Hindawi
Security and Communication Networks
Volume 2023, Article ID 4501050, 15 pages
https://doi.org/10.1155/2023/4501050

Research Article

Research on Network Behavior Risk Measurement Method Based on Traffic Analysis

Qiyao Wang, Xiaolin Zhao, Jiong Guo, Jingfeng Xue, and Bin Zhao

School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China

Correspondence should be addressed to Jingfeng Xue; xuejf@bit.edu.cn

Received 30 December 2021; Revised 27 June 2022; Accepted 24 November 2022; Published 24 April 2023

Academic Editor: Chien Ming Chen

Copyright © 2023 Qiyao Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

At present, the network security problem is facing a serious threat, and network security events continue to occur. It has become an important link to prevent network attacks and ensure network security. According to the network security protection measures and security technical requirements, it has become an urgent need to establish appropriate security measurement methods and strengthen the monitoring and analysis of network security status. This study proposes a network behavior risk measurement method based on traffic analysis to accurately and objectively evaluate the security state of the network. Traffic is the most basic behavior of the network and the basis of security risk measurement. Firstly, we regard the traffic data as network behavior to build scenarios. Through differential manifold modeling, the traffic data and topology of the network system are semantically described to form a matrix. Then, after manifold dimensionality reduction, the objective risk assessment value can be obtained by manifold mapping and Riemann metric. In this study, the differential manifold theory is applied to network behavior risk measurement, and the innovation of differential manifold in the field of network behavior risk measurement is given. After giving the network behavior risk measurement theory, we first verify the effectiveness of the proposed method through the simulation experiments. Secondly, the public CIC-IDS-2017 data set is used for analysis and calculation to prove the accuracy of the proposed method.

1. Introduction

1.1. Background. At present, computer network is playing a more and more important role. However, the potential threat of computer network is its own vulnerability and the vulnerability of communication equipment. On the one hand, computer network hardware and communication equipment are vulnerable to the influence of natural environmental factors such as dust, humidity, temperature, electromagnetic field, and man-made physical damage [1]. On the other hand, due to the nature of information sharing and open platform of the network itself, important assets, software resources, and data information in the computer are vulnerable to illegal theft, replication, tampering, and destruction. All these lead to the damage, loss, and security accidents of assets and data information in the computer network system. Network behavior risk assessment can judge the security performance of the network to a certain extent. On this basis, it can continuously improve the security of the network for the weak links of the network and further improve the network security situation [2]. Therefore, it is very important to propose effective network security measurement methods and improve them. With the rapid development of computer network, traffic attacks appear frequently which is the most common type of network attacks [3]. Therefore, it is also very important to propose network security metrics for traffic attacks.

At present, the research on network security measurement is mainly divided into two perspectives: network management security and network technology security. The research of network management security mainly focuses on the published network security guidelines or international standards [4]. Network technology security measurement is mainly divided into qualitative measurement and quantitative measurement [2, 5]. Qualitative measurement generally does not use mathematical methods. The evaluator can directly draw a conclusion on the evaluation network through expert

experience and existing knowledge and through the inductive analysis of the current network security situation [6]. Quantitative measurement makes a quantitative judgment on the network security situation by constructing a mathematical model or through a certain quantitative method [7–10]. Compared with the subjective judgment of qualitative evaluation, quantitative evaluation can effectively quantify the network security situation, but it requires a lot of data analysis and comparison, and the implementation is more complex [6, 11]. Both of them have the problems of weak objectivity and inaccurate measurement.

1.2. Innovation. This study summarizes and analyzes the common methods of network security measurement. Aiming at the problems of weak objectivity and inaccurate measurement in the existing methods, this study puts forward the network behavior risk calculation method, obtains the network attack and defense behavior through the traffic analysis, and uses the differential manifold theory to describe the network behavior state in the attack and defense process, so as to measure the network behavior risk. Finally, based on the measurement model proposed in this study, the feasibility and effective ness of the algorithm are verified by attack and defense experiments in real environment and public CIC-IDS-2017 data set.

The network behavior risk measurement method based on traffic analysis proposed in this study can reflect the security state of the network, intuitively analyze the change degree of the security state of the network system in the process of attack and defense, and accurately evaluate the performance of the network.

The innovation of this study is as follows:

(1) The network traffic is regarded as network behavior, and the definition of network behavior risk is proposed to realize the quantitative analysis of network behavior

(2) The local linear embedding dimension reduction algorithm of manifold learning is used to reduce the dimension of the index

(3) Aiming at the problems of weak objectivity and inaccurate measurement in the existing methods of network security measurement by describing the network behavior state in the process of attack and defense, the differential manifold theory is applied to the network behavior risk measurement, and the network behavior risk calculation method is proposed

2. Related Research

Network technology security is the evaluation and analysis of the system security of the network, such as availability, integrity and confidentiality, and the vulnerability risk of the network. Network technology security measurement is mainly divided into qualitative measurement and quantitative measurement [2, 6].

Sheng et al. [12] introduced analytic hierarchy process, according to the characteristics of network architecture defined by software, selected several typical indicators affecting network security status, and calculated the overall network security value. Wang et al. [13] made full use of the advantages of grey analytic hierarchy process to evaluate the network security risk. The qualitative measurement model has the advantages of convenient evaluation and strong applicability, but human factors have a great impact on the final evaluation results, lack of objectivity, and often have the problem of inaccurate evaluation [6].

The network security measurement method based on attack graph is a common quantitative measurement method. Phillips and Swiler [14] mapped the network system into an attack graph for the first time, intuitively displayed and analyzed the possible attack paths, vulnerabilities, and important nodes in the network, and proposed a new network security measurement algorithm based on these attacks information. Literature [15] combined with attack graph technology used Bayesian network to determine the atomic attack nodes of the network, so as to obtain the overall security value of the network and optimize the measurement results. However, the network security measurement method based on attack graph is not objective and is not suitable for complex networks.

The detection of network traffic data can also reflect network anomalies. The latest trend of network anomaly detection based on network traffic data includes emerging machine learning technologies such as artificial neural network (ANN), support vector machine (SVM), l-nearest neighbor (KNN), decision tree, clustering, and statistics [16]. In related research, traffic classification is the first step to identify malicious use of network resources by anomaly detection and other activities [17]. Wang et al. [18] proposed a malware traffic classification method based on convolutional neural network and taking traffic data as image for security detection. Marir et al. [19] used a group of multilayer support vector machines and deep feature extraction in large-scale networks to identify abnormal behaviors and detect network security. First, the distributed deep trust network is used to nonlinear reduce the dimension of network traffic data, and then the extracted features are used as input to construct multilayer support vector machine through spark-based iterative dimension reduction paradigm. Shubair et al. [20] proposed an intrusion detection system based on traffic data, which takes advantage of the combination of KNN method and fuzzy logic. The minimum mean square method is used for error reduction, KNN selects the best matching class, and fuzzy logic selects the flow class label. Liu et al. [10] proposed a detection method based on Riemannian measurement of traffic data, which uses fast Fourier transform and information entropy to detect attacks.

With the continuous development of network security performance requirements, the previous measurement methods are difficult to meet the needs of measurement accuracy and accuracy, and the introduction of mathematical principles can describe the network security situation with more objective and accurate methods and values

[21, 22]. In this study, the differential manifold theory is applied to network behavior risk measurement. Differential manifolds have been widely used in theoretical physics and high-dimensional data dimensionality reduction research [23]. With the rapid development of network informatization, more and more differential manifolds have been applied in the field of computer networks [24]. For example, the differential manifold and Riemann metric are applied to the robot performance and network control simulation to improve the robot operation and motion performance. In the field of computer vision, introducing differential manifold for information extraction [1, 25] and using differential manifold to improve image processing efficiency [26]. Using differential Manifolds and Riemann metrics to study network attack and defense effectiveness and to achieve the evaluation of network system security performance [27, 28]. Therefore, analyzing network risk and evaluating cyber security situation through mathematical principles have gradually become the trend of measurement research.

To sum up, the comparison of various common network security measurement methods is shown in Table 1.

Aiming at the problems of weak objectivity and inaccurate measurement in the existing network security measurement methods, this study summarizes and analyzes the common methods, puts forward the network behavior risk calculation method, and applies the differential manifold theory to the network behavior risk measurement by describing the network behavior state in the process of attack and defense. Finally, based on the measurement model proposed in this study, we verify the feasibility and effectiveness of the algorithm by using the public CIC-IDS-2017 data set and conducting attack and defense experiments in real environment.

3. Traffic Behavior Analysis and Differential Manifold

This study proposes the network behavior risk calculation method, obtains the network attack and defense behavior through traffic analysis, uses the differential manifold theory to model the network attack and defense behavior, and makes the network security measurement through the network attack and defense behavior.

3.1. Network Security Measurement. Network security means that valuable assets such as data and information in the network system will not be leaked, tampered with, or damaged due to wrong operation inside the network or malicious attack outside the network. The ideal situation of network security is that the network will not be affected by external attacks. However, the network is always facing threats.

Network security measurement is to detect the vulnerabilities in the network, judge the possible network attack means and several existing network attack paths, and determine the current security state of the network through the evaluation of security data indicators such as vulnerabilities, assets, and traffic in the network [29].

The basic steps of network security measurement are shown in Figure 1.

3.2. Traffic Behavior Analysis. Traffic is the most basic behavior of the network and the basis of security risk measurement. The complete traffic includes the data information of application layer, transport layer, network layer, and physical layer. The definition of traffic [30] on the transport layer is it describes the packet string with the same IP address, port number, and protocol (TCP, UDP, ICMP, and so on).

The behavior analysis of network traffic mainly analyzes the behavior characteristics of traffic by analyzing the characteristic parameters such as bandwidth/throughput and delay. Taking network traffic as the research object, this study takes the characteristic parameters such as bandwidth and delay of traffic as indicators to analyze the behavior of network traffic. The behavior analysis of network traffic is a direct and effective means to obtain the state of the network. It can understand and master the behavior of traffic, help to obtain the characteristics of network performance, reliability, and security, and establish the behavior model of the network.

From the perspective of network traffic data analysis, this study regards the network traffic data collected from the actual network as a network behavior by collecting and monitoring the network packet information in real time and then proves that the network system is a topological manifold, uses the differential manifold to model the network behavior, and measures the network security through the network behavior.

3.3. The Relationship between Network Security Metrics and Differential Manifolds. We use the differential manifold theory to study the network security metrics. It is necessary to prove that the network system is a topological manifold in order to calculate the network risk and judge the network security state by using the differential structure and given Riemannian metric. The specific proof is as follows.

Definition 1. Network topology.

Network topology is the shape of network and the physical connectivity of network. Network topology refers to the physical layout of various devices interconnected by transmission media [31].

From the definition of network topology, it is obvious that the network system is a topological space. Any subsystem of a network system must also be a network system. Several network systems can be connected to form a large network system through topology. Hausdorff space is a topological space, and Hausdorff space is a topological space whose points are "separated by domains." Therefore, the network system is a Hausdorff space.

Definition 2. Topological manifold.

Let m be a Hausdorff space. If there exists an open field $U \in M$ at any point such that the open field is homeomorphic with the open subset in Euclidean space R^n, then M is a topological manifold [31].

Table 1: Comparison table of common network technology security measurement methods.

Measurement method	Advantage	Disadvantage
Analytic hierarchy process	Qualitative and quantitative measurement method	Strong subjectivity, incomplete analysis, and poor comparability of measurement results
Attack graph	Mature method and can measure the direction and path of network attack	Weak objectivity and not suitable for complex networks
Machine learning	The current research hotspot and can identify various network attacks	The model relies on a large amount of data training
Flow analysis	Can accurately reflect network anomalies	At the stage of development
Principles of mathematics	Markov chain and differential manifold at el. and can accurately describe network behavior and network security state	Little research on relevant aspects and at the stage of development

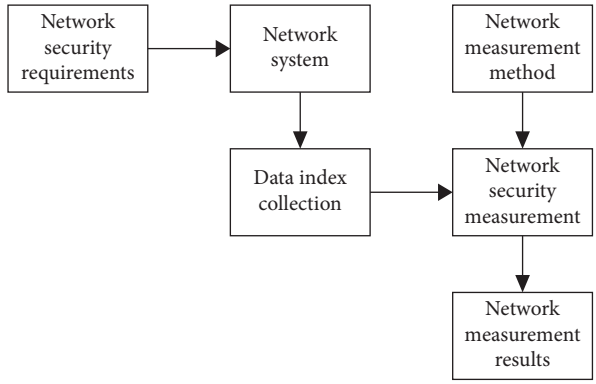

Figure 1: Network security measurement process.

According to the definition of topological manifold, if every point in a Hausdorff space can find an open field homeomorphic to a Euclidean space, then the space becomes a topological manifold. For a network system, we can always find a homeomorphism mapping, which satisfies $f: x \longrightarrow U(x) \in R_+^n$, and then the network system is a topological manifold.

Definition 3. Riemannian metric.

Let M be a n dimensional optical slip flow shape and construct a positive definite and symmetric second-order covariant smooth tensor field g on M, that is, $g(p)$ is for any $p \in M$ a positive definite, symmetric second-order covariant tensor on T_p^M, then g is a Riemannian metric of M, and M is a Riemannian manifold [32].

3.4. The Feasibility of Measuring Network Security by Differential Manifold. Differential manifold has been widely used in theoretical physics and dimensionality reduction of high-dimensional data [23]. With the rapid development of network informatization, there are more and more applications of differential manifold in the field of computer network [24]. For example, differential manifold and Riemannian metric are applied to the simulation of robot performance and network control to improve the robot operation and motion performance. In the field of computer vision, the information extraction method of differential manifold is introduced to improve the efficiency of image processing [25], differential manifold is used to improve image processing efficiency [26], differential manifold and Riemannian metric are used to study network attack and defense utility, to realize the evaluation of network system security performance [27, 28], and so on.

Network security measurement is an effective process to measure security and protect data based on a certain scale [33]. The network needs to quantify the security elements related to the system security quality, such as vulnerability, risk, attack, and defense [34].

Differential manifold is a mathematical model that can objectively calculate and measure things. The advantage of differential manifold is that it can keep the data topology unchanged in the change of dimension and explore the internal geometric structure and regularity hidden in the data. Therefore, differential manifolds can be used to measure network behavior risk. The network system itself is regarded as a manifold in one or more scenarios.

Compared with traditional methods, network security assessment based on differential manifold can solve problems that are not objective and comprehensive and can better reflect the impact of changes in security metrics on network security changes, making the metrics more objective and accurate than previous assessment methods [21, 27]. At the same time, the network security evaluation method based on differential manifold can consider the network security risk at multiple levels and explain the transformation of the network security state from the perspective of attack and defense utility.

4. Research on Network Behavior Risk Measurement Based on Manifold

The process of using differential manifold to measure network behavior risk is as follows: first, collect data and reduce the dimension of indicators to obtain a series of measurement indicators. In addition, second, construct a network security measurement index group through these indexes. Third, calculate the network security state value before and after network attack by using network system differential manifold. By comparing the risk values in different time periods, we can judge whether the network is at risk in this period.

4.1. Definition of Network Behavior Risk. Network behavior risk involves key elements such as vulnerability, threat, asset, risk, and so on [35]. The factors involved in network behavior risk are the result of mutual influence and interaction. Vulnerability and threat will increase network risk. Risk mainly affects assets. Security measures to deal with risk can reduce the impact of vulnerability and threat. The relationship between various factors of network behavior risk is shown in Figure 2.

Network security events cause network behavior risk. The occurrence of network behavior risk is a function of the emergence of threats and the utilization of vulnerability. The impact of network behavior risk is the destruction and loss of network assets. Therefore, network behavior risk can be defined as follows:

$$R = f(T, V, A). \tag{1}$$

Among them, R is network behavior risk, f is network behavior risk calculation function, T is network threat, V is network vulnerability, and A is information assets in the network.

4.2. Network Security Baseline. In order to realize the quantitative assessment of network risk, it is necessary to set an objective baseline that can reflect whether the network is safe or not. Network security baseline is the dividing point to judge whether the network is safe or not. By comparing the network security risk status and

network security baseline, we can determine whether the current network is at risk. First, we need to study the security attributes of the network security infrastructure such as assets and information; second, the evaluation standard and calculation model of network security baseline are established; finally, we compare the security baseline to determine the current risk status of the network. At the same time, when the security requirements or security factors in the network system change, the network security baseline should be adjusted appropriately.

As shown in Figure 3, it is assumed that the network security baseline value under certain security factors is α. The result of network behavior risk value calculated after network security detection is β. By comparison, if the results of the two values are consistent or within a certain error range, then it shows that the network system is in a safe state in this period of time. If the risk value is lower than the risk value β much larger than the baseline α. So, it shows that in this period of time, the security state of the network system has changed, and the network may be attacked in a network risk state.

4.3. The Selection of Measurement Index of Network Behavior Risk. The selection of network behavior risk measurement index should have the following characteristics: (1) the index is clear, the meaning of data index is clear, each index is relatively independent, there is no redundancy, and it is easy to calculate; (2) it can cover all kinds of network indicators, including traffic, host, and other common indicators; and (3) it is easy to expand. With the complexity of the network and the changes of other factors, the network behavior risk measurement index can add the necessary data indicators that affect the network security factors.

In this study, the indicators selected in the measurement network are shown in Table 2. Section 6.2 of this study uses CIC-IDS-2017 data set for experiment. Among them, CIC-IDS-2017 data set contains more than 80 characteristic indicators.

4.4. Dimension Reduction of Network Behavior Risk Measurement Index. Network behavior risk measurement is a comprehensive analysis of the existing network security state. Therefore, there are some problems in the measurement: (1) there are many attributes involved in the measurement index and (2) there are many kinds of indicators. Each level collects dozens or even hundreds of indicators. Based on the above two points, after the completion of the index collection, we need to simplify the index. The comparison of common dimensionality reduction methods is shown in Table 3:

To sum up, locally linear embedding algorithm, which is based on manifold learning, can better maintain the original key features and geometric properties of data than other methods. Therefore, this study uses manifold learning method to reduce the dimension of the index.

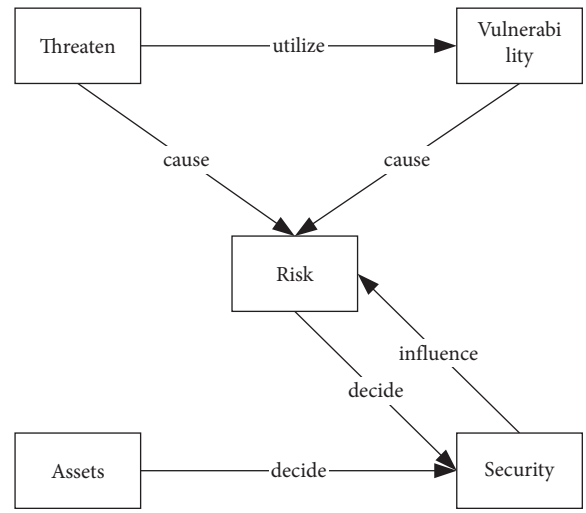

Figure 2: The relationship among various factors of network behavior risk.

Locally linear embedding algorithm considers that every data point can be constructed by the linear weighted combination of its nearest neighbors. The main steps of the LLE algorithm are divided into four steps:

(1) Find k nearest neighbors of each index data point in the original index data sample space

(2) Approximately calculate the weight matrix M of the index sample space through these nearest neighbors

(3) Decompose the weight matrix M to obtain eigenvalues and eigenvectors

(4) Take the eigenvector corresponding to the smallest d eigenvalues, that is, the new index data after dimension reduction

4.5. Network Behavior Risk Measurement. According to the definition of network behavior risk in Section 4.1, this study uses differential manifold to measure and calculate network behavior risk, which can describe network attack and defense process, and describe network scene and network behavior. At the same time, differential manifold can map network system and network index data space into a high-dimensional space to better describe the change degree of network behavior risk. When the network is threatened by external attacks, the state of network indicators will also change to a certain extent. Then, the network security risk value can be expressed by measuring the change value of network indicators through a certain calculation method. The relationship between network risk and index changes is shown in Figure 4.

In Section 4.3, the network risk measurement index group has been established. The vector group composed of these indexes can form a high-dimensional data manifold space. If the high-dimensional data manifold is surface integrated, the calculated results can represent the corresponding network risk state change of the network system when the data index changes. The surface integral of

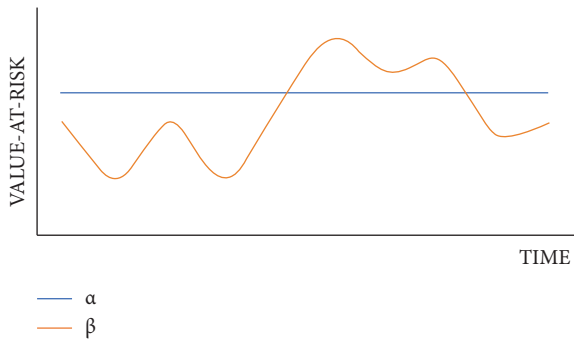

Figure 3: Network security status change.

Table 2: Network security measurement metrics.

One-level indicators	Two-level indicators	Three-level indicators
Network security risk	Computing storage	CPU utilization
		Memory utilization
		Disk utilization
	Bandwidth consumption	Bandwidth utilization
		Throughput
	Flow change	Flow rate
		Instantaneous flow
	Data packet	Packet loss rate
		Packet length
		Packet quantity

a manifold is actually the volume of the manifold in a high-dimensional space. Therefore, the results of network behavior risk can be expressed by the hypervolume of the high-dimensional data manifold composed of network security indicators.

In the high-dimensional data manifold space, we can define certain differential structures and Riemannian measures to calculate the changes of these indicators in the network attack and defense. After integral operation, the transformation quantity can represent the risk of the network. If the matrix form is used to represent the current network index state of the network system, assume that the data index set is $(x_1, x_2, \ldots, x_m)$. Then, in time $(t_1, t_2, \ldots, t_n)$, there are $m * n$ state variables in the matrix. Therefore, the network index state matrix S can be expressed as follows:

$$S = \begin{bmatrix} s(x_1, t_1) & s(x_2, t_1) & \cdots & s(x_m, t_1) \\ s(x_1, t_2) & s(x_2, t_2) & \cdots & s(x_m, t_2) \\ \cdots & \cdots & \cdots & \cdots \\ s(x_1, t_n) & s(x_2, t_n) & \cdots & s(x_m, t_n) \end{bmatrix}. \quad (2)$$

In the measurement of network behavior risk, we need to define the measurement function f. After the definition of network risk is given, the change process of network security state is expressed as the change of points and data on the differential manifold. The change state of network system security index constitutes a "point" in the differential manifold. By integrating the change state of security index on the differential manifold, the risk measurement result is obtained. For matrix S, the process of calculating network risk by using differential manifold and metric function can be expressed as follows:

$$f: R^{n^2} \longrightarrow R_+^n. \quad (3)$$

The metric function f represents the integral function of the differential manifold to calculate the network risk. In the process of network attack and defense, the risk of network security behavior changes instantaneously. There is no reference significance to calculate the value of network security state at a single time. Only in a period of dynamic change can it have the significance of measuring security. Therefore, in a period of time t, when the network index set $X = (x_1, x_2, \ldots, x_n)$ changes, the calculation of network risk is expressed by the following formula:

$$R = \int \Delta(S) \mathrm{d}s. \quad (4)$$

Through formula (4), the index state in the network system is mapped into a matrix, and the change of the index is combined with the change of the network risk, and the general calculation formula of the network risk is given. In this study, the description of the change of the network index set is based on the differential manifold. The process of the change of the index set is the change process of the high-dimensional manifold of the index data. The integral of the manifold change represents the change of the network security state. Finally, the network risk can be determined by comparing with the security baseline value.

5. Network Behavior Risk Calculation Model

The network behavior risk measurement process can be divided into three parts: data index collection and processing, network measurement manifold construction, and network behavior risk calculation.

5.1. Index Dimension Reduction Calculation Model. In this study, the locally linear embedding LLE algorithm is used to reduce the dimension. The LLE algorithm considers that the original data sample is linear in a small part. Suppose there is a sample x_i. Then, several sample points x can be found in the original high-dimensional neighborhood $x_1, x_2, \ldots, x_k$. It exists as follows:

$$x_i = w_{i1}x_i + w_{i2}x_2 + \cdots + w_{ik}x_k, \quad (5)$$

where $w_{i1}, w_{i2}, \ldots, w_{ik}$ is the weight coefficient. After dimension reduction by the LLE algorithm, part of the linear relationship of data can still be maintained in the new space, and the weight relationship before and after dimension reduction can be kept unchanged or slightly changed. Namely,

$$x_{i'} = w_{i1}x_{i'} + w_{i2}x_{2'} + \cdots + w_{ik}x_{k'}. \quad (6)$$

Table 3: Comparison of dimension reduction algorithms.

Algorithms	Advantage	Disadvantage
PCA	Linear mapping to eliminate the interaction of data	Only deal with the sample variance, not nonlinear data
LDA	Used for big data classification	Not suitable for non-Gaussian distribution samples
KPCA	Nonlinear data can be processed on the basis of PCA	Depend on the choice of kernel function
MDS	Keep sample difference on Euclidean distance	Not consider the distribution and interaction of adjacent data
Isomap	Preserve the geometric properties of samples on manifold distance	Not suitable for manifolds with large curvature
LLE	Solve the problem of high-dimensional data distribution	Need to assume that the manifold of the sample exists

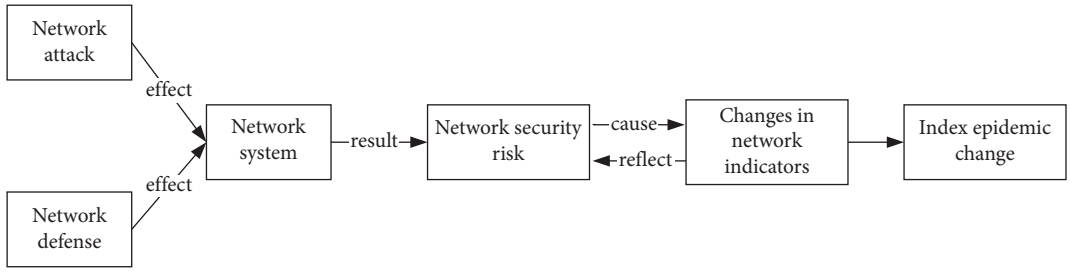

Figure 4: Relationship between network risk and network index change.

The main steps of LLE algorithm are divided into four steps as shown in Section 4.4.

In order to illustrate the calculation process, the data space of m n-dimensional samples $X = x_1, x_2, \ldots, x_m$ is selected and the loss function is matrixed to obtain as follows:

$$\begin{aligned} J(W) &= \sum_{i=1}^{m} \left\| x_i - \sum_{j \in Q(i)} w_{ij} x_j \right\|_2^2 \\ &= \sum_{i=1}^{m} \left\| \sum_{j \in Q(i)} w_{ij} x_i - \sum_{j \in Q(i)} w_{ij} x_j \right\|_2^2 \\ &= \sum_{i=1}^{m} \left\| \sum_{j \in Q(i)} w_{ij} \left(x_i - x_j \right) \right\|_2^2 \\ &= \sum_{i=1}^{m} W_i^T \left(x_i - x_j \right) \left(x_i - x_j \right)^T W_i, \end{aligned} \tag{7}$$

where $Q(i)$ is the k nearest neighbor sample set of i, $Wi = w_{i1}, w_{i2}, \ldots, w_{ik}{}^T$. The weight coefficient satisfies the following equation:

$$\sum_{j \in Q(i)} w_{ij} = W_i^T I_k = 1. \tag{8}$$

Let matrix $Z_i = (x_i - x_j)(x_i - x_j)^T$, calculate the weight coefficient W_i as follows:

$$Wi = \frac{z_i^{-1} I_k}{I_k^T Z_i^{-1} I_k}. \tag{9}$$

Suppose that the projection of sample set in low dimension $d\,(d < m)$ is $Y = \{y_1, y_2, \ldots, y_m\}$. In order to keep the linear relationship after dimension reduction, the matrix objective loss function is as follows:

$$\begin{aligned} J(Y) &= \sum_{i=1}^{m} \left\| y_i - \sum_{j=1}^{m} w_{ij} y_i \right\|_2^2 \\ &= \sum_{i=1}^{m} \left\| Y I_i - Y W_i \right\| \\ &= \mathrm{tr}\left(Y (I - W)(I - W)^T Y^T \right). \end{aligned} \tag{10}$$

Let $M = (I - W)(I - W)^T$, then $J(Y) = tr(YMY^T)$. Then, we can get the new data sample Y after dimension reduction.

To sum up, the specific flow of the LLE algorithm is shown as follows:

Input: sample set $D = x_1, x_2, \ldots, x_m$

The nearest neighbor parameter k

After dimension reduction, the dimension of space d

Process:

For $i = 1, 2, \ldots, m$ do

Calculate k-nearest neighbors of x_i

Calculate reconstruction coefficient $w_i j$

End for

Obtain the correlation matrix M

Eigen decomposition of matrix M

Returns the eigenvectors corresponding to the minimum d eigenvalues of a matrix

Output: the sample after dimension reduction of the original sample set d

5.2. Data Index Collection and Processing. In order to eliminate the impact of the indicator units and make each indicator have the same impact on the calculation results, it is necessary to standardize the collected network security related indicator data.

Standardization can remove the restrictions of different units and scales between data; that is, different data are scaled as a whole according to a unified scale and converted into pure values in a specific interval. Generally, the min-max standardization method is used to map the original data to [0, 1] interval. For example, a standardized transformation of (11) is carried out for a certain index data as follows:

$$y_i = \frac{x_i - \min_{1 \le j \le n} \{x_j\}}{\max_{1 \le j \le n} \{x_j\} - \min_{1 \le j \le n} \{x_j\}}. \tag{11}$$

So, the new sequence $y_1, y_2, \ldots, y_n \in [0, 1]$ is obtained by calculation and is nondimensional, where $\max_{1 \le j \le n} \{x_j\}$ is the maximum value of the original data and $\min_{1 \le j \le n} \{x_j\}$ is the minimum value of the original data.

5.3. The Construction of Risk Measurement Model of Network Behavior. The change of network security state is a function of the change of network metrics over time. Under the condition of function representation, a set of C^r compatible

total covers can be found in the network topological manifold and the network topological manifold can be constructed as a network differential manifold. In the network differential manifold, we only need to give the corresponding Riemannian metric, and then we can use the differential manifold theory to measure the network behavior risk.

For n-dimensional manifold space, the distance between any two points can be expressed as follows:

$$ds^2 = g_{uv}(x)dx^u dx^v, \tag{12}$$

where $x = (x^1, x^2, \ldots, x^n)$ and g_{uv} is a Riemann metric defined in n-dimensional space. Generally, we choose the Riemann metric with symmetric positive definite, $g_{uv} = g_{vu}$, and then ds^2 is the distance calculation method of two points in n-dimensional space under different Riemann metric.

If we use matrix form to describe Riemannian metric, let $g = g_{uv}$, $x = x^\alpha$, and $dx = dx^\alpha$. Thus, the distance formula (12) can be expressed as follows:

$$ds^2 = dx^T g dx. \tag{13}$$

For a given symmetric positive definite Riemannian metric matrix g, we can decompose it that is, $g = h^T h$, where h and g are of the same order. Then,

$$ds^2 = dx^T g dx = (hdx)^T (hdx) = |hdx|^2. \tag{14}$$

In other words, the distance is converted into the module length of hdx. Then, the matrix h just describes the local local coordinate system. The vector dx in this coordinate system h is equivalent to the vector hdx in the local rectangular coordinate system. At this time, h becomes the Jacobian matrix under coordinate transformation.

5.4. Network Behavior Risk Calculation. Because there is no concept of measure in differential manifold in the process of using differential manifold to measure network security, it is necessary to give Riemannian measure g on differential manifold, so that the behavior risk value of network can be calculated through differential manifold. The Riemannian metric g selected in this study is as follows:

$$g_{uv} = \begin{cases} e^{\left(x_u^2 + x_V^2\right)}/2 & u = v, \\ 0 & u \neq v, \end{cases} \tag{15}$$

where x_u and x_v are the coordinates of point u and point v, respectively. After the Riemannian metric is determined, the corresponding geometric quantity can be given on it. For any vector $A = (a_1, a_2, \ldots, a_n)$ in a Riemannian manifold, the module length of the vector can be expressed as follows:

$$\begin{aligned} |\hbar A| &= \sqrt{(\hbar A)^T (\hbar A)} = \sqrt{A^T \hbar^T \hbar A} \\ &= \sqrt{A^T g A} = \sqrt{\sum_{u=1}^{n} g_{uu} a_u^2}, \end{aligned} \tag{16}$$

For any vector A and any vector B in a manifold, their inner product in a Riemannian manifold can be expressed as follows:

$$(\hbar A)^T (\hbar B) = A^T \hbar^T \hbar B = A^T g B. \tag{17}$$

It can be seen from Section 4.5 that the network behavior risk result can be expressed by the hypervolume of the high-dimensional data manifold formed by the network security index.

Formula (15) has given the selected Riemannian manifold. Combined with the differential manifold structure of the network system, it can be seen that in the Riemannian manifold, the volume element of the data manifold can be expressed as follows:

$$\begin{aligned} \det(\hbar) \prod_u dx^u &= \sqrt{\det\left(\hat{h}^T \hbar\right)} \prod_u dx^u \\ &= \sqrt{\det(g)} \prod_u dx^u \\ &= \sqrt{\det(g)} d\Omega, \end{aligned} \tag{18}$$

where g is the selected Riemannian metric in Riemannian manifold and $\sqrt{\det(g)}$ represents the volume scaling factor of Riemannian manifold space relative to Euclidean space. Given n vectors $A^1, A^2, \ldots, A^n$ in a manifold, the super volume composed of these vectors can be expressed as follows:

$$R = \int \Omega \sqrt{\det(g)} \mathrm{d}\Omega. \tag{19}$$

According to formula (19), we can get the network behavior risk measurement value, which can be used to evaluate the network risk quantitatively and judge the security state of the network.

6. Experimental Design and Analysis

6.1. Small-Scale Network Environment Experiment. In order to verify the effectiveness of the measurement method, this study builds a network environment to simulate DoS attacks. First, we set up an experimental environment and then collect the experimental data. Finally, we use the proposed model method to calculate and draw the conclusion. In order to simulate the attack, four attackers are set up in the network system to simulate DoS attacks of different scales. The attack traffic enters the internal network from the firewall and attacks the internal network through the router $R1$, as shown in Figure 5. This study uses LOIC attack to simulate DoS attack and Wireshark to collect data index.

The experimental design process based on real small environment is as follows: (1) Collection and pretreatment of indicators. Wireshark tool is used to collect data indicators and preprocess them. (2) Calculate the network benchmark security value, namely, network security baseline. (3) Calculate the network risk value under different DoS attack scales. (4) According to the calculated network benchmark

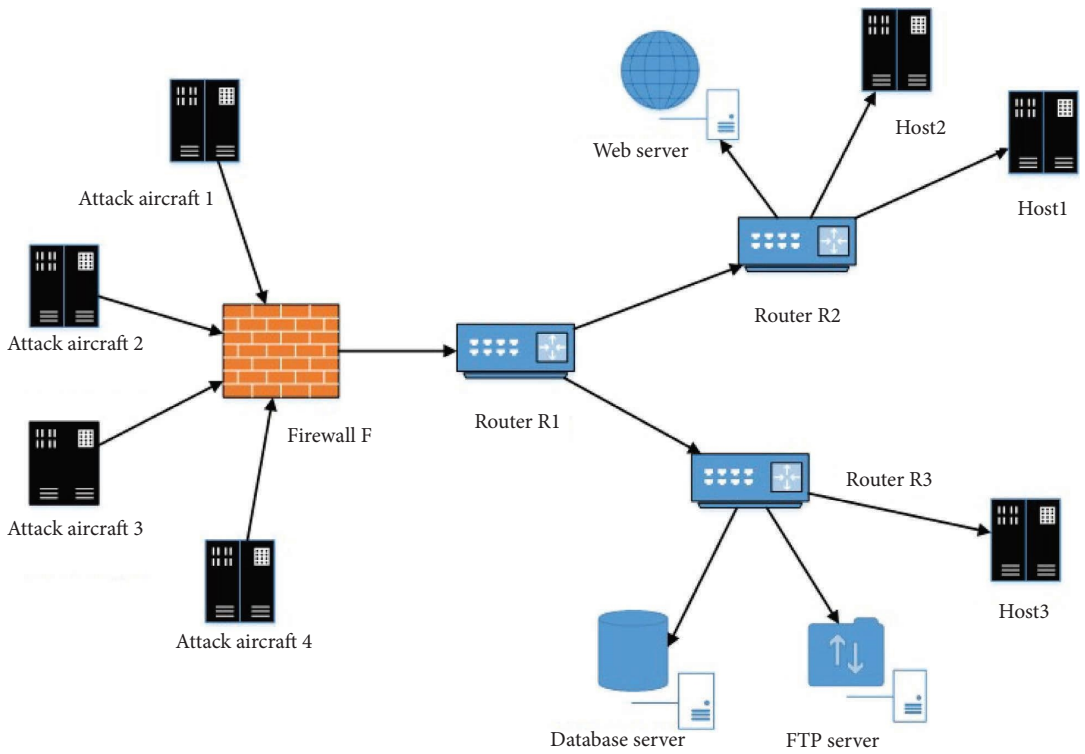

Figure 5: Network environment topology.

security value and network security risk value, the effectiveness of the measurement method is judged.

The calculation process and results are as follows:

(1) Construct the network index state matrix

Collect the data in a certain period of time to form the network index state matrix.

(2) Index pretreatment

For the collected data, the data are standardized and converted into dimensionless pure values between [0, 1].

$$S = \begin{bmatrix} 0.11 & 0.40 & 0 & 0.03 & 0.34 & 0.07 \\ 0.02 & 0.40 & 0.14 & 0 & 0.68 & 0 \\ 0.12 & 0.40 & 0.01 & 0 & 0.59 & 0 \\ 0.12 & 0.40 & 0.02 & 0.02 & 1 & 0.05 \\ 0.21 & 0.07 & 0.02 & 0.06 & 0.63 & 0.04 \\ 0.11 & 0.70 & 0.02 & 0 & 0.81 & 0 \end{bmatrix}. \quad (20)$$

(3) Construct the network Riemannian metric

$$g_{uv} = \begin{cases} e^{\left(x_u^2 + x_V^2\right)/2} & u = v, \\ 0 & u \neq v. \end{cases} \quad (21)$$

In this case, the Riemannian metric matrix under the above network state matrix S' is expressed as follows:

$$G = \begin{bmatrix} 1.01 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1.17 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1.49 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (22)$$

(4) Calculate the volume scaling factor

Firstly, the volume scaling factor of Riemannian manifold relative to Euclidean space is calculated. It can be seen from the above that if the currently selected Riemannian metric matrix is G, the determinant of Riemannian metric matrix can be obtained as $A = |G| = 1.76$. Therefore, the volume scaling factor of Riemannian manifold relative to Euclidean space is 1.33.

(5) Calculate the network security baseline

In the Riemannian manifold of data matrix, the volume element can be expressed as follows:

$$\det(\hbar) \prod_u dx^u = \sqrt{\det(G)} d\Omega = 1.33 d\Omega. \quad (23)$$

Then, the super volume of index data manifold is as follows:

$$R = \int \Omega \sqrt{\det(G)} d\Omega = 1.33 \int \Omega d\Omega = 2.905. \quad (24)$$

From the above, it can be seen that in the small network environment when the network is running normally, the network security benchmark result is 2.905. Using the same calculation method, we can calculate the network security risk value of DoS attack under different scales, as shown in Table 4.

6.2. CIC Open Data Set Experiment. In order to explain the accuracy of the network behavior measurement method based on differential manifold, this study analyzes the CIC-IDS-2017 public data set [36] and draws a conclusion by comparing the calculation results of the open data set on Monday and other time periods. CIC-IDS-2017 data set builds abstract behaviors of 25 users based on HTTP, FTP, and other protocols, including common attacks and traffic analysis results [36]. This study calculates the network behavior risk value based on the attack data from Tuesday to Friday, compares the network security benchmark value under normal conditions on Monday, and draws a conclusion.

The experimental design process based on CIC public data set is as follows: (1) Collection of indicators. Each group of data of the same data tag is collected to form a number of index matrix V_i. Then, the new index state matrix V_i' is obtained by preprocessing and dimensionality reduction. (2) Calculate network benchmark security value. The data set on Monday is the index data collected for normal operation, and the index state matrix of normal data after dimensionality reduction is set as V_1' and the network benchmark security value is calculated. (3) Calculate the network security risk value under each attack. The dataset collected data from Tuesday to Friday, including DoS attack, Heartbleed attack, Web attack, and other types of attacks. Analyze the index state matrix $V_i'(i = 2, 3, \ldots)$ of these attacks and calculate the corresponding network security risk values, respectively. (4) According to the calculated network benchmark security value and network security risk value, judge the network security state in the attack period and draw a conclusion.

The experimental results are as follows.

In CIC data set, Monday is normal data and the collection time is 8:55–10:27, a total of more than 500000 sets of data and a total of more than 80 indicators. After calculation, the network benchmark security value is 0.17. The experimental results are shown in Table 5.

6.3. Experimental Analysis and Conclusion. For the small physical network environment, the experimental verification shows that the network security benchmark value is 2.905 when the network is running normally. In addition, the network security risk value after DoS attack is greater than 2.905 and the risk multiple is about 3 times. It indicates that the current network is under external attack, and the network is in an insecure situation. This is exactly the same as the actual situation. Based on the experimental verification of small-scale network environment, the security status values of the network in the normal state, the first DoS attack, and the second DoS attack are compared, which shows the effectiveness of the model method proposed in this study.

Table 4: Network security risk calculation results.

Operation status	Security risk value
Normal operation	2.905
The first DoS attack	8.053
The second DoS attack	9.976

As shown in Figure 6, the normal fluctuation range of network risk is set between (0, 0.32) that is, the network security risk baseline is set to 0.32. As can be seen from Figure 6, the network security state calculated by the network behavior risk measurement method based on differential manifold is basically consistent with the attack tag given in CIC-IDS-2017. By comparing the calculation results of network activity risk under normal conditions on Monday and from Tuesday to Friday, it can be seen that the network behavior risk measurement method based on differential manifold proposed in this study is basically effective and can detect most of the network attacks, which proves the effectiveness of the network behavior risk measurement method based on differential manifold.

Furthermore, we use differential manifold to illustrate the accuracy of behavior risk measurement (BRM). In Section 6.2, we used BRM and several traditional measurement methods based on machine learning to measure the risk of CIC open dataset. We use the following three common information retrieval evaluation indicators: precision (PR) is the proportion of the number of positive instances correctly classified to the number of instances classified as positive instances; recall (RC) is the proportion of the predicted number of all positive samples in the data set to all positive samples; F-measure ($F1$) is a weighted harmonic average of accuracy rate and recall rate. In addition, the execution time of the test process is calculated and displayed in Table 6. The result of the comparison between several mentioned machine learning methods in reference [37] and BRM is shown in Table 6. We can observe that the execution time of KNN is 1908.23 seconds which is the slowest, while that of BRM is 226 seconds. According to the weighted average of the three evaluation indexes PR, RC, and $F1$, the BRM algorithm has a high accuracy. In addition, these traditional machine learning measurement methods rely on a large amount of data training in the test process. By comparing the accuracy, recall rate, and execution time of the measurement methods, the performance of the proposed method is better than that of some measurement methods based on machine learning, that further proves the accuracy of the model method in this study.

In CIC-IDS-2017 dataset experiment, this study proposes a network behavior risk measurement method based on differential manifold which has limitations under SSH attack and BOT attack. Compared with other attacks, the fluctuation of network security risk under SSH

Table 5: Experimental result.

Time	Attack type	Network security risk value
Monday	Nothing	0.17
Tuesday	FTP attack	25.9
	SSH attack	0.297
Wednesday	DoS slowhttptest attack	4.15
	DoS slowloris attack	1.44
	DoS goldeye attack	0.63
	Heartbleed attack	72.9
Thursday	XSS attack	53
	Sql injection attack	98.3
	Brute force attack	53.7
	Infiltration attack	267
Friday	Bot attack	0
	DDoS attack	0.403
	Portscan attack	0.582

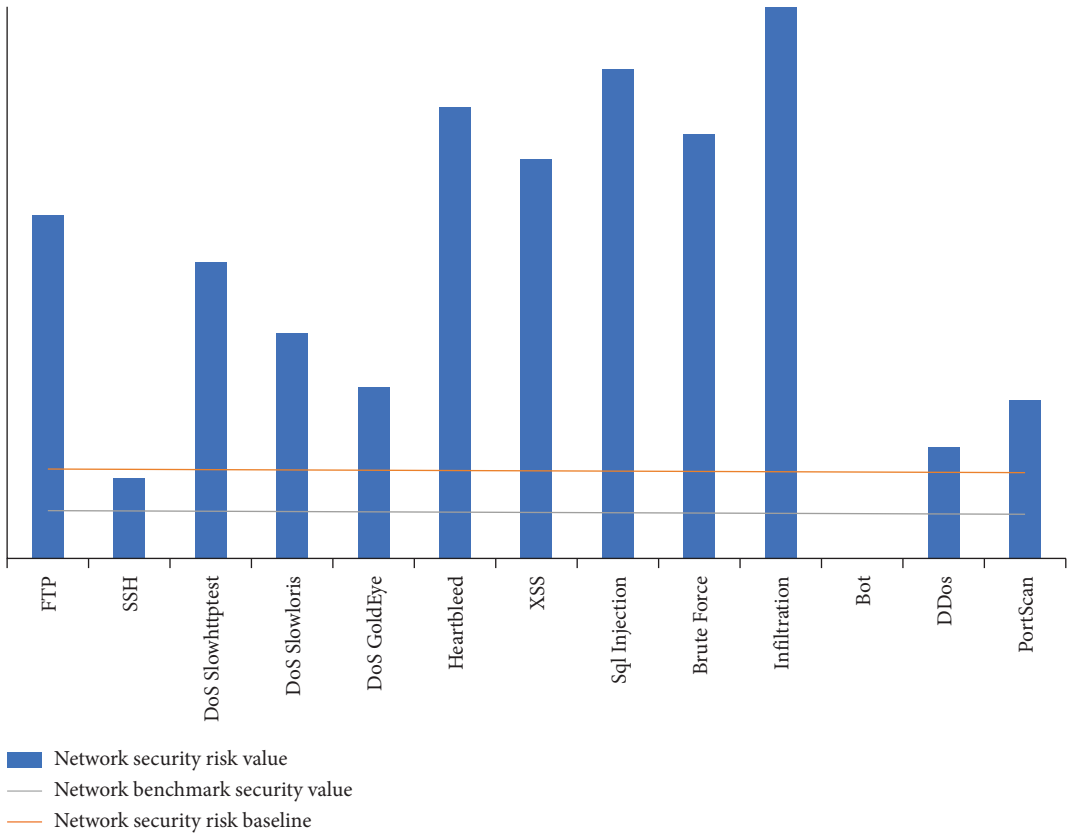

Figure 6: Comparison of network security results under various attacks.

Table 6: Comparison table of various network security measurement methods.

Common methods	Pr	Rc	$F1$	Execution time (s)
KNN	0.96	0.96	0.96	1908.23
RF	0.98	0.97	0.97	74.39
AdaBoost	0.77	0.84	0.77	1126.24
MLP	0.77	0.83	0.76	575.73
Naïve Bayes	0.88	0.04	0.04	14.77
QDA	0.97	0.88	0.92	18.79
ID3	0.98	0.98	0.98	235.02
BRM	0.85	0.85	0.85	226

attack is small and the calculated network risk value is also small. BOT attacks are malicious code that invades the network. BOT attacks on the network are difficult to detect, and the attack characteristics are not obvious enough.

7. Conclusion

This study measures the network behavior risk based on the traffic analysis, regards the network traffic data as the network behavior, depicts the network system as a differential manifold, determines the network risk measurement index group, collects the network operation index data for preprocessing, and uses the differential manifold theory to calculate the security benchmark value under the normal operation of the network and the network security risk value under the attack, and draw a conclusion by comparison. Finally, the proposed method is verified by comparative experiments.

The following three aspects are focused on this study: (1) Regard network traffic as network behavior and propose the definition and measurement method of network behavior risk. Through traffic analysis, carry out risk measurement and realize the quantitative analysis of network behavior. (2) Use the local linear embedding dimension reduction algorithm of manifold learning to reduce the dimension of the index. (3) Apply the differential manifold theory to network security measurement. With the help of differential manifold theory, the description of the security state of the whole network system can be transformed into the change of the state in the high-dimensional manifold composed of network indicators, and then the network security activities are abstracted in the high-dimensional space to calculate the network behavior risk value.

This study focuses on the method of measuring network behavior risk by differential manifold but still has some limitations including (1) When it comes to the measurement of the network security, less attention is paid to the measurement of other indicators such as the vulnerability of the network itself, while more attention is paid to the drastic changes of indicators in network attack and defense. The follow-up research needs to add the measurement of assets and network vulnerability on the basis of the existing network activity measurement. (2) Use the dimension reduction method of local linear embedding to reduce the dimension of data. The performance of the local linear embedding algorithm mainly depends on the selection of nearest neighbor number. A large number of nearest neighbors will cause the smoothness of manifold, and too few nearest neighbors may divide disjointed submanifolds. The subsequent research on dimension reduction parameters can optimize the measurement method and improve the measurement accuracy.

Data Availability

CIC-IDS-2017 public data set is provided by Canadian Institute of cyber security.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank for CIC-IDS-2017 public data set provided by Canadian Institute of cyber security. This work was supported by the National Key Research & Development Program of China (2020YFB1712104) and Major Scientific and Technological Innovation Projects of Shandong Province (2020CXGC010116).

References

[1] G. Wang, H. Zhang, and D. Chen, "Risk analysis of network security," *Modern Computer*, vol. 8, pp. 46–48, 2001.

[2] J. Wang, K. Fan, W. Mo, and D. Xu, "A method for information security risk assessment based on the dynamic bayesian network," in *Proceedings of the 2016 International Conference on Networking and Network Applications (NaNA)*, pp. 279–283, IEEE, Hakodate, Japan, June, 2016.

[3] Y. Yang, "Ddos attack detection of internet of things based on traffic (in Chinese)," Master's Thesis, Beijing Jiaotong University, 2020.

[4] L. Hu, H. Li, Z. Wei, S. Dong, and Z. Zhang, "Summary of research on it network and industrial control network security assessment," in *Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 1203–1210, IEEE, Chengdu, China, March, 2019.

[5] X. Lei, T. Ma, Z. Niu, C. Ma, and H. Shan, "Research on ad hoc network security risk assessment method," in *Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, vol. 1, pp. 2272–2279, IEEE, Chongqing, China, June, 2020.

[6] Y. Ye, L. Yan, W. Sun, Q. Zhang, and N. Wang, "Discussion on risk assessment of network security management," in *Proceedings of the 2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, pp. 409–411, IEEE, Changsha, China, February, 2018.

[7] A. Ramos, M. Lazar, R. H. Filho, and J. Rodrigues, "Model-based quantitative network security metrics: a survey," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 2704–2734, 2017.

[8] L. Yu, Y. Sheng, and Z. Pan, "Hierarchical quantitative evaluation of vulnerability exploitability," in *Proceedings of the 2018 Eighth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, pp. 115–118, IEEE, Harbin, China, June, 2018.

[9] J. David and C. Thomas, "Efficient ddos flood attack detection using dynamic thresholding on flow-based network traffic," *Computers and Security*, vol. 82, pp. 284–295, 2019.

[10] Z. Liu, C. Hu, and C. Shan, "Riemannian manifold on stream data: Fourier transform and entropy-based ddos attacks detection method," *Computers and Security*, vol. 109, no. 10, Article ID 102392, 2021.

[11] M. Di Penta and D. A. Tamburri, "Combining quantitative and qualitative studies in empirical software engineering research," in *Proceedings of the 2017 IEEE/ACM 39th International Conference on Software Engineering Companion*

(ICSE-C), pp. 499-500, IEEE, Buenos Aires, Argentina, May, 2017.

[12] M. Sheng, H. Liu, X. Yang, W. Wang, J. Huang, and B. Wang, "Network security situation prediction in software defined networking data plane," in *Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, pp. 475–479, IEEE, Dalian, China, August, 2020.

[13] J. Wang, N. Zeng, and Z. Hu, "Research on information security risk assessment of computer network based on gray analytic hierarchy process," in *Proceedings of the 2017 International Conference on Computer Technology, Electronics and Communication (ICCTEC)*, pp. 1429–1434, IEEE, Dalian, China, December, 2017.

[14] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proceedings of the 1998 Workshop on New Security Paradigms*, pp. 71–79, Charlottsville, VA, USA, September, 1998.

[15] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using bayesian attack graphs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74, 2012.

[16] S. Zavrak and M. Iskefiyeli, "Anomaly-based intrusion detection from network flow features using variational autoencoder," *IEEE Access*, vol. 8, no. 99, pp. 108346–108 358, 2020.

[17] E. Biersack, C. Callegari, and M. Matijasevic, "Data traffic monitoring and analysis: from measurement, classification, and anomaly detection to quality of experience," *Lecture Notes in Computer Science*, vol. 5, no. 23, pp. 12561–12570, 2013.

[18] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in *Proceedings of the 2017 International Conference on Information Networking (ICOIN)*, pp. 712–717, IEEE, Jeju Island, Korea, January, 2017.

[19] N. Marir, H. Wang, G. Feng, B. Li, and M. Jia, "Distributed abnormal behavior detection approach based on deep belief network and ensemble svm using spark," *IEEE Access*, vol. 6, pp. 59 657–659 671, 2018.

[20] A. Shubair, S. Ramadass, and A. A. Altyeb, "kenfis: knn-based evolving neuro-fuzzy inference system for computer worms detection," *Journal of Intelligent and Fuzzy Systems*, vol. 26, no. 4, pp. 1893–1908, 2014.

[21] X. Zhao, Y. Zhang, J. Xue, C. Shan, and Z. Liu, "Research on network risk evaluation method based on a differential manifold," *IEEE Access*, vol. 8, pp. 66 315–366 326, 2020.

[22] C. Hu, "Calculation of the behavior utility of a network system: conception and principle," *Engineering*, vol. 4, no. 1, pp. 78–84, 2018.

[23] Z. Hao, *Research on nonlinear dimensionality reduction method based on differential manifold*, Shanghai University, Ph.D. dissertation, 2016.

[24] X. Mei and L. He, *Differential Manifolds and Riemannian Geometry*, (in chinese), Differential Manifolds and Riemannian Geometry, Gulf Professional Publishing, Houston, TX, USA, 1987.

[25] L. Wang, "Application of discriminative manifold learning algorithm in face recognition (in Chinese)," Master's Thesis, Chongqing University, 2009.

[26] B. C. Hall, *Lie Groups, Lie Algebras, and Representations*, Springer Science and Business Media, Berlin, Germany, 2013.

[27] X. Zhao, X. Jiang, J. Zhao, H. Xu, and J. Guo, "Measurement method of network attack and defense effectiveness based on differential manifold," *Journal of Tsinghua University: Natural Science Edition*, vol. 60, no. 5, p. 6, 2020.

[28] C. Hu, Z. Liu, C. Shan, X. Zhao, and S. Guo, *Construction Method of Network State Model and State Evaluation Method Based on Differential Manifold*, 2018.

[29] S. Zhao, C. Wu, W. Xie, Z. Jia, H. Wang, and Y. Zhang, "Research on network security measurement based on attack graph," *Journal of Information Security*, vol. 4, no. 1, pp. 53–67, 2019.

[30] C. Barakat, P. Thiran, G. Iannaccone, C. Diot, and P. Owezarski, "Modeling internet backbone traffic at the flow level," *IEEE Transactions on Signal Processing*, vol. 51, no. 8, pp. 2111–2124, 2003.

[31] W. Chen, *Preliminary of Differential Manifold*, Higher Education Press, Beijing, China, 1998.

[32] Z. Bai, "Preliminary of riemannian geometry," in *Geometric Analysis of Quasilinear Inequalities on Complete Manifolds*, Springer Science and Business Media, Berlin, Germany, 2nd edition, 2004.

[33] L. Hayden, *It Security Metrics a Practical Framework for Measuring Security and Protecting Data*, McGraw-Hill Education Group, New York, NY, USA, 2010.

[34] R. Henning, M. Abrams, J. Kahn et al., "Information system security attribute quantification or ordering," in *Workshop on Information Security System Scoring and Ranking*, pp. 1–70, 2002.

[35] L. Lin and C. Liu, "Research on key technologies of internet risk assessmen," *t Network Security Technology and Application*, vol. 4, p. 14, 2017.

[36] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, *Intrusion Detection Evaluation Dataset (Cic-ids2017)*, Proceedings of the of Canadian Institute for Cybersecurity, Fredericton, New Brunswick, 2018.

[37] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proceedings of the International Conference on Information Systems Security and Privacy*, vol. 1, pp. 108–116, Copenhagen, Denmark, February, 2018.