Detection Method of Large Industrial CT Data Transmission Information Anomaly Based on Association Rules

Xiafu Pan[1] and Chun Zheng[2](✉)

[1] Department of Public Safety Technology, Hainan Vocational College of Political Science and Law, Haikou 571100, China
[2] Anhui Sanlian University, Hefei 230601, China
zhenghaha020@163.com

Abstract. In the abnormal detection of large industrial CT data transmission information, the network is unstable and vulnerable to noise interference, resulting in the unstable output energy of the ray source, making the detection accuracy of data transmission information abnormal low. To solve this problem, a large industrial CT data transmission information anomaly detection method based on association rules is designed. Through association rule mining algorithm, the data transmission information of large-scale industrial CT is analyzed, and the association rules are obtained by introducing interest threshold. The improved Apriori algorithm is adopted to improve the accuracy of association rule mining. According to the results of association rule mining, the nonlinear wavelet transform threshold denoising algorithm based on the improved threshold function is used to denoise the information data. By calculating the abnormal probability of information entropy in data flow and sliding window, the abnormal detection of data transmission information is realized. Experimental results show that the proposed method has high detection accuracy and short average anomaly detection time.

Keywords: Association Rules · Large Industrial CT · Data Transmission Information · Wavelet Basis Function · Anomaly Detection

1 Introduction

Large-scale industrial X-CT is a nondestructive testing technology, which is regarded as one of the best nondestructive testing means, and has wide application prospects in aviation, spaceflight, national defense, machinery, electronics, petroleum and electric power. With the development of science and technology, people have higher requirements for nondestructive testing technology. Especially for some large workpieces such as rails, railway axles, etc., because of its higher technological requirements and larger volume, so its detection accuracy, detection of the maximum diameter, detection speed, etc. [1]. Such trends have led to the increase in the number of channels and acquisition speed of the detector to collect and detect rays, and the amount of data to be processed and

B. Wang et al. (Eds.): ICMTEL 2023, LNICST 534, pp. 79–91, 2024.
https://doi.org/10.1007/978-3-031-50577-5_7

transmitted to the upper computer has increased exponentially; at the same time, because the user requires that the distance between the upper computer and the CT is getting farther and farther when using large industrial CT, it is necessary to find a way to balance the contradiction between the speed and distance of industrial CT in data transmission, and also need to consider the complexity and cost of the system[2].

The data transmission system transfers the data to the upper computer through the data bus interface such as PCI, USB or ARM FPGA. These transfers are often restricted by the transmission distance. However, there are few practical applications of data transmission through network interface, which can overcome the limitation of transmission distance, and the network transmission protocol is universal and reliable.

In this data transmission mode, there are some hidden troubles, such as monitoring, interference, data forgery and so on. At the same time, the network is unstable and vulnerable to interference. Therefore, the anomaly detection of large-scale industrial CT data transmission information is an important security issue to be solved, which has great practical significance.

The anomaly detection of large-scale industrial CT data transmission has its particularity compared with network data anomaly detection. At present, the research on anomaly detection of large-scale industrial CT data transmission is less, and it has more practical value to study the comprehensive anomaly detection method.

In the current research, foreign researchers have more experience in the research and application of this problem, and have given some more comprehensive anomaly detection schemes. Reference [3] proposed an anomaly detection method based on SVM. Firstly, the essential concepts of SVM classifier and intrusion detection system are introduced. Then the ADS methods are classified, and various machine learning and artificial intelligence technologies are discussed. These technologies are combined with SVM classifier to detect exceptions. In addition, it defines the main capabilities, possible limitations or advantages of the ADS method. In addition, the ADS schemes studied are compared to illustrate their various technical details. Reference [4] proposed a multi-scale attention memory automatic coding network for anomaly detection - MAMA network. First, in order to overcome a series of problems caused by the limited fixed receptive field of the convolution operator, a multi-scale global spatial attention block is proposed, which can be directly inserted into any network as the sampling, up sampling and down sampling functions. Because of its efficient feature representation capability, the network can obtain competitive results with only a few level blocks. Secondly, due to the lack of constraints in the training and reasoning process, the traditional automatic coder can only learn the fuzzy model, which can also reconstruct the anomaly well. In order to alleviate this challenge, a hash addressing memory module is designed, which can prove the abnormal situation, thus generating higher classification and reconstruction error. In addition, the mean square error (MSE) is coupled with Wasserstein loss to improve the distribution of coded data. Experiments on various data sets, including two different COVID-19 data sets and one brain MRI (rider) data set, prove the robustness and good generalization of the proposed Mama network.

With the deepening of the understanding of large-scale industrial CT, domestic researchers have also carried out related research, but more research focuses on data transmission method optimization and scheduling. But with the development of large-scale industrial CT, abnormal detection of data transmission information is crucial, just like the firewall to the computer. Therefore, a number of well-known industrial enterprises established a research group, engaged in research in this area, and have introduced some anomaly detection programs. Referring to the present research contents, this paper designs an anomaly detection method based on association rules for large-scale industrial CT data transmission. The association rule mining algorithm is used to analyze the data transmission information of large-scale industrial CT. According to the joint rule mining results, the nonlinear wavelet transform threshold denoising algorithm based on the improved threshold function is used to de-noise the mining data information. The anomaly detection of data transmission information is realized by calculating the anomaly probability of data flow. The experimental results show that the proposed method can achieve high precision detection.

2 Abnormality Detection of Large Industrial CT Data Transmission Information

2.1 Correlation Analysis

Association rules mining algorithm is used to implement association analysis of large industrial CT data transmission information. Apriori algorithm is a classical association rule mining algorithm, which can mine meaningful association rules from massive data according to support and confidence, but its I/O load is high and time efficiency is low. In fact, the Apriori algorithm still has the problem of whether the association rules mined are really useful to users. Aiming at the problem that Apriori algorithm may generate inappropriate strong association rules, this paper improves the algorithm by introducing interest threshold to mine valuable strong association rules.

The degree of interest describes the degree of correlation between itemset A and itemset B in rule $A- > B$. Because users in different roles pay attention to different association rules and have different attributes of selected datasets, their mathematical descriptions have many forms. At present, the relevance based interestingness is widely used, so the research also uses the relevance based interestingness to improve the Apriori algorithm.

Let $Q(A)$ represent the probability of occurrence of event A in a transaction, $Q(B)$ represent the probability of occurrence of event B in a transaction, and $Q(AB)$ represent the probability of simultaneous occurrence of event A and event in a transaction.

Immediate establishment:

$$Q(AB)=Q(A)Q(B) \tag{1}$$

Explain that A and B are independent of each other.

Immediate establishment:

$$Q(A)(B) \neq Q(A)Q(B) \tag{2}$$

It indicates that A and B are not independent of each other, that is, events A and B are related.

The interest threshold is generally 1 by default. For the mined association rule $A- > B$, the interest degree of itemset A and itemset B is expressed as:

$$QU(A- > B) = \frac{Q(AB)}{Q(A)Q(B)} \tag{3}$$

When $QU > 1$, it indicates that there is a positive correlation between itemset A and itemset B, and when A occurs, the probability of B will increase.

When $QU < 1$, it indicates that there is a negative correlation between itemset A and itemset B, and when A occurs, the probability of B will be reduced.

When $QU{=}1$, that is, $Q(AB){=}Q(A)Q(B)$, it means that A and B are independent of each other and have no correlation [5].

The introduction of interest can filter the association rules without correlation or with negative correlation, and further reduce the number of candidate association rules (the candidate association rules here refer to the association rules that have just been generated by frequent itemsets and have not been compared with the minimum confidence level), which ensures that the association rules judged by confidence threshold are practical.

The improved Apriori algorithm (hereinafter referred to as I-Apriori, or Improved Apriori) is designed to improve the accuracy of extracting association rules. I-Apriori algorithm is still divided into two steps, the first step to find the frequent itemsets, the second step from the frequent itemsets to generate strong association rules.

Let D_k be the set of candidate K-itemsets, G_k be the set of frequent K-itemsets, $S_{\min}$ be the minimum support threshold, $C_{\min}$ be the minimum confidence threshold, I_{min} be the interest threshold, and R_t be the list of elements that can appear on the right side of the rule with the size of t.

The specific operation steps of the algorithm are as follows:

(1) Generate frequent itemsets.

1. Find frequent itemset E;
2. Generate candidates and prune;
3. Scan B to count candidates;
4. Return the itemset G_k in the candidate set that is not less than the minimum support;
5. Connection step;
6. If subset d already exists in k-1 term set, prune it;
7. Pruning step: delete infrequent candidates;
8. Pruning step.

(2) Generate strong association rules.

1. For each itemset G_i in set G_k, if G_i is not 1_ Item sets are filtered and generated. 1 - Item sets cannot generate strong association rules;
2. Only association rules greater than the interest threshold can be filtered;
3. If the following formula holds:

$$c > C_{\min} \tag{4}$$

In Eq. (4), c represents the confidence level.

The association rule is displayed.

The I-Apriori algorithm is parallelized based on Spark. The specific scheme is as follows:

(1) Configure Spark.

The original transaction data is stored on the distributed file system HDFS and transformed into a compressed matrix. The Spark driver reads the configuration file to generate the SparkConf object, then creates the SparkContext object to connect to the Spark cluster, scans the compression matrix on the HDFS using the textFile operator, and creates the RDD from the compression matrix data. As mentioned earlier, the Spark parallel framework compute process actually transforms the data set into a pending RDD, then performs a series of Transformation operations against the pending RDD to get a new RDD, and finally invokes the Action operation to get the result value. Because the elastic distributed data set RDD is the biggest characteristic of Spark big data framework, it is also the important reason for its high efficiency. Therefore, when computing tasks, the number of RDDs must match the computing resources allocated to the program by the Spark cluster, otherwise the Spark framework will be less computationally efficient and program concurrency will be reduced [6].

(2) Parallelization process of the I-Apriori algorithm.

The implementation of I-Apriori algorithm on Spark is divided into two steps. The first step is to utilize the advantage of Spark platform with multi-nodes.

In the second step, the candidate association rules are generated from the frequent itemsets. Then the association rules are filtered by the interest threshold and the confidence threshold. In the first step, the parallelization of the algorithm is realized by encapsulating the data into RDD and performing RDD operations. The key of the parallelization of the Apriori algorithm is the iterative call and action, which are solved by using the results of the previous iteration. For parallelization, each worker node performs the calculations required by the Apriori algorithm on the data in its RDD partition in a multi-threaded manner.

2.2 Denoising of Association Rules

For the mining association rules, the information data is transmitted and denoised.

The denoising method is a nonlinear wavelet transform threshold denoising algorithm based on improved threshold function. The selection of wavelet basis function is as follows: the denoising performance of different wavelet basis functions is tested for Doppler standard test signals with signal to noise ratio of 5dB and 15dB with different noise pollution.

Try to evaluate the de-noising performance of various wavelet basis functions from two aspects: different vanishing moments (filter length) of the same wavelet basis function and different wavelet basis functions of the same vanishing moment (filter length). By analyzing the test data, we can see that under the 5dB low SNR noise pollution, the root mean square error (RMSE) can better evaluate the de-noising performance of the wavelet basis function. Under the 15dB high SNR noise pollution, Signal to noise ratio (SNR) can better evaluate the denoising performance of wavelet basis function. Therefore, in order to better test the denoising performance of different wavelet basis functions, the denoising performance of wavelet basis functions is analyzed according to different threshold functions under low and high signal-to-noise ratios and different characteristics of two quality evaluation indicators. In the case of low SNR noise pollution, the root mean square error (RMSE) is used as the quality evaluation index to analyze the processing results of the soft threshold method; In the case of high signal to noise ratio noise pollution, the signal to noise ratio (SNR) is used as the quality evaluation index to analyze the processing results of the hard threshold method [7].

By comparing and analyzing the test results, under the condition of low signal-to-noise ratio noise pollution:

(1) From the perspective of single vanishing moment, Sym7, Coif4, Sym9, Sym13 and Sym14 wavelets have good denoising performance. Among them, Sym7 wavelet is the best and Bior3.1 is the worst;

(2) In terms of the overall denoising effect, Sym N wavelet system has a good noise suppression effect, followed by Coif N wavelet system, followed by Db N wavelet system, and Bior Nr. Nd wavelet system has a poor overall noise processing performance.

In the case of high signal-to-noise ratio noise pollution:

(1) From the perspective of single vanishing moment, Bior5.5, Sym15 and Sym11 wavelets have good denoising performance. Among them, Bior5.5 wavelet is the best, and Bior3.1 has the worst denoising performance;

(2) In terms of the overall denoising effect, Sym N wavelet system has a good noise suppression effect, followed by Coif N wavelet system, followed by Db N wavelet system, and Bior Nr. Nd wavelet system has a poor overall noise processing performance.

According to the test results, Sym N wavelet system is selected as the wavelet basis function.

In order to overcome the shortcomings of soft and hard thresholding methods, the selection of threshold function is improved on the basis of nonlinear wavelet transform thresholding method. The improved method is weighted average method. The basic idea of the weighted average method is to combine the soft and hard threshold functions with the weighted average method, introduce the weighting factor η, and construct a new type of threshold functions, as follows:

$$\dot{R}_{f,g} = \begin{cases} (1-\eta)\cdot R_{f,g} + \eta \cdot \mathrm{sign}\left(R_{f,g}\right) \\ \cdot\left(\left|R_{f,g}\right| - \mathrm{p}\right), \left|R_{f,g}\right| \geq \mathrm{p} \\ 0, \left|R_{f,g}\right| < \mathrm{p} \end{cases} \tag{5}$$

In formula (5), $R_{f,g}$ represents wavelet coefficient; p is the weighted average threshold.

Immediate establishment:

$$\eta = 0 \tag{6}$$

At this time, the method is hard threshold method.

Immediate establishment:

$$\eta = 1 \tag{7}$$

At this time, the method is soft threshold method.

This method can overcome the shortcomings of the soft and hard threshold functions to some extent, and make the reconstructed signal approach the real signal better. In practice, there are generally two methods for weighting factor η. One method is to simplify the value of η, and obtain the optimal value of η through comparison and analysis, usually $\eta = 0.5$; the other method is to use certain mathematical principles to calculate the wavelet coefficients $R_{f,g}$ and threshold p, and obtain the value of η through calculation as follows:

$$\eta = \frac{p}{\left|R_{f,g}\right| \cdot \exp\left(\sqrt{\frac{|R_{f,g}|-p}{|R_{f,g}|+p}}\right)} \tag{8}$$

The determination of the optimal decomposition and reconstruction scale is as follows:

Add noise with signal to noise ratio of 10dB to Doppler standard test signal, use non-linear wavelet transform threshold method to conduct wavelet denoising quality evaluation research, analyze the specific characteristics of each traditional quality evaluation index and two composite quality evaluation indexes, and then build a new wavelet denoising composite evaluation index to guide the determination of the optimal decomposition and reconstruction scale.

Specifically, in view of the one-sided nature of a single quality evaluation indicator, a new fusion method of composite evaluation indicators is obtained by comprehensively considering four traditional quality evaluation indicators. The calculation steps are as follows:

1. Determine the parameters required for wavelet decomposition, such as wavelet decomposition level (2–8 layers), wavelet basis function, threshold and threshold function;

2. When the true value is unknown, four evaluation indexes, namely Signal to Noise Ratio (SNR), Root Mean Square Error (RMSE), Correlation Coefficient (R) and Smoothness (r), are obtained by wavelet decomposition and reconstruction of various parameters and normalized;

3. Comprehensively considering the different characteristics of four traditional single quality evaluation indicators, the normalized root mean square error (RMSE), signal to noise ratio (SNR) and correlation coefficient (R) are averaged to obtain the fusion indicator U, which is calculated as follows:

$$U = \frac{F_{RMSE}(N) + F_{SNR}(N) + F_R(N)}{3} \tag{9}$$

In Formula (9), $F_{RMSE}(N)$ refers to the mean value of normalized root mean square error; $F_{SNR}(N)$ is the mean value of normalized signal-to-noise ratio; $F_R(N)$ refers to the mean value of normalized correlation coefficient.

4. The method of determining the weight of the coefficient of variation is adopted to calculate the coefficient of variation of the normalized fusion index U and smoothness g, and weight them according to the size to obtain the weights W_1 and W_2;

5. The weighted fusion index U and smoothness g are linearly combined to obtain the composite index H. The smaller the value of H, the better the denoising effect. The corresponding decomposition scale is the best decomposition and reconstruction scale.

$$H = W_1 \cdot U + W_2 \cdot g \tag{10}$$

The improved method of threshold estimation is as follows: use the 3 σ criterion in electronic measurement to detect and eliminate the abrupt part of the signal and noise, so as to calculate the noise standard deviation on different decomposition scales, and then determine the threshold on each decomposition scale.

2.3 Information Anomaly Detection

An anomaly detection method is proposed by calculating the anomaly probability of the data stream, which improves the detection rate and reduces the false alarm rate. The algorithm first obtains the data series of the data stream in a period of time, then calculates the data series to get the information entropy series of the sliding window, then calculates the abnormal probability of the data value and the abnormal probability of the information entropy in the sliding window respectively, and finally judges whether the data stream is abnormal through the comprehensive calculation of the abnormal probability.

The algorithm steps are as follows:

(1) Information entropy sequence calculation.

Information entropy can reflect the statistical distribution characteristics of data series in the window. The data sequence in the sliding window is abstracted as a system. The information entropy l_i of sampling data sequence $y_i(k)$ in the sliding window is defined, and the sliding window size is V.

Assume that the value range of $y_i(k)$ is:

$$S = \{Y_1, Y_2, \cdots, Y_i\} \tag{11}$$

In Eq. (11), Y_i refers to the value of the i th $y_i(k)$.

Calculate the sampling probability of each data value, which can be expressed as follows:

$$\alpha_j = P(y = Y_i) = \frac{\text{count}(Y_i)}{\sum_{j \geq 1} \text{count}(Y_i)} \tag{12}$$

In Eq. (12), $P(\cdot)$ represents the sampling probability; $\text{count}(Y_i)$ represents the number of occurrences of Y_i in data sequence $y_i(k)$.

The sliding window information entropy is calculated based on the sampling probability:

$$\beta_i = \sum_{j \geq 1} \alpha_j \lg \frac{1}{\alpha_j} \tag{13}$$

As the window slides, the information entropy of window data is calculated in turn, so the time series of information entropy can be expressed as:

$$\beta = \{\beta_1, \beta_2, \cdots, \beta_i\} \tag{14}$$

Abnormal probability calculation.

Anomaly probability and joint anomaly probability are defined so that they can be applied to the comprehensive determination of anomalies under multiple conditions, and thus applied to the comprehensive utilization of time correlation and statistical characteristics of data streams.

The sensor data anomaly is defined as: in dataset χ, for a data object L, if the number of data objects in the circle with distance r is less than ω, it is considered as an anomaly. In each detection condition, there is a threshold ω of the number of adjacent data objects, which is independent of each other, so it is difficult to make a comprehensive decision under multiple detection conditions. On the basis of the above, the anomaly probability and joint anomaly probability are defined, making them applicable to the comprehensive determination of anomalies under multiple conditions, and thus applied to the comprehensive utilization of time correlation and statistical characteristics of data streams.

Suppose there are v data objects in dataset χ. If there is a data object L in dataset χ, and the distance between γ data objects and object L is greater than φ, then the anomaly probability ς_0 of data object L is defined as $\frac{\gamma}{v}$. Where r is the standard deviation ϕ of dataset χ.

For the sampling data sequence $y_i(k)$ in the sliding window, it is expressed as $Y_1, Y_2, \cdots, Y_i$, and the size of the sliding window is set as τ. For each data value Y_i, there are two cases as follows:

1. Current establishment:

$$\overline{d}\left(Y_i, Y_j\right) \leq \phi \tag{15}$$

In Eq. (15), $\overline{d}\left(Y_i, Y_j\right)$ represents the distance between Y_i and Y_j.

The number m_1 of points not adjacent to Y_i in the window remains unchanged.

2. Current establishment:

$$\overline{d}\left(Y_i, Y_j\right) > \phi \tag{16}$$

The number of points in the window that are not adjacent to Y_i is m_1 plus 1.

Where m_1 is initialized to 0.

The abnormal probability of Y_i data value of data point can be calculated by the following formula:

$$\varsigma_1 = \frac{m_1}{\tau} \tag{17}$$

Similarly, the information entropy sequence β in the sliding window is expressed as $\{\beta_1, \beta_2, \cdots, \beta_i\}$, and β_i is the information entropy of the sampling data sequence $y_i(k)$. For each entropy value, there are two cases as follows:

1. Current establishment:

$$\overline{d}\left(\beta_i, \beta_j\right) \leq \phi \tag{18}$$

In Eq. (18), $\overline{d}\left(\beta_i, \beta_j\right)$ refers to the distance between β_i and β_j.

The number m_2 of points not adjacent to β_i in the window remains unchanged.

2. Current establishment:

$$\overline{d}\left(\beta_i, \beta_j\right) > \phi \tag{19}$$

The number of points in the window that are not adjacent to β_i is m_2 plus 1. Where m_2 is initialized to 0.

The information entropy anomaly probability of data point $y_i(k)$ can be calculated by the following formula:

$$\varsigma_2 = \frac{m_2}{\tau} \tag{20}$$

It is undoubtedly not accurate to judge data exceptions only by the time correlation or statistical characteristics of the data stream. It is necessary to combine these two aspects for comprehensive analysis. Based on ς_1 and ς_2, joint probability can be calculated. When the joint probability satisfies the following formula:

$$P_L - \frac{\vartheta + \rho}{2} > \varsigma_0 \tag{21}$$

In Eq. (21), P_L refers to joint probability; ϑ refers to the mathematical expectation of abnormal probability in the event area of large-scale industrial CT data transmission information; ρ refers to the mathematical expectation of abnormal probability of large industrial CT data transmission.

The network node corresponding to the data transmission information is abnormal.

3 Experimental Test

3.1 Experimental Environment

The experiment test is carried out for the designed anomaly detection method of large-scale industrial CT data transmission information based on association rules. The hardware configuration in the test is shown in Table 1.

Table 1. Hardware Configuration in Test

Serial No	Equipment name	Specific configuration
1	notebook	Portable notebook
2	Hard disk	SanDisk SSD TLC Cache Granules 128G capacity
3	operating system	CentOS release 7.2
4	Memory	16G*2 3200MHz DDR4L
5	CPU	Intel Core Gen6 i8-1254H

The large industrial CT data transmission system in the experiment is composed of digital processing module, PHY chip, etc. A data transmission system board is connected with multiple data acquisition boards. The data transmission system collects the data on each board and sends the data to PHY chip through the MII interface. PHY chip converts the data into differential signals and sends them to the network.

50 network nodes are arranged for the experimental system for experimental testing.

3.2 Test Method

It is a common way to validate anomaly detection methods by manually injecting attacks on real node data. In the test, on the basis of the experimental system network and data set, the nodes in the network are selected as the targets of data attack.

Select representative data attack methods for testing. During the test, discrete abnormal data and fixed abnormal data are injected by tampering with the data reported by the node, so as to realize the data attack on the system network. The design method is used to detect the abnormal data caused by the attack.

Among them, node 5 is selected as the attack target for injecting discrete abnormal data, and node 16 is selected as the attack target for injecting fixed abnormal data.

During the testing process, 50 different false data injection points are randomly selected from the reported data streams of node 5 and node 16, and one injection point is selected for each test to inject false data, and abnormal detection is conducted for the data in this section. The detection algorithm sets the sliding window size to 1000 and the window sliding distance to 100 sample data values.

3.3 Test Result

The experimental design method is applicable to the anomaly detection accuracy and average anomaly detection time of two types of injected anomaly data. The higher the detection accuracy and the shorter the average anomaly detection time, the better the detection effect of this method. In the test, the methods proposed in Reference [3] and Reference [4] are used as the comparison test methods to jointly test.

3.3.1 Abnormal Detection Accuracy Test

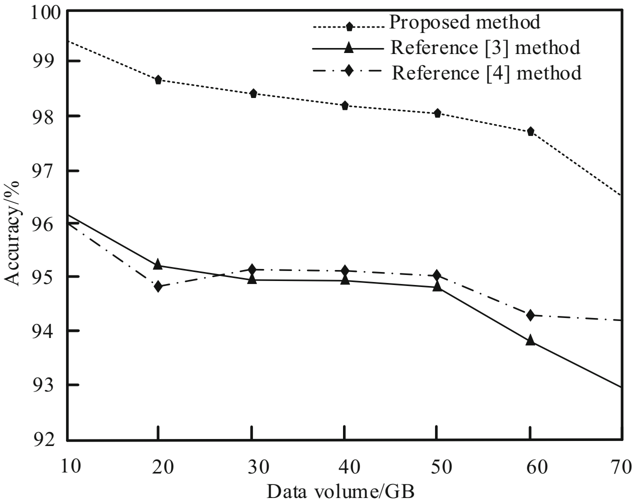
For two types of injected abnormal data, the test results of the three methods are shown in Fig. 1.

According to the test data in Fig. 1, for discrete abnormal data, the accuracy of anomaly detection of the design method can reach 99.38% at most, and that of the methods proposed in Reference [3] and Reference [4] can reach 96.18% and 96.02% respectively. The accuracy of anomaly detection of the design method is much higher than that of Reference [3] and Reference [4]. For fixed abnormal data, the accuracy of anomaly detection of the design method is also higher than that of the other two methods.

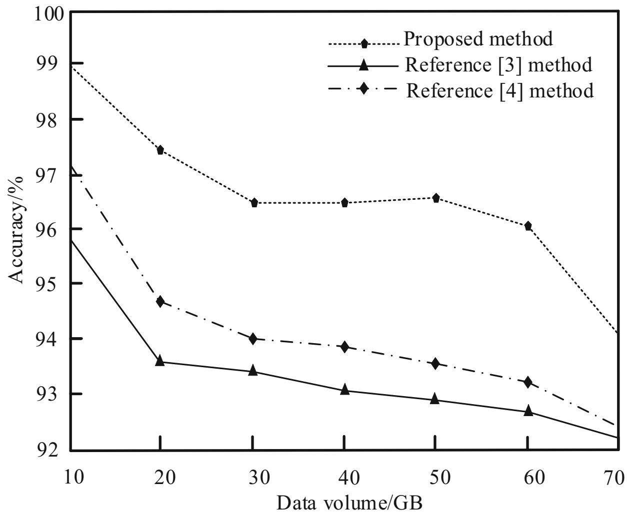
3.3.2 Time Test

For the two injected abnormal data, the average anomaly detection time test results of the three methods are shown in Fig. 2.

It can be seen from the experimental results in Fig. 2 that the detection time of the three methods increases with the increase of data volume. The average anomaly detection time of the proposed method is kept within 300ms, while the detection time of the method in reference [3] and the method in reference [4] is 200ms ~ 500ms. The comparison shows that the average anomaly detection time of the proposed method is significantly lower than that of the other two methods. Therefore, the detection time of the proposed method is the shortest.



(a) Discrete abnormal data



(b) Fixed abnormal data

Fig. 1. Test Results of the Accuracy of Anomaly Detection of the Three Methods. (a) Discrete abnormal data. (b) Fixed abnormal data.

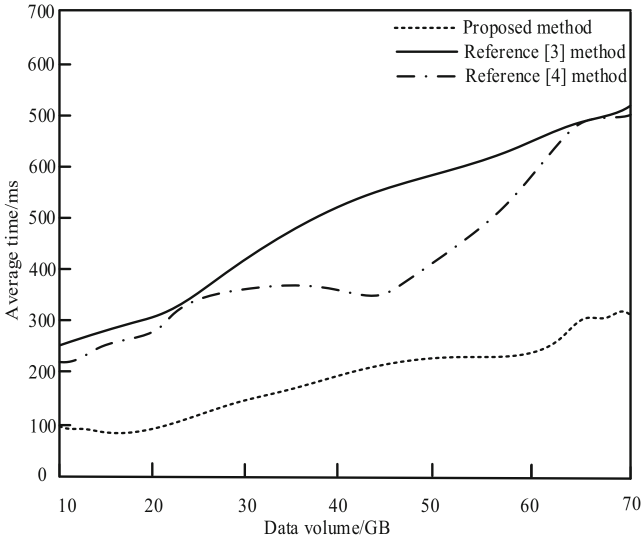


Fig. 2. Test Results of Average Abnormal Detection Time

4 Conclusion

In the field of industry, large-scale industrial CT is widely used. Based on the demand of large industrial CT data transmission, an anomaly detection method of large industrial CT data transmission based on association rules is designed in this paper. Experimental results show that the proposed method has high detection accuracy and short average detection time. Due to the high detection cost in the detection process, the application scope of this technology is limited. In the future research, the focus will be on reducing the detection cost and expanding the scope of use.

References

1. Pang, G., Shen, C., Cao, L., et al.: Deep learning for anomaly detection: a review. ACM Comput. Surv. **54**(2), 1–38 (2021)
2. Cheng, S.L.: High-speed network multi-mode similar data string isolated transmission simulation. Comput. Simul. **38**(6), 117–120 (2021)
3. Hosseinzadeh, M., Rahmani, A.M., Vo, B., et al.: Improving security using SVM-based anomaly detection: issues and challenges. Soft. Comput. **25**(4), 3195–3223 (2021)
4. Chen, Y., Zhang, H., Wang, Y., et al.: MAMA Net: multi-scale attention memory autoencoder network for anomaly detection. IEEE Trans. Med. Imaging **40**(3), 1032–1041 (2021)
5. Natalino, C., Udalcovs, A., Wosinska, L., et al.: Spectrum anomaly detection for optical network monitoring using deep unsupervised learning. IEEE Commun. Lett. **25**(5), 1583–1586 (2021)
6. Ata-Ur-Rehman, T.S, Farooq, H., et al.: Anomaly detection with particle filtering for online video surveillance. IEEE Access **9**, 19457–19468 (2021)
7. Kotlar, M., Punt, M., Radivojevic, Z., et al.: Novel meta-features for automated machine learning model selection in anomaly detection. IEEE Access **9**, 89675–89687 (2021)