behaviors may be gradually optimized with the continuous update of technology, and new technology may be used to achieve their goals.

Attack and defense behavior impact refers to the network status change caused by attack and defense behavior through a series of operations. Before a multitude of attack and defense behaviors function to the network system, the network status value needs to be set to S. The network status value after attack and defense behavior is set to S', and the status value rate is used to calculate comprehensive attack and defense forces $F_{AD} = S'/S$. Attack and defense behavior is shown in Figure 1.

As is shown in Figure 2, the essence of network system security is a balance between attack and defense. In a specific network scene, network attack and defense are regarded as behaviors, which can establish network system security judgments and identification of the behavior utility standards.

The definition of attack and defense utility is as follows: Suppose the attack function is A, the defense function is D, and the combined attack and defense force is $F_{AD} = A - D$ (if F is greater than 0, it indicates that the defense function cannot resist the attack; if F is less than or equal to 0, the defense function can resist the current scale of attack).

After calculating the attack and defense force, the attack and defense utility is the sum of the effects caused by the attack and defense forces, which is used to represent the comprehensive effect of the network system after the combination of attack and defense in the process [22]. The attack and defense utility is shown in Figure 3.

By calculating the utility value of the attack and defense behavior of the network system, the effects of various AL-DDoS attack and defense methods can be accurately and objectively obtained. The calculated value of attack and defense utility can provide a more complete and objective evaluation standard for researchers in network security measurement field. The mathematical methods of evaluating attack and defense behavior are more objective and easy to compare with other methods.

3.1. Attack and Defense Utility Calculation Model. When an attack occurs, the relevant metric status of the network will change. No single network metric can completely represent an attack. Therefore, the network status can be obtained by combining the metric values according to the changes of various metrics in the network during the attack.

In this method, the metrics in the network are taken as dimensions in the n-dimensional space, and each metric corresponds to a vector in the space. The change of the metric means that the length of the vector will change.

The AL-DDoS attack utility calculation model is divided into three steps: the first step is to determine the corresponding metric items according to the attack and defense features and map each metric to the n-dimensional parallelotope to calculate the parallel volume. The second step is to obtain the status value of the network system by the parallel volume. The third step is to calculate the change rate of the parallel volume according to the selection of threshold value and the calculation method of attack and defense utility and then compare the change rate with the threshold value to obtain the attack and defense utility value. Finally, the attack and defense utility value during the attack is obtained by calculating the average attack and defense value.

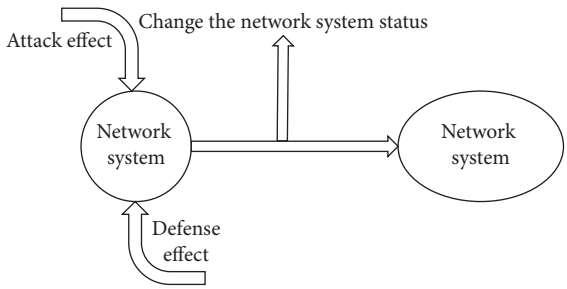

Figure 1: Attack and defense behavior effect in network system.

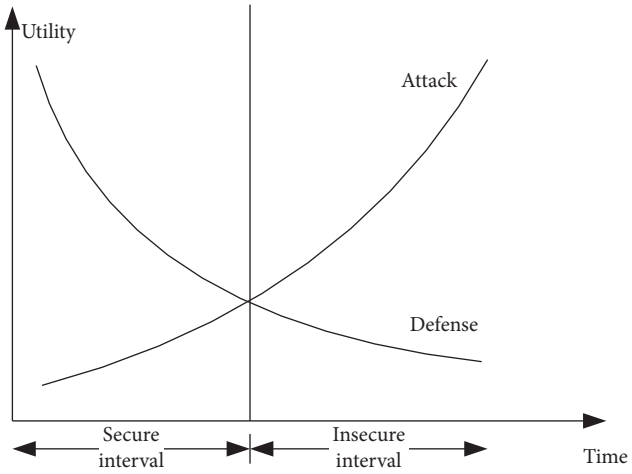

Figure 2: Utility criteria for network system security.

In this calculation method, the attack and defense effect should be compared with the threshold. The calculation method of threshold set is the calculation result of node status value by measuring the compound metric value without attack and defense effect. According to the average record, after an AL-DDoS attack, the average time for the defender to detect the attack is 1–5 hours. It is recommended to collect far more than the operation status of the server within 5 hours. Through the analysis of server data records, network analysis, application services, and other relevant indicators, the status value within 1–5 hours that is the most stable data fluctuation and relatively consistent with the legal access behavior track is selected as the threshold.

In the simulation, the attack strength is preset to 1, and the defense base strength is preset to 0. The current attack method and the effect of attack strength are obtained by calculating the change rate of the node status value caused by the attack effect. Under the condition that the initial value of node status is set to 0, that is, without adding defense measures, the attack effect is equal to the node status value. The calculation method of the defense effect can be derived in this way. Based on the variability of attack and defense behaviors, in order to ensure the universality of the calculation results of attack and defense effects, it is necessary to obtain the average attack effect within a certain period of time after the change of attack intensity is obtained by analyzing attack effect at each moment. In this way, the peak

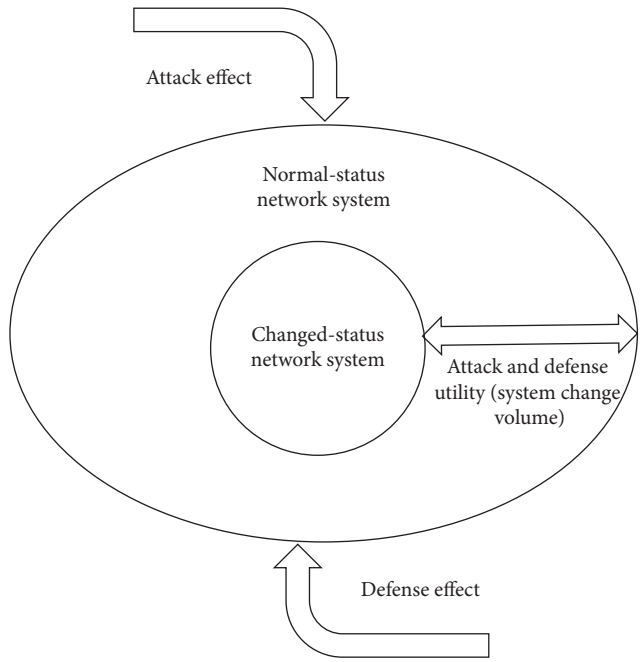

Figure 3: Attack and defense utility in attack and defense process.

and minimum values of the attack effect are eliminated to fully describe the attack effect.

On the premise that the time span remains unchanged, the calculation method of attack and defense is shown in Table 1. Table 1 lists the change value of the attack effect caused by the change of the attack strength and the change amount of the defense effect caused by the accumulation of defense measures. The data in the table are abstract values.

The attack and defense utility value can be used to describe the total attack on the network system during the attack and the total defense capability during the attack and defense. In AL-DDoS attacks, the attack traffic is not constant under normal circumstances, and the influence of network traffic is limited by many factors. Therefore, the expression of the attack effect can obtain the attack size at a certain point, but it cannot reflect the impact of the attack in the entire attack process.

On the basis of threshold value, the size of the attack effect at each moment can be obtained, and then the attack utility can be used to illustrate the impact value caused by the attack type during the entire attack process. In other words, the utility is the sum of the effects and the cumulative amount of the attack effect changing with time. If the attack effect size is F, when setting and selecting the threshold, the attack effect is 0, and the attack effect is also 0. If an attack occurs, set t_1 attack effect to be F_1, t_2 attack effect to be F_2, and t_n attack effect to be F_n. Based on the threshold setting, the calculation method of attack utility E is

$$E = \sum_{F_{t1}}^{F_{tn}} F. \tag{1}$$

The attack scale and intensity may change during the attack, but when the defense measures are attacked, it is

Table 1: Attack and defense parameter simulation calculation.

Time span	Attack strength	Defense strength	Node status	Attack effect	Defense effect
1	1	0	1	1	0
1	1	1	0	1	1
1	2	0	2	2	0
1	2	1	1	2	1

necessary to know whether the defense effect is constant. The defense effect can be obtained by comparing different attack effects. In this case, the average attack force will be calculated.

3.2. Utility Calculation Metric Selection. It is important to select appropriate metric to measure and analyze the impact value of attacks. As for the selection of metrics, the existing metrics when calculating the impact of the current DDoS attack are as follows. Sardana et al. [20] select effective network throughput, average access failure time and average response time as metrics in the measurement method. Dantas et al. [23] use the volume of traffic as the measurement metric. In the calculation method of influence value based on user service quality, the selected metrics are successful transaction rate, average response time, number of connections, average service rate, and request rate.

Comprehensive consideration of network traffic, hardware performance and other related indicators will be more suitable for analyzing the impact of DDoS attacks. 6 metrics were selected using the proposed metric selection [24].

(1) Network throughput rate: network throughput rate is used to describe the total number of data packets received and sent by the network card in the server during the attack. These data packets not only include the packets generated by normal user access, but also calculate the packets generated by attackers.

(2) TCP data segment transmission rate: AL-DDoS attacks may take advantage of the three-handshake mechanism of the TCP protocol to attack the server. The number of TCP segments is used to describe the number of TCP segments at any time during the attack.

(3) IP datagram transmission rate: in attack detection technology, IP datagrams are usually used to analyze the structure of datagram to detect the occurrence of attacks. Because of the nature of the TCP/IP protocol, it is essential to analyze the TCP data segment transmission rate and the IP datagram transmission rate.

(4) Transaction failure rate: when there are a large number of attacker requests in the server, the successful server accessing rate will be greatly affected due to bandwidth, server performance, and other factors. The failure rate is the ratio of the number of failed accesses to the total number of accesses at any time. According to the purposes and characteristics of AL-DDoS attacks, the access failure rate is the most important metric to detect attack.

(5) Average traffic arrival time: the average traffic arrival time refers to the time it takes to successfully access the server. When an AL-DDoS attack occurs, the average server response time must increase. As the attack strength increases, access timeouts may occur.

(6) Server CPU utilization: when an attack sends a large number of high-frequency service requests to the target server, the server will be busy providing response resources to the attacker, and the occupation of resources will inevitably affect the performance of the server hardware.

3.3. Network State Value Calculation. Given the combination of the current attack size and defense effect, the server status value represents the server status at each moment. In the calculation process, the average value of server status at each moment in the entire attack and defense process is selected as the calculation result [25]. The specific calculation steps are as follows.

The first step is to construct an **n**-dimensional matrix. In this calculation model, the values of the six metrics are, respectively, set as $\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4, \mathbf{m}_5, \mathbf{m}_6$. As mentioned above, each metric is a linearly independent vector in the **n**-dimensional Euclidean space **V**. Therefore, six metrics are selected to map to the vector dimension in the six-dimensional space, and the vectors are expressed as

$$\begin{bmatrix} \mathbf{m}1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ \mathbf{m}2 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \mathbf{m}3 \\ 0 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ \mathbf{m}4 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \mathbf{m}5 \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \mathbf{m}6 \end{bmatrix}. \tag{2}$$

Therefore, the 6-dimensional matrix composed of these six vectors can be expressed as a diagonal matrix, namely,

$$\mathbf{M} = \begin{bmatrix} \mathbf{m}1 & 0 & 0 \\ 0 & \dots & 0 \\ 0 & 0 & \mathbf{m}6 \end{bmatrix}. \tag{3}$$

As is shown in Figure 4, this is a 4-dimensional parallelotope. The second step is to calculate the volume of parallelotope in 6-dimensional space. The volume of parallelotope composed of six vectors in six-dimensional Euclidean space is as follows:

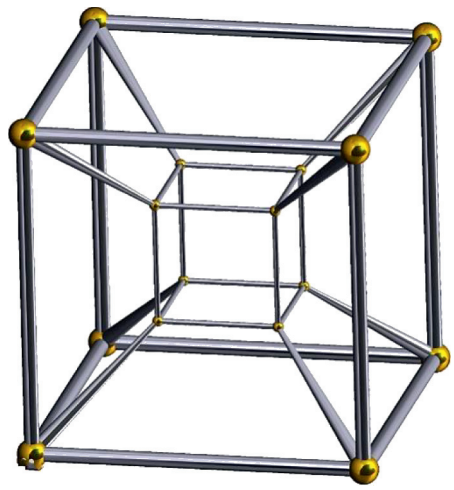

Figure 4: 4-dimensional parallelotope graphic model.

$$\mathbf{V}(\mathbf{m}_1, \mathbf{m}_2, \ldots \mathbf{m}_6) = \mathbf{V}(\mathbf{m}_1, \mathbf{m}_2, \ldots \mathbf{m}_5) \times \mathbf{gh}_6, \tag{4}$$

where $\mathbf{h}_6$ represents the length of the orthogonal component of $\mathbf{m}_6$ in the subspace generated by vectors $\mathbf{m}_1, \mathbf{m}_2, \ldots \mathbf{m}_6$, and $\mathbf{V}_1(\alpha_1) = |\alpha_1|$. It has been proved that $\mathbf{V}(\mathbf{m}_1, \mathbf{m}_2, \ldots \mathbf{m}_6) = \sqrt{\mathbf{G}(\mathbf{m}_1, \mathbf{m}_2, \ldots \mathbf{m}_6)} = |\mathbf{D}|$, where $\mathbf{D}$ is the determinant of coordinates on a set of standard bases of $(\mathbf{m}_1, \mathbf{m}_2, \ldots \mathbf{m}_6)$.

Therefore, the network status value at a certain time $\mathbf{t}$ is the determinant of the diagonal matrix $\mathbf{M}$. Set the network status value to $\mathbf{S_t}$, and the specific calculation method is

$$\mathbf{S_t} = |\mathbf{M}|. \tag{5}$$

The third step is to calculate the arithmetic average of the network status during the attack. During the duration of attack and defense effect of the network system, the network status value at each moment is, respectively, $\mathbf{S_{t_1}}, \mathbf{S_{t_2}}, \mathbf{S_{t_3}}, \ldots, \mathbf{S_{t_n}}$. Therefore, the arithmetic average of the network status is as follows:

$$\mathbf{S} = \frac{\sum_{\mathbf{i}=1}^{\mathbf{n}} \mathbf{S_{t_i}}}{\mathbf{n}}. \tag{6}$$

3.4. Effect Calculation. According to the calculation model of the status value, a part of the normal operation status of the network is selected and the status value $\mathbf{S}_0$ is calculated. When an attack effect occurs, the change of network status value can be described by the attack effect. When the attack strength is $\mathbf{X}$, the network status value is $\mathbf{S_i}$ at time $\mathbf{t_i}$. Then, the attack effect $\mathbf{A_{Xt_i}}$ is calculated as follows:

$$\mathbf{A_{Xt_i}} = \frac{\mathbf{S_i}}{\mathbf{S}_0}, \quad \mathbf{i} = (1, 2, \ldots, \mathbf{n}). \tag{7}$$

The attack effect value is averaged to reasonably describe the attack force of attack type during the attack. The calculation method of average attack force is as follows:

$$\overline{A} = \frac{\sum_{\mathbf{i}=1}^{\mathbf{n}} \mathbf{A_{Xt_i}}}{\mathbf{n}} = \frac{\sum_{\mathbf{i}=1}^{\mathbf{n}} \mathbf{S}_{1_i}/\mathbf{n}}{\sum_{\mathbf{i}=1}^{\mathbf{n}} \mathbf{S}_{0_i}/\mathbf{n}}. \tag{8}$$

There is a defense effect before the attack, but it is impossible to measure the defense effect. When the status value of the attacked system is obtained under the defense status of 0, the defense function is gradually added under the premise that the attack effect remains unchanged, and the defense effect is obtained through the system status value when each defense effect occurs.

If the attack intensity is X with no defense measures, the network status value is S_1, then the attack effect at time t_1 can be set to A_{Xt_1}. If defense measures are added to the system at this time, the network status value is S_1, the attack effect is changed to A_{Xt_1}, and the change value of attack effect is denoted as $\Delta A = A_{Xt_1} - A'_{Xt_1}$. According to the formula, the calculation method of defense effect at time t_1 is expressed as

$$\mathbf{D_{t_i}} = \frac{\mathbf{S_i} - \mathbf{S'_i}}{\mathbf{S}_0}, \quad \mathbf{i} = (1, 2, \ldots, \mathbf{n}). \tag{9}$$

The calculation method of the average defense force is as follows:

$$\overline{\mathbf{D}} = \frac{\sum_{i=1}^{n} \mathbf{S_{Xt_i}}}{\mathbf{n}}, \quad \mathbf{i} = (1, 2, \ldots, \mathbf{n}). \tag{10}$$

3.5. Utility Calculation. The attack and defense utility value represents the cumulative value of attack and defense effects. In the process of attack and defense, the role of attack and defense means changes at any time in practice. Therefore, in the evaluation process, it is necessary to obtain the utility value of two kinds of effects in the whole process; that is, the utility value can represent the total amount of the attack and defense effects in the process.

According to the calculation results obtained in (7) and (9), if the attack duration is t, the attack intensity is X, and the defense intensity is Y, and the average attack force is denoted as $\overline{A_X}$, and the average defense force is $\overline{D_X}$, then the calculation methods of attack utility E_A and defense utility E_D are as follows:

$$\mathbf{E_A} = \overline{\mathbf{A_X}} \cdot \mathbf{t}, \tag{11}$$

$$\mathbf{E_D} = \overline{\mathbf{D_X}} \cdot \mathbf{t}. \tag{12}$$

According to the calculation result of the attack and defense utility value, it can be concluded that the defense measures can resist a certain attack effect, and then the concept of defense efficiency is proposed. According to (11), when the defense is 0, it can be concluded that the attack utility value is E_A at the certain time t. After adding defense measures to the current system, the attack utility is E_A. Then, the calculation method of defense efficiency D_E is

$$D_E = \frac{E_D}{E_A} \times 100\%. \quad (13)$$

4. Experiment Design and Analysis

4.1. Experiment Design. According to the general attack methods and the application range of defense measures in the AL-DDoS attack types, HTTP/POST attack was selected as the attack type in the simulated attack and defense experiment, and load balancing and limiting the maximum number of connections were adopted as defense measures. Under the premise of using the same attack threads, 10, 20, and 30 attack nodes were selected to gradually increase the attack intensity. The program was designed for 10 combinations of attack and defense. The network topology of the attack and defense experiment is shown in Figure 5.

The environment configuration is shown in Tables 2 and 3.

The specific implementation process is as follows. The first step is to set the combination of attack and defense scale. The specific design of 10 scales was as follows: without attack and defense effect, and 10, 20, and 30 attack nodes, respectively, in three defense modes: no defense, load balancing, and limiting the maximum number of connections.

The second step is to collect experiment data. Performance monitoring tools JMeter and Spotlight are used to collect experiment data. According to the level of detail and accuracy of the tool, the experiment data were collected separately. In this simulated experiment, JMeter was used to collect three metrics, namely, server failure rate, average server access time, and peak server access traffic, while Spotlight was mainly responsible for collecting four metrics, namely, packet volume, TCP segment number, IP datagram number, and server CPU utilization.

The third step is to analyze the experiment results. Through the proposed calculation model, the data collected by simulation experiment of attack and defense were calculated and the calculated results were obtained. The calculation results were compared with the existing technical results, and the rationality and correctness of the calculation results were analyzed.

It is aimed at calculating various utility values of attack and defense after the occurrence of AL-DDoS attack, so the main purpose of constructing the experiment environment is to simulate the actual AL-DDoS attack. In order to better simulate distributed attacks, 30 attack nodes were constructed in the simulation experiment, and one of the small servers deployed web applications as the target. The environment was divided into three subnets by IP, which were connected by switches, respectively, and the network topology is a star structure.

4.2. Experiment Calculation Result

4.2.1. Effect Calculation Result. According to the experiment steps, two defense methods were selected for comparison experiments, namely, load balancing and limiting the maximum number of database connections. Because load balancing defense refers to reduce server pressure through distributed deployment, the average defense effect should be calculated to evaluate its defense effect. As the attack intensity changes, the average of HTTP/POST attack effects on the network system of the current experiment is shown in Table 4.

When the number of load balancing distributed deployment machines is constant, the effect of HTTP/POST attack on the network system changes with the attack intensity. Particularly, the average defense effect of load balancing and limiting the maximum number of connections is shown in Table 4 with the change of attack intensity.

4.2.2. Utility Calculation Result. According to the concept that the attack and defense utility is defined as 0 under the threshold status, the utility value and attack and defense efficiency under each combination can be calculated by using the calculation model of attack and defense utility. And the attack utility value under each attack intensity can be calculated.

Since at least 60 attack and defense data were continuously collected in this attack experiment, the time was set to 60.

4.3. Experiment Analysis. The defense efficiency of load balancing and limiting the maximum number of connections in the combination of HTTP/POST attack intensity are shown in Figure 6.

According to Figure 6, when the attack intensity is small, the defense effect of load balancing is larger, and the defense effect of limiting the maximum number of connections is relatively negligible. As the attack strength increases, the defense utility of limiting the maximum number of connections increases exponentially, far exceeding the defense utility of load balancing. This shows that when the attack intensity is small, the load balancing defense effect is good, and limiting the maximum number of connections can resist large-scale DDoS attacks.

As is shown in Figures 6 and 7, when the attack intensity is 10 nodes, the maximum number of connections obviously exceeds the number of connections sent by the attacker, and the defense effect is close to 0. When the attack intensity is 20 nodes, it can be seen that the set maximum number of connections can resist some attacks. When the attack intensity is 30 attack nodes, it can be observed that the system can almost completely resist the current scale attacks. This also raises the question of how to set the number of connections. If the limit is set too high, the system may not be able to resist the current strength of the attack. If the limit is set too small, it will easily lead to congestion or overflow and other abnormal phenomena, affecting the normal operation of the system. Therefore, we can judge how to set the maximum number of connections based on the existing

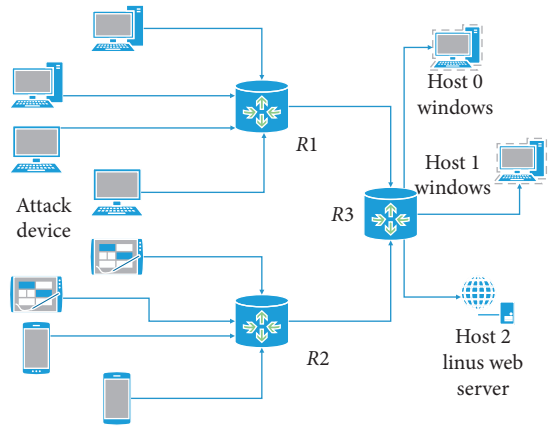

Figure 5: Attack and defense experiment network topology.

Table 2: Hardware and software environment configuration of attack nodes.

Device/software	Performance/function
ROM	2 GB
Processor	1
RAM	60 GB
Windows, Ubuntu operating system	Install test software and perform access service
Kali attack tool	Simulate various attacks and penetration tests
Wireshark	Capture packets and get messages
Burp Suite	Intercept log messages
LOIC	Package tool
JMeter	Website stress test tool
VMware Workstation	Simulate attack nodes

Table 3: Hardware and software environment configuration of target drone.

Device/software	Performance/function
ROM	4 GB
Processor	8
RAM	500 GB
Spotlight on Windows	Monitor server performance indicators
bWAPP	Target drone used for attack experiments
Java, php + MySQL + Apache	Build a web server environment
VMware Workstation	Build a virtual environment and software load balancing

experiment data and analyze the calculation results of this experiment.

4.4. Experiment Comparison. Through the study of the current AL-DDoS attack effect evaluation technology, a method is selected that Mirkovic [26] puts forward for the use of the user's quality of service (QoS) as a measure model. In the comparison technique, the author chooses the transaction failure rate as a measure of the QoS of various services. The author puts forward the method of calculating the amount of customer QoS degradation.

$$N = \frac{(d - t)}{t}. \tag{14}$$

N is the QoS degradation, t is threshold, and d is the value greater than the threshold value.

The value of QoS degradation N means that the service of transaction failure is N times the service that the user can tolerate. As calculated by the experiment data, the transaction threshold of failure rate is 0.075%. In order to show clearly, the attack utility is reduced by 10^{14} times in the figure.

As is shown in Figure 8, the utility method is more effective to determine the impact of an attack. The calculation model comprehensively considers the metric values of the impact of various AL-DDoS attack on the network system. Therefore, this method can obtain more comprehensive, accurate, and reasonable results compared with the existing methods.

Table 4: Average attack effect and defense effect.

	HTTP/POST attack	Load balancing	Limiting connections
10 nodes	4.651×10^{13}	2.895×10^{13}	0.031×10^{13}
20 nodes	1.076×10^{15}	6.951×10^{14}	7.521×10^{14}
30 nodes	1.437×10^{16}	7.714×10^{15}	1.405×10^{16}

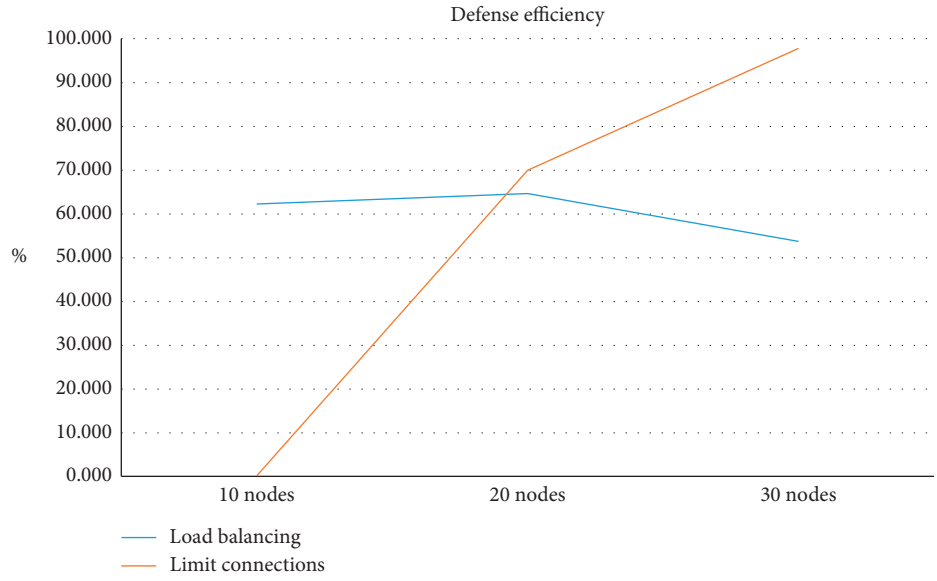

Figure 6: Defense efficiency based on the load balancing and limiting the maximum number of connections.

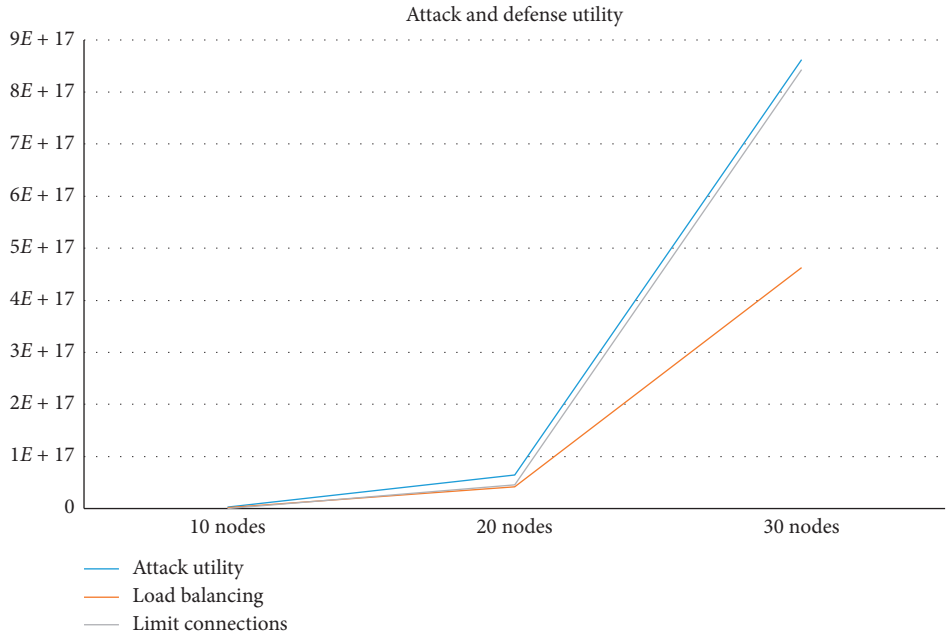

Figure 7: Attack and defense utility based on the load balancing and limiting the maximum number of connections.

By analyzing the attack and defense measures used in this experiment, we can obtain the attack utility value caused to the application layer of the current network under different attack intensity and calculate the defense utility value of each defense method under different attack intensity. The proposed attack and defense utility measurement method can quickly obtain the attack and defense utility value, without manual calculation and judgment, and can

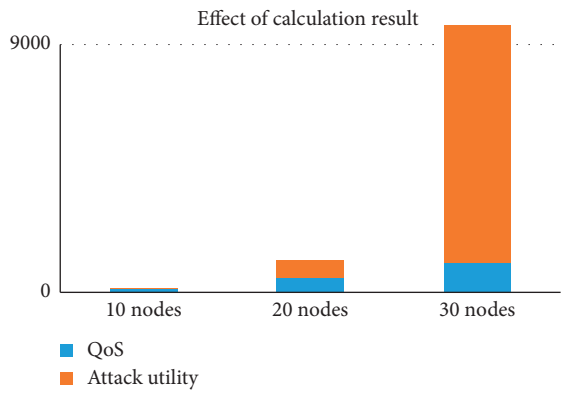

Figure 8: Influence of different attack strengths on calculation results under the same attack technology and defense strength.

accurately obtain the attack and defense impact value. This method has certain accuracy and objectivity and can judge the impact of attack and defense and the occurrence of potential attacks in real time.

5. Conclusion

Some factors are analyzed such as the characteristics of AL-DDoS attack and defense utility and the selection method of the existing indicators, and then the 6 metrics are selected. The attack and defense impact on the network itself and the impact on users are both considered, so as to accurately and objectively describe the network attack and defense behavior. For various network attacks, the metrics may be different, but traffic attacks also can use these metrics. Different models can be compared, so the method is objective.

Existing evaluation methods used to describe the measure results of the proposed concept lack theoretical support, while the concept of utility is used to describe the attack effect value. The concept of attack and defense utility is put forward by analyzing the characteristics of network behavior and combining traditional theory. The theoretical support makes the utility more reliable. At the same time, it is proposed to use hyperparallel volume to describe the network status. Based on this method, any number of indicators can be combined and calculated. Hyperparallel is used to map network space, which is an innovative attempt to network structure and interactive mathematical modeling.

The measurement is based on some certain information such as traffic, so the conclusion is objective. For example, the role and defense efficiency of defense technology in the attack can be analyzed separately, the attack effect on the network at a certain time can be analyzed, the status value that can be used to describe the network can be obtained, the attack and defense efficiency value can be calculated, and finally the attack and defense utility value can be calculated.

This method is more objective and effective than traditional methods. This method has smaller deviation and higher accuracy compared with single or few index methods. This method also provides a reference for various attack and defense methods. The use of mathematical methods to evaluate attack and defense behavior is more objective and easier to compare. More attack and defense methods can be used to conduct combined experiments on network systems for security evaluation against AL-DDoS attacks, so as to verify the utility of other attack and defense methods on the target network.

These 6 metrics are selected only for AL-DDoS attacks. These metrics are mainly suitable for traffic attacks. For other types of attacks, the calculation model is suitable but the metrics may be different. In the experiment design, the attack strength change. Attack and defense types are limited. There are only three changes in attack strength. The subdivision of the experiment is not enough.

In future work, we may try other different types of datasets, change other metrics, and conduct attack and defense experiments. Attack and defense experiments with smaller gradient changes and more types will be designed.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key Research and Development Program of China under Grant 2016QY06X1205.

References

[1] S. Boyer, O. Dain, and R. Cunningham, "Stellar: a fusion system for scenario construction and security risk assessment," in *Proceedings of the Third IEEE International Workshop on Information Assurance*, March 2005.

[2] A. A. Ramaki, M. Khosravi-Farmad, and A. G. Bafghi, "Real time alert correlation and prediction using Bayesian networks," in *Proceedings of the 2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, Rasht, Iran, Sepetember 2016.

[3] P. Mukherjee and C. Mazumdar, "Attack difficulty metric for assessment of network security," in *Proceedings of the ARES 2018*, Hamburg, Germany, August 2018.

[4] Z. Wen, C. Cao, and H. Zhou, "Network security situation assessment method based on naive Bayes classifier," *Journal of Computer Applications*, vol. 35, no. 8, pp. 2164–2168, 2015.

[5] J. X. Wang, Y. Feng, and R. You, "Network security measurement based on dependency relationship graph and common vulnerability scoring system," *Journal of Computer Applications*, vol. 39, no. 6, pp. 1719–1727, 2019.

[6] M. T. Manavi, "Defense mechanisms against distributed denial of service attacks: a survey," *Computers & Electrical Engineering*, vol. 72, pp. 26–38, 2018.

[7] H. Luo, Y. Lin, H. Zhang, and M. Zukerman, "Preventing DDoS attacks by identifier/locator separation," *IEEE Network*, vol. 27, no. 6, pp. 60–65, 2013.

[8] X. Ma and Y. Chen, "DDoS detection method based on chaos analysis of network traffic entropy," *IEEE Communications Letters*, vol. 18, no. 1, pp. 114–117, 2014.

[9] S. Bravo and D. Mauricio, "DDoS attack detection mechanism in the application layer using user features," in *Proceedings of the 2018 International Conference on Information and Computer Technologies ICICT*, March 2018.

[10] Y. J. Li, B. Y. Liu, S. Zhai, and M. R. Chen, "DDoS attack detection method based on feature extraction of deep belief network," *IOP Conference Series Earth and Environmental Science*, vol. 252, Article ID 032013, 2019.

[11] A. Praseed and P. S. Thilagam, "DDoS attacks at the application layer: challenges and Research perspectives for safeguarding web applications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 661–685, 2019.

[12] P. Sivakumaran and J. Blasco, "A study of the feasibility of co-located app attacks against BLE and a large-scale analysis of the current application-layer security landscape," in *Proceedings of the 28th USENIX Security Symposium*, pp. 1–18, Santa Clara, CA, USA, August 2019.

[13] W. Zhou, Y. Jia, Y. Yao et al., "Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms," in *Proceedings of the 28th USENIX Security Symposium*, pp. 1133–1150, Santa Clara, CA, USA, August 2019.

[14] M. Kumar and A. Bhandari, "Performance evaluation of web server's request queue against AL-DDoS attacks in NS-2," *International Journal of Information Security and Privacy*, vol. 11, no. 4, pp. 29–46, 2017.

[15] C. Wang, T. T. N. Miu, X. Luo, and J. Wang, "SkyShield: a sketch-based defense system against application layer DDoS attacks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 559–573, 2018.

[16] K. S. Sahoo, S. K. Panda, S. Sahoo, B. Sahoo, and R. Dash, "Toward secure software-defined networks against distributed denial of service attack," *The Journal of Supercomputing*, vol. 75, no. 8, pp. 4829–4874, 2019.

[17] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[18] J. Cao, Q. Li, R. Xie et al., "The crossPath attack: disrupting the SDN control channel via shared links," in *Proceedings of the 28th USENIX Security Symposium*, pp. 19–36, Santa Clara, CA, USA, August 2019.

[19] A. Procopiou, N. Komninos, and C. Douligeris, "ForChaos: real time application DDoS detection using forecasting and chaos theory in smart home IoT network," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 8469410, 14 pages, 2019.

[20] A. Sardana and R. C. Joshi, "An integrated honeypot framework for proactive detection, characterization and redirection of DDoS attacks at ISP level," *Journal of Information Assurance and Security*, vol. 1, pp. 1–15, 2018.

[21] K. Tang and X. Zhang, "Construction of human subject: expansion and limitation of the perspective of network sociology," *Social Sciences in Hunan*, vol. 5, pp. 67–74, 2017.

[22] C. Hu, "Calculation of the behavior utility of a network system: conception and principle," *Engineering*, vol. 4, no. 1, pp. 171–185, 2018.

[23] Y. G. Dantas, V. Nigam, and I. E. Fonseca, "A selective defense for application layer DDoS attacks," in *Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference*, The Hague, Netherlands, September 2014.

[24] K. Singh, P. Singh, and K. Kumar, "User behavior analytics-based classification of application layer HTTP-GET flood attacks," *Journal of Network and Computer Applications*, vol. 112, pp. 97–114, 2018.

[25] X. Zhao, Q. Chen, J. Xue, Y. Zhang, and J. Zhao, "A method for calculating network system security risk based on a lie group," *IEEE Access*, vol. 7, pp. 70610–70623, 2019.

[26] J. Mirkovic, A. Hussain, B. Wilson et al., "Towards user-centric metrics for denial-of-service measurement," in *Proceedings of the Workshop on Experimental Computer Science*, San Diego, CA, USA, June 2007.