Hindawi
Security and Communication Networks
Volume 2023, Article ID 9827541, 1 page
https://doi.org/10.1155/2023/9827541

Retraction

Retracted: Design of Network Intrusion Detection Model Based on TCA

Security and Communication Networks

Received 26 December 2023; Accepted 26 December 2023; Published 29 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Q. Wen, “Design of Network Intrusion Detection Model Based on TCA,” *Security and Communication Networks*, vol. 2022, Article ID 9248853, 6 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 9248853, 6 pages
https://doi.org/10.1155/2022/9248853

WILEY | Hindawi

Research Article

Design of Network Intrusion Detection Model Based on TCA

Quan Wen

College of Computer Science and Cyber Security (CSCS), Chengdu University of Technology, Chengdu 610059, China

Correspondence should be addressed to Quan Wen; wenq@cdut.edu.cn

Received 25 April 2022; Accepted 25 May 2022; Published 7 July 2022

Academic Editor: Hangjun Che

The traditional machine learning model cannot effectively identify the new network traffic data set, resulting in the model failure. Therefore, in this paper, by analyzing the problems of current network intrusion detection (NID) and combining the application of transfer theory in the detection model, a NID model based on transfer component analysis (TCA) is proposed. Among them, the specific mathematical derivation of the algorithm and the detection process of transfer model are introduced in detail. Then, the classification performance of KNN and SVM based on TCA algorithm for network abnormal traffic is compared. The results show that the TCA algorithm proposed in this paper can effectively improve the accuracy of NID, which is meaningful to expand the application scope of network abnormal traffic detection scheme based on machine learning.

1. Introduction

With the rapid development of Internet in social life, people's attention to network security has gradually increased, and more network traffic data have brought great challenges to traditional intrusion detection systems. When the traditional machine learning method is used for intrusion detection, it is necessary to extract features manually, then use feature selection method to distinguish the most meaningful features, and finally adopt to discover new threats [1, 2]. In any case, with the rise of new assaults and the changing improvement of assault situations, these techniques for AI are confronted with numerous challenges in building highlights. Various elements chose for realized noxious examples are totally appropriate for obscure or new kinds of vindictive examples, and traditional machine learning needs a lot of manpower and material resources, while deep learning has the characteristics of automatic learning and feature extraction [3–5]. However, the existing neural network can only be used in a closed or static network environment. When performing classification, all possible classes are already known during training; therefore, if unknown classes appear, the existing detection system cannot correctly identify them, which will greatly threaten the network security.

Besides, the abnormal traffic detection schemes based on machine learning all require that the training and testing data sets have the same feature distribution. However, with the diversity and secrecy of network abnormal traffic, the detection based on signature and specification is not reliable. Once the time of traffic collection, the node location, and traffic type change, it cannot identify effectively, when the traditional machine learning model is applied to new network traffic data sets, resulting failure in model [6, 7]. Usually, tag data are difficult to obtain and expensive, and at the same time, numerous expired data are not fully utilized. By introducing the transfer learning theory into the NID system, it can solve the learning problem of the target domain without or with only little labeled data by transferring the knowledge of the source domain and use the original data in the shared subspace to train the basic classifier model and detect the new sample flow [8].

Since the 1980s, NID has been studied. Faced with the ever-changing network attacks and increasing traffic data, the following problems still exist in intrusion detection system.

1.1. *Low Training Efficiency.*

Although the deep learning model can extract advanced abstract features, it also sacrifices computing resources. To extract effective features from large

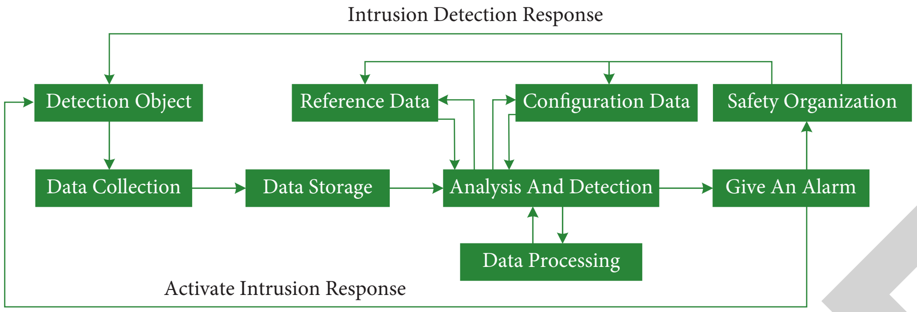

Figure 1: Architecture of the NID system.

and high-dimensional data, it will increase more computational cost and time. Therefore, how to solve the problem of large and high-dimensional data, improve the training efficiency of the model, and ensure the accuracy of the system classifier is particularly important.

1.2. The Real-Time Performance of Intrusion Detection Is Low. Reliable intrusion detection system can quickly identify the network when it is attacked, and network security managers can take corresponding security measures to defend it. This requires high real-time performance of intrusion detection algorithms, but the current intrusion detection algorithms have low real-time performance. When the network is invaded, the network security managers cannot find it in time to intercept it, which attacks the network system. Therefore, it is necessary to solve the real-time problem of intrusion detection algorithm.

1.3. The Detection Rate of Rare Sample Data Is Low. The detection rate of rare attacks is extremely low due to bit of rare attacks. The increase of the number of features and the imbalance of data are the key reasons for the low detection accuracy. If a hacker makes use of a rare attack, the intrusion detection system will have no way to successfully warn or intercept it, thus endangering the security of the network system and causing serious consequences. Therefore, it is necessary to study the problems of multi-classification and data imbalance in intrusion detection.

Therefore, the identification of abnormal network traffic data can effectively support the location of network intrusion behaviors; especially for the discovery of unknown attacks, this paper improves and combines the transfer learning theory in the research of NID, aiming at solving the problems derived from classification in NID, such as scarcity of tags, inconsistent distribution of source and destination data, and difficulty in distinguishing unknown attacks, so as to meet the original intention of pursuing higher accuracy.

2. Analysis of Problems in NID

The process of NID is shown in Figure 1, in which the solid line represents the transmission direction of data and control instructions in the system, and the dotted line represents the reaction of the terminal nodes in the system to possible intrusion.

A universal intrusion detection system is mainly composed of monitoring object, data collection, data storage, data processing, analysis and detection, and alarm modules [9].

Data collection: the data collected at this stage are analyzed to find traces of suspicious activities, which can be host, network activity log, command-based log, application-based log, etc.

Data storage: intrusion detection systems usually store data indefinitely or for a long time for future reference, so the amount of data is usually very large.

Analysis and detection: the processing module is the core of the intrusion detection system where an algorithm for detecting suspicious behavior is executed. Traditionally, intrusion analysis and detection algorithms are divided into three categories: misuse detection, anomaly detection, and hybrid detection.

Configuration data: it is the most delicate piece of interruption location framework. It contains data connected with the activity of interruption location framework itself, for example, data about when and how to gather information, how to manage interruption, and so forth.

Reference data: it stores information about known intrusion signatures or profiles of normal behaviors where knowledge about system behavior can be used to update configuration information.

Alarm: this piece of the framework handles all the result from the interruption recognition framework. The result can be a programmed reaction to the interruption or a suspicious behavior alarm of the system security officer.

In summary, the process of intrusion detection is shown in Figure 2.

The general process of intrusion detection is that first, the detection system collects the required original data from the data source and then preprocesses the data to get the data format that the system can recognize. After identification and detection by the detection engine, the detection result is obtained and the response is made according to the security policy set by the administrator.

3. Implementation of Transfer Learning in NID

The main idea of transfer learning is to apply the trained machine learning model to other related fields. Through transfer learning, the generalization of another task can be improved by the knowledge learned in one task [10, 11].

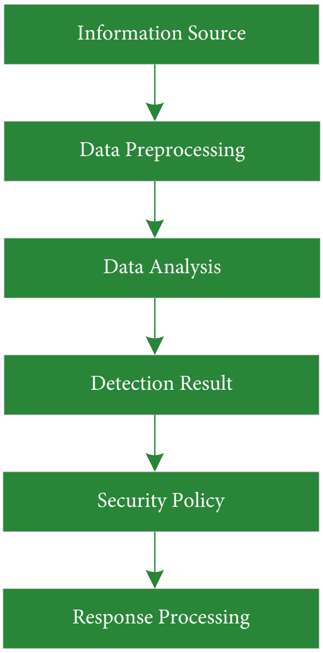

Figure 2: Process of intrusion detection.

The main advantage of learning is that based on a small amount of data, the performance of neural network can be rapidly improved in a short time. Usually, training neural networks from scratch requires numerous data, but in reality, getting such a lot of data is unimaginable all the time. Through move learning, a solid AI model can be worked with moderately little preparation information, in light of the fact that the model has been preprepared. The main implementation mode is shown in Figure 3:

(1) *Adopting the Training Model*. If users want to solve task (A) but there are not enough data to train the neural network, they can find the connected errand B with a ton of information, train the profound neural network on task B, and utilize the model as the beginning stage to tackle (A) while whether the entire model or a couple of layers are required relies upon the issue to be addressed.

(2) *Pretraining Model*. Use trained models, such as nine pretraining models provided in Keras, which can be used for transfer learning, prediction, feature extraction, and fine-tuning.

(3) *Feature Extraction*. With the help of the deep learning training model, the features of the shallow network can be used to show the elements to be learned, that is, the representation of the original data, without using the network output, so that the size of the data set can be reduced, thus reducing the calculation time.

In intrusion detection, the knowledge learned from known network attacks is used to enhance the detection of new network attacks. The source domain (SD) and the TD, respectively, represent the training and testing data sets in machine learning tasks, and both the data include normal and abnormal traffic records. In a generalized scenario, the attacks in the SD are marked, while the attack in the TD is new and unmarked. The purpose of learning in intrusion detection is to use source data to help distinguish new attacks from TDs, as shown in Figure 4.

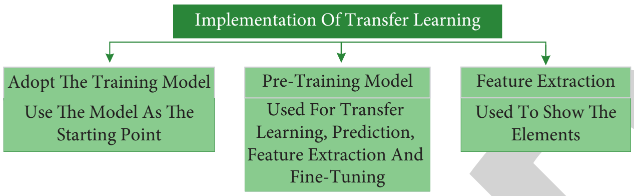
Implementation Of Transfer Learning
Adopt The Training Model
Use The Model As The Starting Point
Pre-Training Model
Used For Transfer Learning, Prediction, Feature Extraction And Fine-Tuning
Feature Extraction
Used To Show The Elements

Figure 3: Implementation of transfer learning.

4. NID Model Based on TCA

4.1. Establishment of the Problem Model. Define the SD network traffic data set with label as $D_S, X_S = \{x_s\}_{s=1}^{n_s} \in R^{m\times n_s}$. As a feature input, the corresponding tag set $Y_S = \{y_s\}_{s=1}^{n_s} \in R^{1\times n_s}$ is set as an output, and a new network traffic data set with different structures is defined as a TD after data preprocessing. $D_T, X_T = \{x_t\}_{t=1}^{n_T} \in R^{m\times n_T}$ is set as a feature input, and the sample label is unknown.

m is the traffic characteristics extracted from the SD and the TD. Considering the edge distribution of SD traffic and TD traffic $P(X_S) \neq Q(X_T)$, the SD model cannot be trained to detect the abnormal traffic in the TD.

The solution of this paper is to find a suitable transformation Φ to make $P(\Phi(X_S)) \approx Q(\Phi(X_T))$, and $P(Y_S|\Phi(X_S)) \approx P(Y_T|\Phi(X_T))$, so that the corresponding labels can be trained $\Phi(X_S)$ and the corresponding label. Y_S can be used to train the data of the TD traffic $\Phi(X_T)$, where the SD traffic data $\Phi(X_S)$ and the classifier trained by the corresponding label matches the TD traffic $\Phi(X_T)$ can used to classify the data and detect the abnormal traffic.

The following two conditions of transformation function Φ must be met:

(1) Minimize the gap between the edge distribution $P(X_S)$ and $Q(X_T)$

(2) Retain the internal attributes of X_S and X_T to the maximum extent possible

Φ is a feature mapping between SD and TD caused by general kernel, while the essence of TCA algorithm is to reduce the distance between the distribution of SD P and target source distribution Q, and the distribution distance of the objective function P and Q is shown in

$$\mathrm{Dist}\left(X_S', X_T'\right) = \left\| \frac{1}{n_1}\sum_{i=1}^{n_1}\Phi\left(x_{s_i}\right) - \frac{1}{n_2}\sum_{i=1}^{n_2}\Phi\left(x_{T_i}\right)\right\|_H^2, \qquad (1)$$

where H is a universal regenerative kernel Hilbert space, Φ is a feature mapping caused by a kernel, X_S' and X_T', respectively, representing the characteristics of the SD traffic and the TD traffic in the transformation space, and n_1 and n_2, respectively, represent the number of samples contained in

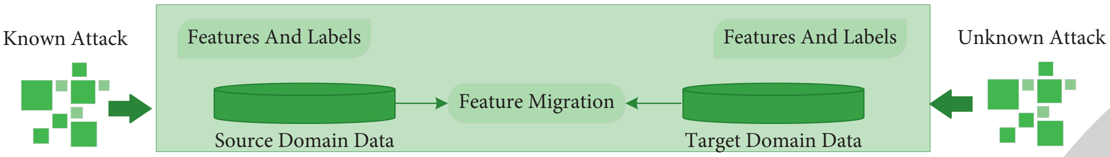

Figure 4: NID based on transfer learning.

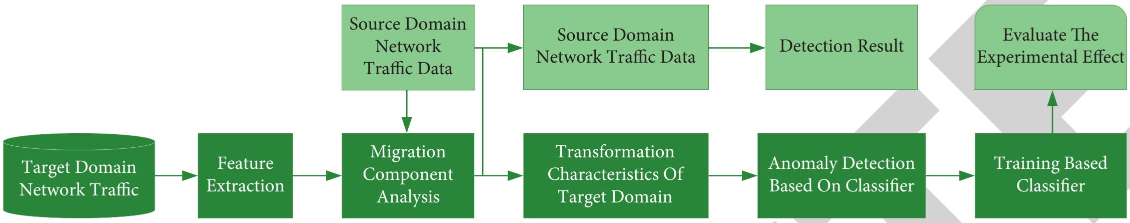
Source Domain Network Traffic Data
Source Domain Network Traffic Data
Detection Result
Evaluate The Experimental Effect
Target Domain Network Traffic
Feature Extraction
Migration Component Analysis
Transformation Characteristics Of Target Domain
Anomaly Detection Based On Classifier
Training Based Classifier

Figure 5: Detection model based on TCA.

each. Therefore, if the conversion function Φ is found, the objective function can be calculated.

It is very difficult to direct explicit definition of nonlinear transformation Φ and calculate the distance between features. Therefore, a kernel matrix K is introduced by using the kernel embedding method, where formula (1) is rewritten as follows:

$$Dist\left(X_S', X_T'\right) = tr\,(KL), \tag{2}$$

where KL represents the distance and is used to measure the difference of probability distribution K of traffic characteristics in different network environments, as shown in

$$K = \begin{bmatrix} K_{SS} & K_{S,T} \\ K_{T,S} & K_{T,T} \end{bmatrix} \in R^{(n_1+n_2)\times(n_1+n_2)}, \tag{3}$$

where $K_{S,S}$, $K_{T,T}$, and $K_{S,T}$ represent the inner core matrix composed of the features of the SD, the TD, and the synthesis domain L, respectively, which are defined as

$$L_{ij} = \begin{cases} \dfrac{1}{n_1^2} & x_i, x_j \in X_S, \\[2ex] \dfrac{1}{n_2^2} & x_i, x_j \in X_T, \\[2ex] -\dfrac{1}{n_1 n_2} & \text{otherwise}, \end{cases} \tag{4}$$

n_1 and n_2, respectively, represent the number of samples contained in each.

Therefore, the distance of the above objective function is transformed into an operation problem between matrices, which is shown in

$$tr\,(KL) - \lambda tr\,(K), \tag{5}$$

where $\lambda \geq 0$ is a trade-off parameter, $tr\,(KL)$ is used to minimize the difference between the distributions of the two fields, and $\lambda tr\,(K)$ is used to maximize the variance of feature space.

As can be seen from the above discussion and definition, formula (5) is a semidefinite programming problem in mathematics, and it takes a lot of time to solve it by general methods. Therefore, the kernel matrix K in formula (3) is reduced by the dimension reduction, which is broken down into $K = (KK^{-1/2})(K^{-1/2}K)$. The final kernel matrix can be expressed by

$$\widetilde{K} = \left(KK^{-1/2}\widetilde{W}\right)\left(\widetilde{W}^T K^{-1/2} K\right) = KWW^T K, \tag{6}$$

where $W = K^{-1/2}\widetilde{W}$. The distance between characteristics of traffic in SD and TD in transformation space X_S' and X_T' can be converted into

$$\text{Dist}\left(X_S', X_T'\right) = \text{tr}\left(\left(KWW^T K\right)L\right) = \text{tr}\left(W^T KLKW\right). \tag{7}$$

Under the minimization rule, the normalization term $\text{tr}\,(W^T W)$ is used to control complexity W, and the final objective function is transformed into

$$\min_W \text{tr}\left(W^T W\right) + \mu \times \text{tr}\left(W^T KLKW\right), \tag{8}$$

where $\mu > 0$ is a trade-off parameter, so that the sample matrix $X^* = KWKW$ in the shared subspace can be calculated. It ensures that the distance between the SD and the TD is reduced, and the mapped data have the largest variance, which satisfies the set of abovementioned transformation function Φ.

To sum up, the working principle of TCA is as follows: the goal of TCA is to find an optimal shared feature subspace, in which the distribution difference between the SD and the TD can be minimized, and then the unlabeled data in the TD can be classified by using the classifier trained in the SD.

4.2. Detection Model. In this paper, KNN, SVM, and RF are used as basic classifiers, and a network abnormal traffic detection model based on TCA is designed as shown in Figure 5. The specific detection process is divided into the following five steps:

(1) Extract network traffic characteristics and corresponding characteristic values of a TD

Table 1: Description of test data set.

Data set	Data sample	Number of categories	Subset
CICIDS2017	16000	12	A, B, C
CTU	11200	11	M, N

(2) Migrate the traffic characteristics and original characteristics of the TD to be identified to the shared subspace

(3) Train the base classifier with SD traffic data in the shared subspace

(4) Adopt the base classifier to detect the features of the TD after traffic transformation

(5) Calculate the detection accuracy, and then evaluate the experimental results

5. Model Test

5.1. Construction of the Data Set. The core problem of this paper is that the SD and the TD do not meet the same feature distribution, so the two domains need to use different data sets. The experimental data sets are CICIDS2017 and CTU, as shown in Table 1, where 10 groups of transfer learning experiments are designed.

CICIDS2017 contains normal traffic and the most common attack traffic at present, and gives pcap file data, in which data files are divided according to different dates, all of which are normal traffic on Monday, and attack traffic is collected from Tuesday to Friday. In this paper, it is found that if the data set contains all kinds of attacks, it is prone to negative transfer. Therefore, according to different types of attacks, CICIDS2017 data set is divided into three subsets: a subset mainly contains DDOS and DOS attacks, B subset contains PortScan, FTP-Patator, and SSH-Patator attacks, C subset contains Web attacks and botnets, and all these subsets contain normal traffic.

CTU data set contains a large number of attack traffic mixed with normal traffic. Similarly, according to different types of attacks, CTU data set is divided into sub-data sets of M and N, of which sub-data set M contains Trickster, TrickBot, and Dridex attacks, and N contains Ursnif, CoinMiner, and HTBot attacks. Similarly, these subsets also contain normal traffic.

5.2. Data Processing. As CICIDS2017 data set and CTU data set are both pcap files, which cannot be directly sent into the model for training, we need to preprocess the pcap files to divide the traffic packets with the same quintuple information into a flow, and mainly use Python script to analyze the remaining header and payload information of each traffic packet and vectorize it. In this way, experiments are carried out on the features that can be extracted from each flow, and the division of network traffic flow can also reflect the time sequence of traffic in NID.

The processing procedure of CICIDS2017 data set and CTU data set is shown in Figure 6.

Mean value removal is to eliminate the deviation between sample features, which is realized by subtracting the mean value of all the feature values of each sample, so as to make the feature mean value zero.

Range scaling is to enlarge or reduce the characteristic values of samples of different units to a reasonable range in proportion, in order to reduce the influence of the large change between different features.

Normalization refers to uniformly scaling the features of different classes to a specified range, and its purpose is to unify the statistical distribution of samples to eliminate the adverse effects caused by singular samples. The most commonly used normalization method in machine learning is L1 norm, which ensures that the data are in the same order of magnitude.

5.3. Parameter Setting. In terms of data, the data sets used in the experiment are all network traffic data, and their distributions are different but related. Attacks in all data sets are uniformly marked as abnormal traffic. This paper conducts two-class detection of normal and abnormal traffic. 4,000 pieces of data are randomly selected from each subset of CICIDS2017 as SD and TD data sets, respectively, which is shown in Table 1. Correspondingly, 3200 pieces of data are randomly selected from each subset of CTU as source and target and data set, respectively.

In the aspect of model, KNN and SVM in machine learning are used as classifiers for tests [12]. In order to control the parameters of experiments, K is uniformly set to 1, the penalty factor C in SVM is equal to $C = 100$, and Gaussian kernel function is adopted where the performance of linear kernel is better than that of RBF and Laplacian kernel, so TCA uses linear kernel function uniformly. In order to avoid overfitting, the experiment was carried out by setting program for 10 times, and the results were obtained by averaging. The main index used to evaluate the effectiveness of traffic classification is the accuracy rate, that is, the percentage of correct traffic classification in total traffic.

5.4. Analysis of Results. Table 2 shows the accuracy of 10 groups of transfer learning data under each model.

It can be seen from the data in the table that in the anomaly detection experiments of 10 groups of cross-domain network traffic data sets, the recognition rate of the TD samples by the traditional machine learning algorithm is very low that the accuracy rate is only about 39%. The main reason is that the distribution difference between the SD traffic characteristics and the TD traffic characteristics is too large to meet the independent and identical distribution rules required by machine learning. In this case, the recognition result can hardly be used as effective reference information, and the TD cannot make use of the valuable tag information in the SD. In addition, the TCA algorithm proposed in this paper is used to adapt the traffic characteristics of SD and TD, and the marginal probability distribution and conditional probability distribution between them are reduced, which can significantly improve the accuracy of detection. Compared with the traditional machine

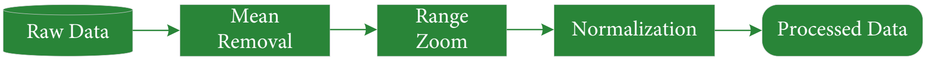

Figure 6: Data processing procedure.

Table 2: Test results of transfer data sets.

Data set	Accuracy (%)			
	KNN	TKNN	SVM	TSVM
A⟶M	36.43	49.57	25.27	50.81
A⟶N	26.95	39.37	47.03	66.35
B⟶M	56.38	69.68	36.60	56.29
B⟶N	27.39	46.21	36.12	50.05
C⟶M	24.90	48.33	49.58	81.97
C⟶N	27.92	62.65	29.81	49.96
M⟶A	31.07	46.94	27.05	42.45
M⟶B	47.77	73.79	48.94	82.52
M⟶C	39.14	57.74	43.29	76.75
N⟶A	49.48	78.16	57.84	89.18
N⟶B	54.09	67.49	40.53	69.15
N⟶C	36.43	63.56	37.78	71.58
Average	38.16	58.62	39.99	65.59

learning algorithm, the accuracy is improved by 20%~25%, up to 89.18%. The feature distributions of CTU and CICIDS2017 are different and do not contain the same attack types, which shows that TCA algorithm improves the detection accuracy and proves the effectiveness and feasibility of the network anomaly detection method based on TCA.

In addition, it can be concluded that the accuracy of SVM classifier after being processed by TCA algorithm is higher than that of KNN, reaching 65.59%, because KNN adopted in this paper is based on Euclidean distance to calculate the difference between different eigenvalues for classification, and TCA algorithm uses the maximum mean difference to reduce the distance between SD features and TD features, which shows that the optimal separation hyperplane found by SVM model in feature space maximizes the interval between positive and negative samples in the TD, and the robustness of anomaly detection is strong.

6. Conclusion

In this paper, the transfer learning theory is introduced into the NID system, and a NID method based on TCA is proposed, in which transfer learning does not require the SD and the TD to obey the same marginal probability distribution or conditional probability distribution. By transferring the knowledge of SD, the problem of learning in TD without or with only a bit of labeled data can be solved. In addition, the original data are used in the shared subspace to train the model with KNN and SVM classifier where the new sample traffic is detected. The results show that the TCA algorithm proposed in this paper can adapt to the characteristics of SD traffic and the TD traffic, thus significantly improving the detection accuracy. The accuracy of SVM classifier after TCA algorithm is higher than KNN, reaching 65.59%, and its robustness in abnormal detection is strong.

Data Availability

The data set can be accessed upon request to the author.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] M. Belouch, S. El Hadaj, and M. Idhammad, “Performance evaluation of intrusion detection based on machine learning using Apache Spark,” *Procedia Computer Science*, vol. 127, pp. 1–6, 2018.

[2] W. Wang, “Research on Network Traffic Classification and Anomaly Detection Method Based on Deep Learning,” *Hefei: University of Science and Technology of China*, vol. 12, 2018.

[3] L. Lixin Duan, I. W. Tsang, and D. Dong Xu, “Domain transfer multiple kernel learning,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 34, no. 3, pp. 465–479, 2012.

[4] S. Qing and J. Jiang, “Survey of intrusion detection technology,” *Journal of Cooperation in Economy and Technology*, vol. 25, no. 7, pp. 19–29, 2004, (in Chinese).

[5] J. Liu, *Research on Key Technologies of NID*, Donghua University, Shanghai, pp. 23–25, 2013, (in Chinese).

[6] C. Yin, Y. Zhu, J. Fei, and X. He, “A deep learning approach for intrusion detection using recurrent neural networks,” *IEEE Access*, vol. 5, no. 99, pp. 21954–21961, 2017.

[7] W. Zhong, N. Yu, and C. Ai, “Applying big data based deep learning system to intrusion detection,” *Big Data Mining and Analytics*, vol. 3, no. 3, pp. 181–195, 2020.

[8] Y. Zhang, Y. Zhang, N. Zhang, and M. Xiao, “A network intrusion detection method based on deep learning with higher accuracy,” *Procedia Computer Science*, vol. 174, pp. 50–54, 2020.

[9] W. li and Z. Yang, “Research summary of intrusion detection system,” *Journal of Jilin University (Earth Science Edition)*, vol. 34, no. 5, pp. 657–662, 2016.

[10] F. Zhuang, P. Luo, and Q. He, “Research progress of transfer learning,” *Journal of Software*, vol. 26, no. 1, pp. 26–39, 2015, (in Chinese).

[11] J. Zhao, S. Shetty, J. W. Pan, C. Kamhoua, and K. Kwiat, “Transfer learning for detecting unknown network attacks,” *EURASIP Journal on Information Security*, vol. 2019, no. 1, p. 1, 2019.

[12] M. Cai, *Classification and Application of Unbalanced Data by Improved Weighted KNN Algorithm Based on SVM*, Anhui University, Anhui, 2020.