A Multi Stage Data Attack Traceability Method Based on Convolutional Neural Network for Industrial Internet

Yanfa Xu[1(✉)] and Xinran Liu[2]

[1] Department of Information Engineering, Shandong Vocational College of Science and Technology, Weifang 261053, China
xxyf5132@163.com

[2] State Grid Liaoning Marketing Servide Center, Shenyang 110000, China

Abstract. In order to accurately define the network area to which data attacks belong and avoid multi-stage delay in industrial Internet, a multi-stage data attack traceability method based on convolutional neural network is proposed for industrial Internet. The convolution neural network is used to solve the training expression of the classifier. Combined with the multi-stage attack data and information samples of the industrial Internet, improve the expression conditions of the encryption algorithm, and realize the construction of the multi-stage consensus mechanism of the industrial Internet. Define the value range of multi-stage data of workflow meta industrial internet, so as to determine the function of the traceability automatic capture mechanism on data samples, and complete the traceability of multi-stage data attacks of industrial internet. The comparative experiment results show that the proposed method can accurately define the sample interval of data attack behavior in the six network regions selected in this experiment, and has strong practical value in solving the multi-phase delay problem of industrial Internet.

Keywords: Convolutional Neural Network · Industrial Internet · Data Attack · Classified Training · Metadata · Automatic Capture Mechanism · Network Area · Multi Stage Delay

1 Introduction

Convolutional neural networks have been widely used in various machine learning tasks. In the process of updating the neural network parameters, the gradient of each layer of the network is obtained by using the back propagation algorithm, which is the chain rule of the neural network [1]. Tracing the big data model processing process can help to evaluate the data quality and reproduce the data generation process; When a certain result data is suspected, its source can be traced and traced through audit; If there is an error in the data, you can locate the location and cause of the error, and finally each data can be relied on. As an important means of data analysis, traceability can help decision-makers remove noisy and useless data and maximize information decision-making. The

B. Wang et al. (Eds.): ICMTEL 2023, LNICST 534, pp. 215–227, 2024.
https://doi.org/10.1007/978-3-031-50577-5_16

traceability technology has been widely studied in the fields of database, workflow and distributed system interaction, but the traceability based on big data model analysis is still a great field worth exploring.

Traditional traceability methods are mainly applicable to databases or data warehouses, but not in the field of big data due to its diversity, heterogeneity, large-scale and other characteristics. Data traceability is information about source data and data creation process, which can be used to evaluate data quality, audit and track data sources, and quickly locate the location of errors. At present, there are many researches on data traceability in the field of database, but few in the field of big data [2]. Multi stage data attacks on the industrial Internet will affect the stability of the network operation, which will not only cause the network system to show multi-stage delay, but also make data samples unable to be transmitted to the correct node units.

In order to avoid the occurrence of the above situation, a multi-stage data attack traceability method based on convolutional neural network is proposed for industrial Internet. On the basis of establishing the multi-stage consensus mechanism of industrial Internet by using convolution neural network, the data traceability framework is constructed. By defining workflow metadata, the automatic traceability capture mechanism is improved, so as to realize the smooth application of the multi-stage data attack traceability method of industrial Internet.

2 Multi Stage Consensus Mechanism of Industrial Internet

As the basis for tracing data attacks, the multi-phase consensus mechanism of the industrial Internet includes three execution processes: convolutional neural network construction, classification focused training, and encryption algorithm improvement. This chapter will focus on the above contents.

2.1 Convolutional Neural Network

Convolution neural network (CNN) is a multilayer feedforward neural application network. Each layer uses a set of convolution checks for multiple transformations. Convolution operation is helpful to extract useful features from locally related data, and distribute the output of convolution kernel to nonlinear processing units. This nonlinearity generates different activation modes for different reactions, which is helpful to learn the semantic differences in images. CNN is specially designed for processing data samples. Therefore, neurons in each layer are organized in the three dimensions of height, width and depth, just as information parameters in data samples will distinguish different definition values. The important attributes of CNN are hierarchical learning, automatic feature extraction, multi task processing and weight sharing, which are mainly composed of convolution layer, incentive layer, pooling layer and full connection layer.

When facing low dimensional data, each layer of the neural network can be designed as a full connection layer. However, it is impractical to connect neurons to all neurons in the previous layer when dealing with high-dimensional inputs such as data samples. To this end, we can divide the data sample space into multiple regions for consideration, and then connect each neuron to a local region of the input. The range of this connectivity is

called the receptive field of the neuron, which is equivalent to the size of the filter [3]. When dealing with spatial dimension and depth dimension, it is important to emphasize this asymmetry. The connection is local in space, but it is always global in the whole depth of input.

Let α, δ and ε represent three unequal neuron parameters, and their minimum values are equal to the natural number "1". l_α represents the data sample connection feature based on the parameter α, l_δ represents the data sample connection feature based on the parameter δ, l_ε represents the data sample connection feature based on the parameter ε, χ represents the data sample space planning coefficient, β represents the data sample input coefficient, and the above physical quantities are combined, Convolution neural network can be defined as formula (1):

$$j = \frac{\chi \sum_{\alpha=1}^{n} \sum_{\delta=1}^{n} \sum_{\varepsilon=1}^{n} (l_\alpha \cdot l_\delta \cdot l_\varepsilon)^2}{\beta} \tag{1}$$

The increase of neural network layers produces a large number of parameters, and CNN uses the weight sharing mechanism to control the number of parameters. Assuming that the weight of each neuron connection data window is fixed, the number of parameters can be greatly reduced through parameter sharing. It is generally understood that scanning the image with the same filter is equivalent to feature extraction once, thus obtaining a feature map. The parameters of the filter are fixed, so each different area of the data sample is scanned by the same filter, so the weight values are the same, which is called weight sharing.

Figure 1 shows the classic CNN structure applied in the traceability method of industrial Internet multi-phase data attacks.

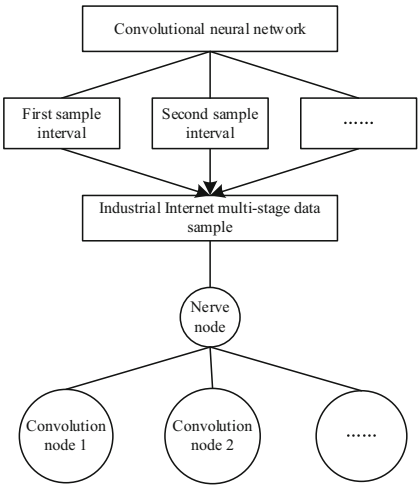

Fig. 1. Classical CNN structure of convolutional neural network

After the two steps of local perception and parameter sharing, the number of weights generated in the original training process will be reduced to a certain extent, but the feature dimensions will increase, leading to the occurrence of over fitting. Therefore, high-dimensional features need to be reduced before training the classifier. Therefore, pooling operation is designed to reduce the complexity of convolutional neural network. Like the convolution layer, the pooling layer also connects neurons to a square area through the width and height dimensions of the previous layer. The main difference between convolution and pooling is that neurons in the convolution layer can learn weights or deviations in the training process, while neurons in the pooling layer do not learn weights or deviations in the training process, but perform certain fixed functions on their inputs, so pooling operation is a non parametric process.

2.2 Classified Training

The transition from source model to intermediate model is a typical transfer learning based on convolutional neural network. The combination of pre training model and layer freezing method is used for the construction and training of CNN model, including the following key processes:

(1) Initialization stage: retain the weight parameters of the pre trained CNN model as the feature extraction source in the first stage of model training;
(2) Load the parameters and weights of the pre training model other than the last fully connected classification layer, freeze the convolution layer and pooling layer of the pre training model, and only train the new classifier layer;
(3) The second stage: transfer the reserved parameters of the convolution and pooling layer of the pre trained model on the CNN model, and dock with the new fully connected classification layer trained in the first stage before to obtain the intermediate model.

Convolutional neural networks usually freeze the weights of the first a layers in the pre training model, and then use the data from the target domain to retrain the next $s - a$ layers. This process is called fine-tuning. The purpose of fine-tuning is to extract high-level features of the target domain, reduce the content difference between the source domain and the target domain, and improve the model recognition rate [4]. In general, increasing the number of network layers can help extract more high-level features. Therefore, it is considered to appropriately increase the number of network layers while conducting migration learning, that is, to add an adjustment module, so that the model can obtain the unique high-order statistical features of the target domain.

The weight value calculation results based on the data samples of the front a layer and the rear $s - a$ layer are shown in Formula (2) and Formula (3).

$$d_a = j^2 - \phi_a \frac{\dot{S}_a^2}{S_{\max} - S_{\min}} \tag{2}$$

$$d_{s-a} = j^2 - \phi_{s-a} \frac{\dot{S}_{s-a}^2}{S_{\max} - S_{\min}} \tag{3}$$

In the formula, ϕ_a represents the content difference coefficient of the data samples in the front a layer, ϕ_{s-a} represents the content difference coefficient of the data samples in the back $s-a$ layer, $\dot{S}_a$ represents the value characteristics of the data samples in the front a layer, $\dot{S}_{s-a}$ represents the value characteristics of the data samples in the back $s-a$ layer, $S_{\min}$ represents the minimum value of the residual error of the data samples, and $S_{\max}$ represents the maximum value of the residual error of the data samples.

The consensus method based on convolutional neural network minimizes the distribution difference between the two domains by projecting the data sample domain and the target domain to the same feature space. Under the new feature space, the distribution difference between the data sample domain and the target domain decreases; The weighting methods based on convolutional neural network focus more directly on comparing the distribution of source data and target data. These methods weight or filter the information parameters in the data sample domain to minimize the distribution difference between the sample domain and target domain.

On the basis of Formula (2) and Formula (3), let γ represent the coding coefficient of the data sample parameters in the convolutional neural network, φ_a represent the convolution vector based on the data samples of the first a layer, φ_{s-a} represent the convolution vector based on the data samples of the next $s-a$ layer, combine the above physical quantities, and derive the retraining of the convolutional neural network classifier as Formula (4):

$$D = \frac{-\sum_{\gamma=1}^{n} \gamma d_a \cdot d_{s-a}}{\sqrt{\varphi_a^2 + \varphi_{s-a}^2}} \tag{4}$$

Calculate the relative weight value of the source domain samples, delete the source domain samples that differ greatly from the target domain data distribution, and select the training data with higher weight value as the new source domain samples. Therefore, although the data distribution of the source domain and the target domain is very different, after calculating the relative weight, the data distribution of the left source domain samples and the target domain samples is relatively small.

2.3 Encryption Algorithm

The multi-phase data encryption algorithm for industrial Internet based on convolutional neural network involves public key and private key, which are selected and saved by users themselves, and can be transferred to anyone. The public key can be calculated through the private key, but the private key cannot be calculated in polynomial time through the public key. The public key cryptosystem can be used to encrypt messages. The sender uses the public key to encrypt the message to get the ciphertext. After receiving the ciphertext, the receiver uses the private key to decrypt the ciphertext to get the plaintext.

The encryption algorithm is built on the basis of the secret sharing scheme. The main idea is to disperse the secrets and let them be kept by multiple people [5]. When it is necessary to reconstruct the shared secret, if the number of people involved in recovering the secret exceeds a given limit, the whole original shared secret can be recovered through

joint efforts. If the number of people involved in recovering the secret is less than the specified limit, even if these people work together, they cannot get any information about the original shared secret, and the specified limit is called threshold or threshold. The threshold encryption algorithm should meet the following requirements:

If the sub key exceeds the threshold value, the whole plaintext can be recovered; if the sub key is less than the threshold value, no information of the whole plaintext can be obtained.

No master key information can be obtained through the sub key.

Let L_1 represent the key threshold value in the first encoding process, and L_2 represent the key threshold value in the second encoding process. The value relationship between the two satisfies $L_1 \geq L_2$. The specific definition of threshold values L_1 and L_2 is Formula (5):

$$\begin{cases} L_1 = \prod_{\iota=1}^{m} D \cdot \iota |l_1|^2 \\ L_2 = \prod_{\iota=1}^{m} D \cdot \iota |l_2|^2 \end{cases} \tag{5}$$

where, ι represents the ciphertext transcoding coefficient, l_1 represents the ciphertext sample value in the first encoding process, and l_2 represents the ciphertext sample value in the second encoding process. In order to establish $L_1 \geq L_2$, it is required that the values of l_1 and l_2 indicators should meet $l_1 \geq l_2$.

The consensus mechanism is an agreement that ensures the state and elasticity of the convolutional neural network connection to reach consensus, and it is also a key component of the network system. In order to ensure the continuous and normal operation of network templates, it is necessary to design appropriate consensus mechanisms according to their different application scenarios [6]. While the consensus mechanism of the industrial Internet based on the improvement of the CNN model can be applied to the cloud storage platform, there are still problems such as the centralization of equity resources, reuse and information disclosure.

3 Data Attack Traceability Scheme

On the basis of convolutional neural network, a data traceability framework is constructed, and then the automatic traceability capture mechanism is improved by defining workflow metadata, so as to achieve the smooth application of the traceability method of industrial Internet multi-phase data attacks.

3.1 Data Traceability and Tracking Framework

The core of data traceability is traceability metadata. Any traceability system needs to manage its traceability information well, which inevitably requires an overall traceability framework. The traceability of industrial Internet multi-phase data attacks was first

developed in the database field, which specifically refers to scientific databases or regulatory databases, that is, such databases need to be annotated under special monitoring management. These annotations are authoritative descriptions of professionals and have a wide range of applications [7]. For example, an encyclopedic database such as Wikipedia needs a large number of professionals to edit behind the scenes, and finally the content presented on the network will contain a large number of other database information, so this regulatory database brings about the problem of data ownership. The traceability methods in the database are mainly annotation method and inversion method. The annotation method records and stores data items and transfers them together with the data; The inversion method does not need additional storage, and directly constructs the inversion expression for reverse tracking.

The concept of workflow is to transfer information or tasks among participants according to certain rules to achieve certain effects. It can be divided into scientific workflow and business workflow. Scientific workflow is to execute the traditional scientific research process in the form of workflow. It does not provide a series of operating steps to describe the whole process as the traditional scientific research process, but uses a data driven approach, taking the output of the previous stage as the input of the next stage. Scientific workflow pays more attention to the reliability of data, and puts forward higher requirements for the accuracy of each step of data traceability.

Δ represents the data traceability set, which is defined as Formula (6):

$$\Delta = \left\{ k|k = \frac{\sqrt{(f_1 g_1)^2 + (f_2 g_2)}}{L_1 \times L_2} \right\} \tag{6}$$

where, k represents a random data sample in the traceability set, g_1 and g_2 represent two unequal data stream parameters, f_1 represents the tracking coefficient based on data stream parameter g_1, and f_2 represents the tracking coefficient based on data stream parameter g_2.

Let k_1 and k_2 be two non coincident sample parameters in the data traceability set Δ, whose value is $k_1, k_2 \in \Delta$. On the basis of this value range, let $\dot{j}$ represent the attack behavior vector of industrial Internet multi-phase data, and deduce the definition condition of data traceability framework as Formula (7):

$$J = \left(1 - \dot{j}^2\right) \left| \frac{k_1 + k_2}{k_1 \cdot k_2} \right|^2 \tag{7}$$

In the industrial Internet environment, data quality evaluation often needs to determine its source or creation process through the context of data. In today's big data environment, the resulting data often comes from various sources or is obtained through continuous and complex transformation and long-term accumulation. In the scientific experiment environment, it is more and more difficult to track the data source and complex data conversion relationship for a specific scientific research result [8]. However, data traceability can capture various traceability metadata in the data generation process, through which the dependency between data or transformations can be analyzed, and then data quality assessment and reliability verification can be carried out.

3.2 Workflow Metadata

The previous section has introduced the data traceability framework, which is designed to ensure the execution of tasks. However, the actual traceability does not require all its data. The key is to extract the relationship between models [9]. The workflow metadata is designed for traceability. It mainly includes the global basic description of the workflow and the dependencies between models. The details are as follows.

The industrial Internet multi-phase data attack behavior represents the global description of the model workflow, as shown in Table 1.

Table 1. Workflow Model of Data Attack Behavior

Name	Category	Explain
Paths	String	Set of IDs of relationship edges between models
ModelflowID	String	Unique identification of the workflow
ModelList	String	Model ID collection contained in Workflow
Description	Text	Workflow description information
ExecuteType	String	Execution type of the model
Version	String	Model version number
Parameter	String	Constrains the transmission time of data samples from one model area to another

Defining workflow metadata can also determine the capability of other traceability objects.

(1) Cloud storage users: have their own cloud data and have data sharing relationships with other cloud storage users.
(2) Cloud service provider: mainly responsible for the registration of industrial Internet users, the storage and monitoring of cloud storage data. When a cloud storage user attacks multi-phase data, CSP monitors its operation to generate cloud storage data source information, and manages the generated cloud storage data source information. CSP will strictly perform its own functions, but it also remains curious about cloud data of cloud storage users.
(3) Data source information database: mainly responsible for storing all cloud data source information. Cloud storage data source information will be used to track user violations.
(4) Blockchain: mainly responsible for publishing cloud storage data source information and generating block vouchers for cloud storage data source information. Blockchain stores the hash value of cloud storage data source information in the block. When the source information of cloud storage data needs to be verified, the blockchain generates a block voucher related to the source information of cloud storage data.
(5) Data source information auditor: mainly responsible for updating and maintaining the data source information database. PA uses block vouchers to verify the cloud

storage data source information, and adds the verified results to the corresponding cloud storage data source information in the data source information database. PA strictly performs its own functions, but will also try to obtain information of interest.

3.3 Traceability Automatic Capture Mechanism

Coarse grain traceability of multi-stage data attacks on industrial Internet will lead to process traceability, which is caused by black box effect in workflow. Because the processing algorithm in any workflow system is transparent to users, as far as workflow process management is concerned, this will undoubtedly reduce the burden on users. However, for traceability management, encapsulation will mean shielding the details. The general workflow traceability model can only be represented as process level traceability, that is, coarse-grained traceability, and has no knowledge of the processing process of nodes, which will inevitably lead to the dependency differentiation problem of data items, That is, it is impossible to analyze the exact source item of a certain item in the result data.

It can be seen that the key problems to be solved in realizing the automatic traceability capture mechanism include:

(1) How to perform traceability capture. This process needs to analyze the internal execution process of the model. Because each model handles different businesses, and we cannot do specific business analysis for all models, we have to solve this problem from a more abstract level;
(2) How to realize the tag storage of traceability information. The tag storage of traceability information is mainly used to record the dependency between the front and back data items during the model execution process, so as to achieve traceability;
(3) How to trace the source. Tracing is a query algorithm based on the traceability information storage in (2).

Let μ represent the performance strength of industrial Internet multi-phase data attacks, $\hat{b}$ represent the performance characteristics of attacks, and $v_1, v_2, \ldots, v_n$ represent the coding coefficients of n traceable nodes that are not zero. With the support of the above physical quantities, simultaneous formula (7) can define the traceability automatic capture mechanism as formula (8):

$$M = \min n \times \frac{\hat{b} \times J}{v_1 \times v_2 \times \ldots \times v_n} \tag{8}$$

The searchable encryption algorithm is used to process the industrial Internet multi-phase data attacks, and the ciphertext is stored in the CSP cloud storage database. By using this data storage method, we can not only ensure the confidentiality of data samples, but also achieve flexible multi-user data sharing [10]. By monitoring users' operations on cloud data, we can collect cloud data source information, so as to accurately trace the source of attacks.

Traceability metadata management refers to the operations of adding, deleting, querying and modifying the traceability metadata of the model workflow. The most critical stage is to describe the input, output and intermediate data of the model before the implementation of the model. Metadata is added by the model developer before the implementation of the model, which provides a basis for subsequent traceability.

Traceability is the core function of the traceability system, including coarse grain traceability, fine grain traceability and traceability diagram display. The coarse grain traceability function is based on the traceability metadata and aims to track users' needs at different levels, including tracking the data source according to the result data, tracking its generation process according to the result data, tracking its source according to the intermediate data and storing the traceability map in sequence. The data targeted by this process are all file level; The fine-grained traceability uses a recursive method to track the data items in the result file. Its implementation depends on the underlying Hadoop extension, mainly including the capture and storage of traceability information in the map and reduce processes; The traceability map display function mainly displays the traceability information in a visual form.

4 Example Analysis

4.1 Variable Description and Experimental Process

The accuracy of the selected traceability method's definition of the sample interval of industrial Internet data attacks can affect the probability of multi-stage delay in the network system. In general, the higher the definition accuracy is, the lower the probability of multi-stage delay. On the contrary, the higher the probability is.

The accuracy of the selected traceability method in defining the sample interval of industrial Internet data attacks is defined by Formula (9):

$$\omega = \xi \cdot \psi \tag{9}$$

where, ξ represents the network complexity coefficient, and ψ represents the aggressiveness intensity index.

The specific implementation process of this experiment is:

Step 1: Build the industrial Internet system as shown in Fig. 2;

Step 2: use the tracing method based on convolutional neural network to control the Internet host, and record the numerical changes of network complexity coefficient and aggressiveness intensity index;

Step 3: Use big data traceability method to control the Internet host, and repeat step 2 again;

Step 4: release the temporary data information samples in the Internet host;

Step 5: Control the Internet host by using the multi-source traceability method, and repeat step 2 again;

Step 6: Compare three groups of different data variables and summarize the experimental rules.

4.2 Experimental Results

Figure 3 and Fig. 4 shows the numerical changes of network complexity coefficient (ξ) and aggressiveness intensity index (ψ) under the influence of convolutional neural network based traceability method, big data traceability method and multi-source traceability method.

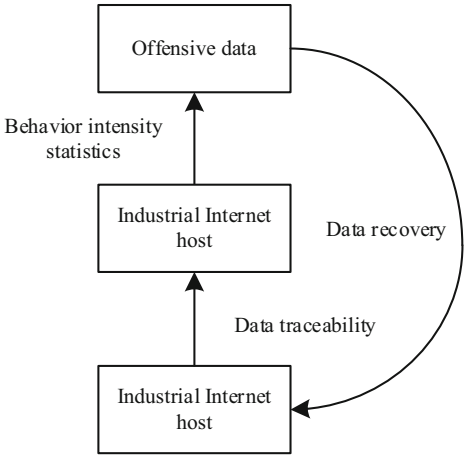

Fig. 2. Industrial Internet Experimental Structure

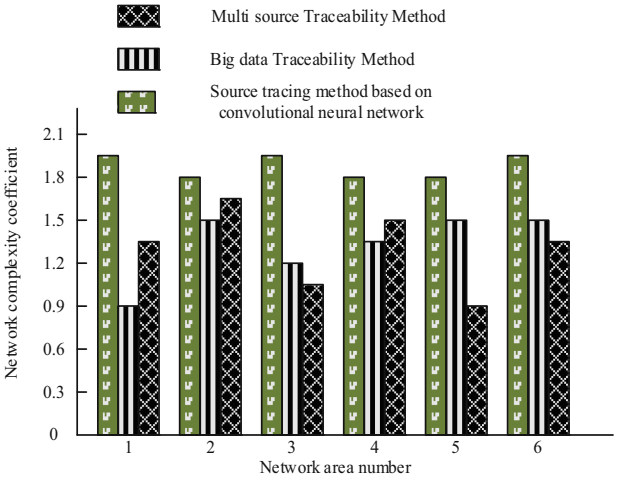

Fig. 3. Network complexity coefficient (ξ)

It can be seen from the analysis of Fig. 3 that the mean value of ξ index is relatively high under the effect of the traceability method based on convolutional neural network, and the maximum numerical result reaches 1.95 in the whole experiment process; Under the effect of big data traceability method, the average level of ξ index is low, and the maximum numerical result can only reach 1.50 in the whole experiment process; Under the action of multi-source traceability method, the average level of ξ index is between the traceability method based on convolutional neural network and big data traceability method. During the whole experiment, the maximum numerical result is 1.65.

It can be seen from the analysis of Fig. 4 that the mean value of ψ index is the highest under the effect of the traceability method based on convolutional neural network, and

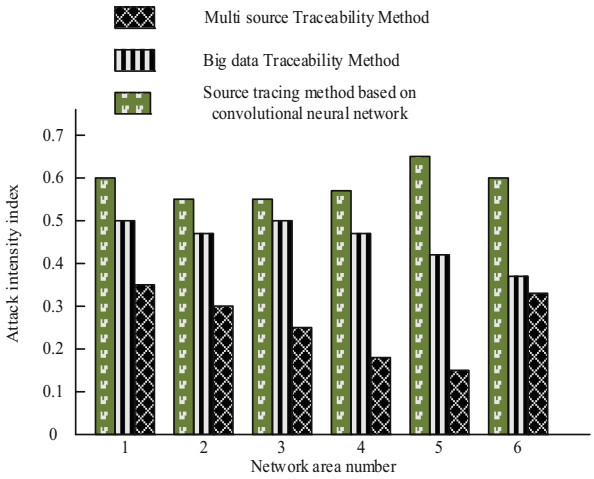

Fig. 4. Aggressiveness intensity index (ψ)

the maximum numerical result reaches 0.65 in the whole experiment process; Under the action of multi-source traceability method, the mean value of ψ index is the lowest, and the maximum numerical result can only reach 0.35 in the whole experiment process; Under the influence of big data traceability method, the average level of ψ index is between the traceability method based on convolutional neural network and the multi-source traceability method. In each experiment process, the maximum numerical result is 0.50.

Combine the experimental results of ξ and ψ indicators in Fig. 3 and Fig. 4 to make statistics on the definition accuracy of the sample interval of the selected traceability method for industrial Internet data attacks. In order to reduce the amount of numerical computation, the maximum numerical results of ξ and ψ indicators are selected. The specific calculated numerical values are shown in Formula (10):

$$\begin{cases} \omega_1 = 1.27 \\ \omega_2 = 0.75 \\ \omega_3 = 0.58 \end{cases} \tag{10}$$

where, ω_1 represents the definition accuracy of the convolutional neural network based traceability method, ω_2 represents the definition accuracy of the big data traceability method, and ω_3 represents the definition accuracy of the multi-source traceability method.

According to the numerical results of Formula (10), the convolutional neural network based traceability method has the strongest ability to accurately define the sample interval of industrial Internet data attacks, and the multi-source traceability method has the weakest ability to accurately define the sample interval. The definition ability of big data traceability method lies between the two methods, that is, the convolutional neural network based traceability method is most suitable for accurately defining the network

area of data attacks, The original intention of the design is to avoid multi-stage delay in the industrial Internet.

5 Conclusion

In order to ensure the data quality after big data platform processing and the process of debugging result data generation, the introduction of data traceability is necessary. Therefore, the traceability of industrial Internet multi-phase data attacks based on convolutional neural network is a topic worthy of research. Firstly, the traceability information metadata model of the model workflow is designed, and a data sample traceability method based on convolutional neural network is proposed based on this metadata model, and the advantages and disadvantages of this method are analyzed; Secondly, specific traceability objects are discussed according to the situation; Finally, the whole industrial Internet environment is tested and the feasibility of the system and the effectiveness of the traceability method are demonstrated through experimental analysis, and the expected goal is finally achieved.

References

1. Liu, S., Li, Y., Fu, W.: Human-centered attention-aware networks for action recognition. Int. J. Intell. Syst. **37**(12), 10968–10987 (2022)
2. Zhu, Y., Liu, X.: Big data visualization of the quantification of influencing factors and key monitoring indicators in the refined oil products market based on fuzzy mathematics. J. Intel. Fuzzy Sys. Appl. Eng. Technol. **40**(4), 6219–6229 (2021)
3. Le, D.-N., Parvathy, V.S., Gupta, D., et al.: IoT enabled depthwise separable convolution neural network with deep support vector machine for COVID-19 diagnosis and classification. Int. J. Machi. Learn. Cybern. **12**(11), 3235–3248 (2021)
4. Chattopadhyay, A., Mitra, U.: Security against false data-injection attack in cyber-physical systems. IEEE Trans. Cont. Netw. Sys. **7**(2), 1015–1027 (2020)
5. Youzhi, F., Yunfeng, Z.: Simulation of automatic encryption algorithm for high-speed network multi-segment support data. Computer Simulation **38**(12), 237–240 (2021)
6. Li, H., Spencer, B.F., Champneys, M.D., et al.: On the vulnerability of data-driven structural health monitoring models to adversarial attack. Structural Health Monitoring **20**(4), 1476–1493 (2021)
7. Mahapatra, K., Ashour, M., Chaudhuri, N.R., et al.: Malicious corruption resilience in PMU data and wide-area damping control. IEEE Trans. Smart Grid **11**(2), 958–967 (2020)
8. Battur, R., Amboji, J., Deshpande, A., et al.: A Distributed deep learning system fornweb attack detection on edge devices. Control. Eng. Pract. **4**(11), 25–36 (2020)
9. Moussa, B., Al-Barakati, A., Kassouf, M., et al.: Exploiting the vulnerability of relative data alignment in phasor data concentrators to time synchronization attacks. IEEE Transactions on Smart Grid **11**(3), 2541–2551 (2020)
10. Bordel, B., Alcarria, R., Robles, T.: Denial of chain: evaluation and prediction of a novel cyberattack in blockchain-supported systems. Futur. Gener. Comput. Syst. **116**(11), 426–439 (2021)