DANTD: A Deep Abnormal Network Traffic Detection Model for Security of Industrial Internet of Things Using High-Order Features

Guolong Shi, Xinyi Shen, Fuke Xiao, and Yigang He

***Abstract*—With the development of blockchain, artificial intelligence, and data mining technology, abnormal network traffic data has become easy to obtain. The traffic detection model detects the traffic patterns in the network to find abnormal traffic that does not conform to the normal traffic law, which has great security significance for Industrial Internet of Things (IIoT) networks and devices in real scenarios. However, previous abnormal detection models rely on expert experience and cannot cope with real-time changes in IIoT scenarios. The manual features cannot be sufficiently representative and adaptive. Moreover, there are few abnormal traffic data in real scenarios, which makes the model unable to fully learn the potential distribution in abnormal data. Therefore, in this work, we propose a deep abnormal network traffic detection model (DANTD) for the security of IIoT using high-order features and novel data augmentation strategies. The DANTD model first adopts a deep convolutional autoencoder to extract effective high-order features to make it more representative. Then, the DANTD model uses generative adversarial networks as data augmentation strategies to enrich the abnormal data, so that the model can fully consider the information of the data distribution. Comprehensive experiments on real IIoT data sets validate the effectiveness of the DANTD model.**

***Index Terms*—Convolutional neural networks (CNNs), detection model, generative adversarial networks (GANs), Industrial Internet of Things (IIoT).**

I. Introduction

With the improvement of the network transmission level, hardware storage, blockchain technology, and computing capabilities, the Internet of Things (IoT) has developed rapidly, and the Industrial IoT (IIoT) has received much attention [1], [2]. As the application of IoT technology in the field of industrial automation production, the IIoT includes technologies, such as edge computing, big data analysis, and intelligent sensing, which realizes the intelligent management of industrial control systems [3], [4], [5]. The production efficiency of the factory can be greatly improved, and the cost of production management can be effectively reduced. And the emergence of blockchain technology facilitates the sharing of abnormal traffic data among enterprises. This is because blockchain technology uses a distributed network to achieve decentralization, thereby improving the security of IIoT network data [6], [7].

However, the deployment of a large number of wirelessly transmitted smart devices increases the risk of IIoT attacks [8], [9], [10]. Attackers can attack local devices first, and then expand their attack range through intermediate nodes, which brings a huge threat to network security and seriously affects industrial production. Therefore, through intelligent analysis of IIoT network traffic, early detection of abnormal traffic in the network and network attack behaviors have great security significance for IIoT networks and devices in real scenarios [11], [12], [13], [14].

Artificial intelligence and data mining technology has been successful in other areas, and the same applies to the IIoT. The abnormal traffic detection model is an important means to maintain IIoT security. It detects the traffic patterns in the network to find abnormal traffic that does not conform to the normal traffic law. However, the existing abnormal detection models of the IIoT face the following difficulties. First, the actual field conditions of the equipment are very complex, which leads to the high-dimensional flow data collected by the sensor equipment. However, the existing IIoT abnormal detection models rely on the experts to manually construct the traffic data, which leads to these manual features are not representative enough and may lose important features. In addition, these manual features have the poor adaptive ability because they do not mine the essence of abnormal traffic. With the changes in the operating environment and structure of the IIoT, in order to detect new unknown attacks, it is necessary to continuously construct and adjust the model, which results in a lot of waste of time and labor. And because the network structure of the previous IIoT abnormal detection model is relatively simple, these manual features with weak representative ability cannot

Manuscript received 2 October 2022; revised 16 January 2023 and 16 February 2023; accepted 4 March 2023. Date of publication 7 March 2023; date of current version 7 December 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 62303018; in part by the National Key Research and Development Plan "Smart Grid Technology and Equipment" Special "Key Technologies of Power Internet of Things" Project "Integration and Application Verification of Key Technologies of Power Internet of Things"; in part by the China Postdoctoral Fund General Project under Grant 2021M692473; in part by the Natural Science Foundation of Anhui Province under Grant 2108085QF260; in part by the Open Research Fund of National Engineering Research Center for Agro-Ecological Big Data Analysis and Application, Anhui University under Grant AE202103; and in part by the Anhui Provincial Department of Education Research Project under Grant KJ2021A0179. *(Corresponding authors: Guolong Shi; Yigang He.)*

Guolong Shi is with the School of Information and Computer, Anhui Agricultural University, Hefei 230036, China, and also with the School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China (e-mail: shiguolong@whu.edu.cn).

Xinyi Shen and Fuke Xiao are with the School of Information and Computer, Anhui Agricultural University, Hefei 230036, China (e-mail: sxy@stu.ahau.edu.cn; xfk@stu.ahau.edu.cn).

Yigang He is with the School of Electrical Engineering and Automation, Wuhan University, Wuhan 430072, China (e-mail: yghe1221@whu.edu.cn).

Digital Object Identifier 10.1109/JIOT.2023.3253777

form an effective nonlinear mapping for the internal distribution of large-scale data sets, resulting in a relatively low fitting ability of the model [15], [16].

Convolutional neural networks (CNNs) have achieved great success in computer vision. This is largely due to its strong ability to extract features. Therefore, in this work, we employ CNN to extract effective features from traffic data, enabling them to outperform the expressiveness of manual features. The reason it works has been proven in computer vision.

Second, in the real IIoT environment, the amount of normal traffic data is large, while the categories of abnormal traffic data are many but the number of each category is small [17], [18]. In the process of training the model, the lack of abnormal traffic data makes the model unable to fully learn the underlying distribution in the abnormal data. This makes the existing IIoT abnormal detection models biased toward a large amount of normal traffic data. However, the detection effect of the model on a small number of abnormal data is not good.

Therefore, in this work, we address the two issues discussed above and propose a deep abnormal network traffic detection model (DANTD) for the security of IIoT using high-order features and novel data augmentation strategies. First, in order to extract representative latent features from high-dimensional traffic data, the DANTD model uses a deep convolutional autoencoder to perform high-order feature extraction on traffic data. Briefly, the deep convolutional autoencoder consists of convolutional layers, bath normalization layers, ReLU function, pooling layers, and fully connected layers. The function of the convolution layer is mainly to extract effective features from the high-dimensional IIoT traffic; the purpose of the pooling layer is to reduce the dimension of the latent feature without losing useful information, thereby reducing the total number of parameters of the model; the bath normalization layers aim to prevent the network from being too complicated; the fully connected layer has two functions: the first one is to restore the original high-dimensional traffic data; and the second function is to predict the category of traffic. Furthermore, in order to balance the amount of normal data and various abnormal data in the data set, the DANTD model utilizes deep generative adversarial networks (GANs) as data augmentation strategies to augment abnormal data. GAN [19], [20] models are essentially unsupervised learning network architectures. We input various abnormal traffic data into the trained GAN model, and the output is a generated fake sample. We put these generated fake samples into the training set to augment the amount of abnormal data for the corresponding category. The DANTD model can better learn appropriate parameters by training on the expanded training set, thereby improving the detection accuracy of the minority class. We conduct extensive experiments on real IIoT traffic data sets to verify the superiority of the DANTD model.

The main contributions of this work are as follows.

1) The DANTD model novelly utilizes a deep convolutional autoencoder to extract high-order latent features from high-dimensional traffic data, enabling it to have better predictive performance.
2) The DANTD model uses the GAN model as data augmentation strategies to expand the amount of abnormal data, so that the amount of each type of traffic data reaches a balanced state, thereby improving the performance of the DANTD model.
3) The DANTD model has undergone extensive experiments on real IIoT data sets, which has verified its effectiveness and practicability.

The contents of the remaining section are arranged as follows. Section II introduces the related work. Section III presents the details of the DANTD model. Section IV shows the experimental result. Section V concludes the content of this work and a discussion of directions for future work.

II. Related Work

In this section, we first introduce related work on some application scenarios of abnormal detection techniques. Then, we introduce the related work of abnormal detection technology in the IIoT [21], [22], [23], [24], [25].

A. Abnormal Detection

Zhang et al. [26] proposed a novel feature engineering-based unsupervised model for detecting abnormal electrical behavior. They argue that traditional research efforts only focus on improving the structure of the model while ignoring improvements in feature engineering. The model first constructs the original feature set manually, and then uses the correlation between the features to select the optimal feature set that can reflect the user's electricity consumption behavior. Finally, in the prediction stage, the model uses a density-based clustering algorithm to detect abnormal electricity consumption behavior.

Xie et al. [27] proposed an abnormal detection model for industrial control systems. The previous abnormal detection models of industrial control systems use network event logs as input and do not consider the correlation and dependence between multiple variables in industrial systems, so the detection effect of unknown and new attacks is poor. They used a 1-D-CNN with a gated recurrent unit structure to learn the correlations and dependencies between parameters in industrial systems. The model shows good detection results on the safe water treatment data set.

Based on the single classification of the support vector model, Li et al. [28] proposed an abnormal detection model for the controller area network in the Internet of Vehicles. Because abnormal data in the past Internet of Vehicles is relatively rare, various message rules are difficult to parse, resulting in difficult deployment and low prediction accuracy. The model proposed by Li et al. can handle large-scale data and reduce computational cost while ensuring detection accuracy.

Yun-Mei et al. [29] proposed a 3-D convolution-based model for detecting anomalies in electroencephalogram (EEG) signals. They fused multiple EEG signals into a larger benchmark data set. And they constructed a 28-layer deep residual network to learn high-order features in EEG signals, so that abnormal signals can be identified.

Wei et al. [30] used a two-stream fully CNN to detect anomalies in crowds. The previous methods all construct complex manual features for surveillance video, but these features are affected by computational complexity and scene transformation, so the detection accuracy is not high. Therefore, they use a two-stream fully CNN to extract features from surveillance video, so that more appearance information and motion information can be obtained, which makes the model have high detection ability.

B. Network Traffic Abnormal Detection in IIoT

Liang et al. [31] proposed a variational few-shot learning model for network intrusion detection in IIoT. Due to the limited computing power of edge devices, previous detection models have major flaws in handling imbalanced data sets. Therefore, they employ variational few-shot learning to overcome specific distributions in imbalanced data sets, thereby improving the performance of intrusion detection models. On multiple real data sets, they validate the effectiveness of the model, especially, against the new attack of category imbalance.

Telikani et al. [32] also proposed a solution to the problem of data imbalance in the IIoT, which would reduce the monitoring effect of the abnormal flow monitoring model. They combined stacked autoencoders and CNN into a new hybrid model and optimized parameters in the model with a newly designed cost-dependent loss function. A large number of experimental results show that the model can effectively deal with the imbalance of traffic data in the IIoT, which has good scalability.

Abdel-Basset et al. [33] proposed a deep neural network model for detecting network intrusion in IIoT traffic. The model first learns local features of flow data using local gated recurrent units. The model then utilizes a multihead attention mechanism to learn the global features of the traffic data. And a residual connection is added to the neural network to prevent information loss. Finally, they verified the effectiveness of the method on real data sets.

Li et al. [34] believed that the existing deep-learning-based abnormal detection models have not fully utilized their potential when dealing with 1-D data, resulting in poor detection results. Therefore, they proposed a multi-CNN intrusion detection model. The model first uses correlation to divide the original feature data into four parts, and then converts these features into grayscale images. Next, CNNs are introduced into the intrusion detection problem. Extensive experimental results show that the model exhibits the advantages of high precision and low complexity on existing real data sets.

Zhou et al. [35] proposed a variational long-short-term memory network based on reconstructed feature representations to detect abnormal traffic in the IIoT. They design an encoder-decoder network associated with variational reparameterization, capable of learning low-dimensional feature representations from high-dimensional raw traffic data. And they define three loss functions for constraining low-dimensional feature representations. Finally, this feature representation is fed into a lightweight network, where anomalies have been detected.

Most of the above-mentioned abnormal detection models rely on manual features and lose the interaction information between features. In addition, these manual features have poor self-adaptability and cannot cope with changes in the operating environment and structure of the IIoT. When a new attack mode appears, the model needs to be continuously constructed and adjusted, resulting in a lot of time and labor waste. Second, during the training process of the above-mentioned abnormal detection model, there is less abnormal traffic data, which makes the model unable to fully learn the potential distribution in the abnormal data. As a result, the detection effect of the model on a small amount of abnormal data is not good.

III. Method

In this section, we first describe how to obtain traffic data from an IIoT platform. We then introduce the implementation details of the DANTD model, including how to extract high-order features with a deep convolutional autoencoder and augment the amount of abnormal data with a GAN model.

A. Using IIoT Platforms to Capture Traffic Data

The architecture of the IIoT platform is shown in Fig. 1. The IIoT platform consists of a device layer, a gateway layer, and a cloud service layer. The device layer is mainly composed of various physical devices and sensors. The relevant data is then passed to the gateway layer. The gateway layer is composed of wireless networks, gateways, hubs, and other devices, and parses the received information and transmits it to the cloud service layer. The cloud service layer stores related traffic data, which can perform various calculations on these data to achieve a certain service. We mainly use the traffic data of the cloud service layer as the training data of the DANTD model. In addition, blockchain technology can enhance the security of data in IIoT platforms.

B. High-Order Feature Extraction Using Deep Convolutional Autoencoders

Fig. 1 shows the operation of the DANTD model to extract high-order features from high-dimensional traffic data and generate predicted values using a deep convolutional autoencoder. First, we look at the traffic data T in the IIoT. The actual field conditions of the equipment are very complex, resulting in the T collected by the sensor equipment being all high-dimensional flow data. The manual features constructed by expert knowledge do not discover the essence of abnormal traffic, resulting in poor adaptive ability. In particular, the operating environment and structure of the IIoT will continue to change, and these manual features alone cannot detect new types of attacks.

Therefore, in order to extract representative latent features from high-dimensional traffic data, the DANTD model uses a deep convolutional autoencoder to perform feature extraction on traffic data. As shown in Fig. 2, DANTD inputs T into a series of convolution and pooling operations. Among them, convolutional layers, batch normalization, ReLu activation

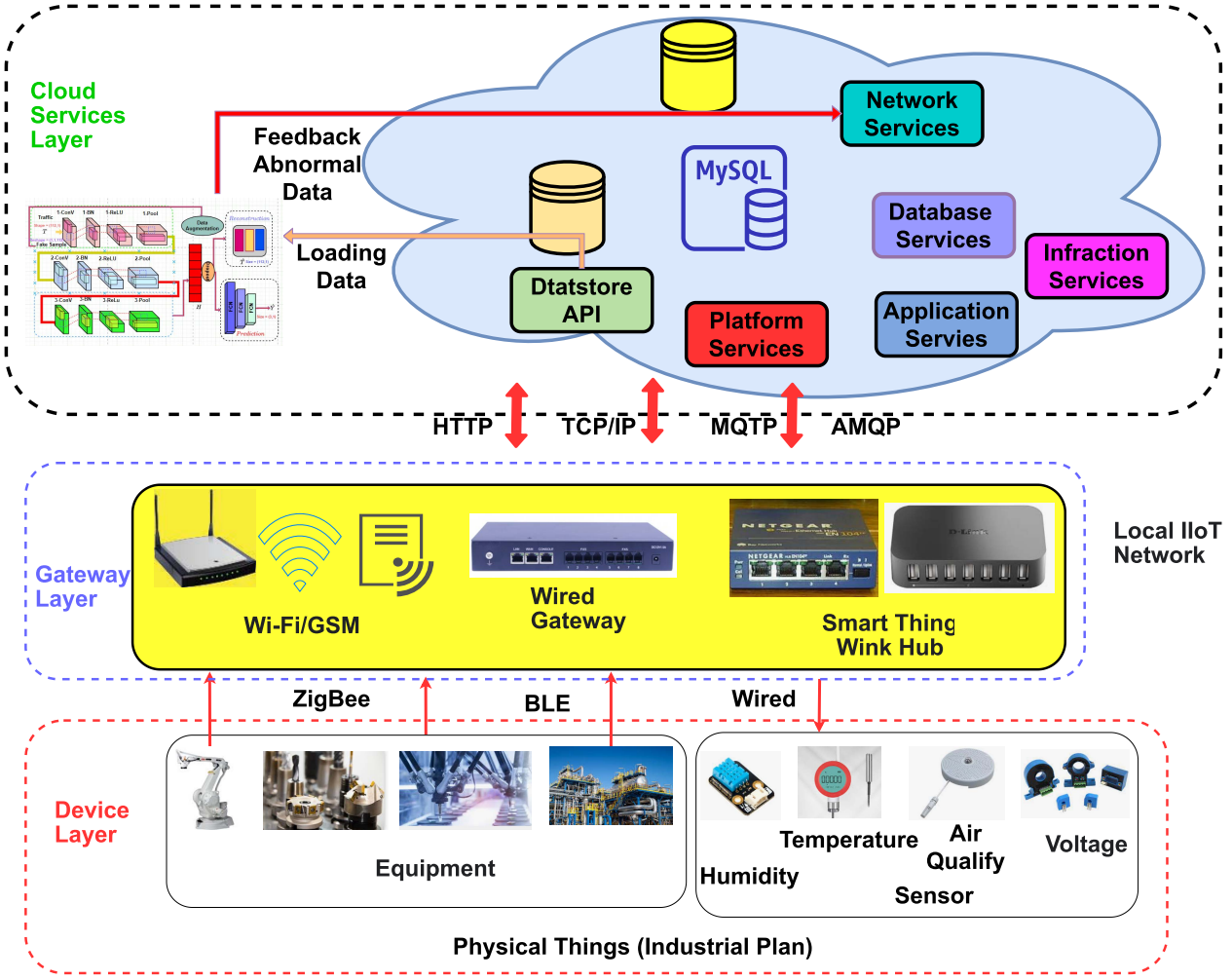


Fig. 1. Process of acquiring real-time traffic data from the IIoT platform in the DANTD model proposed in this work.

function, and pooling layer constitute a block. The function of the convolutional layer is mainly to extract effective features from the high-dimensional IIoT traffic; the purpose of the pooling layer is to reduce the dimension of the feature without losing useful information. Besides, we reshape the 1-D traffic data into tensors of a specific structure, so that it can meet the input format of the CNN

$$H_1 = \mathrm{ConV}\left(T, C^1\right) \tag{1}$$

$$H_2 = \mathrm{BN}(H_1) \tag{2}$$

$$H_3 = \mathrm{ReLU}(H_2) \tag{3}$$

$$H_4 = \mathrm{Pool}(H_3). \tag{4}$$

As shown in (1)–(4), a block contains convolutional layers, batch normalization, ReLU activation function, and pooling layer. ConV stands for convolutional layer. BN stands for batch normalization, ReLU stands for ReLu activation function, and Pool stands for pooling layer. H and C are the output and corresponding parameters of each layer, respectively. As shown in (5), after the calculation of multiple blocks, we get the latent features H of the traffic data T

$$H = \mathrm{Block}(\mathrm{ConV}, \mathrm{Pool}, \mathrm{BN}, \mathrm{ReLU}) + \mathrm{Dropout} \tag{5}$$

where Block is composed of multiple blocks. The Dropout layer is used to reduce redundant information. Then, as shown in (6) and (7), we input H into different fully connected networks through the flattening operation to generate reconstructed original traffic data $\hat{T}$ and the detection category $\hat{Y}$ for this traffic data

$$\hat{T} = \mathrm{ResCon}(H) \tag{6}$$

$$\hat{Y} = \mathrm{Predictor}(H). \tag{7}$$

We can choose to minimize the error between the original traffic T and the reconstructed traffic $\hat{T}$, which can improve the accuracy of some data. Similarly, we can also choose not to perform the above-mentioned error minimization operation to avoid additional calculation requirements. These latent features with strong representation ability, which can form an effective nonlinear mapping to the intrinsic distribution of large-scale data sets, thereby enhancing the fitting ability of the DANTD model. And H is able to adapt to new cyber-attacks, allowing it to be quickly detected and alerted

$$\mathrm{Loss} = \mathrm{CrossEntropyLoss}\left(\hat{Y}, Y\right). \tag{8}$$

As shown in (8), we use the cross-entropy loss function in python to learn the values of the above parameters, where Y

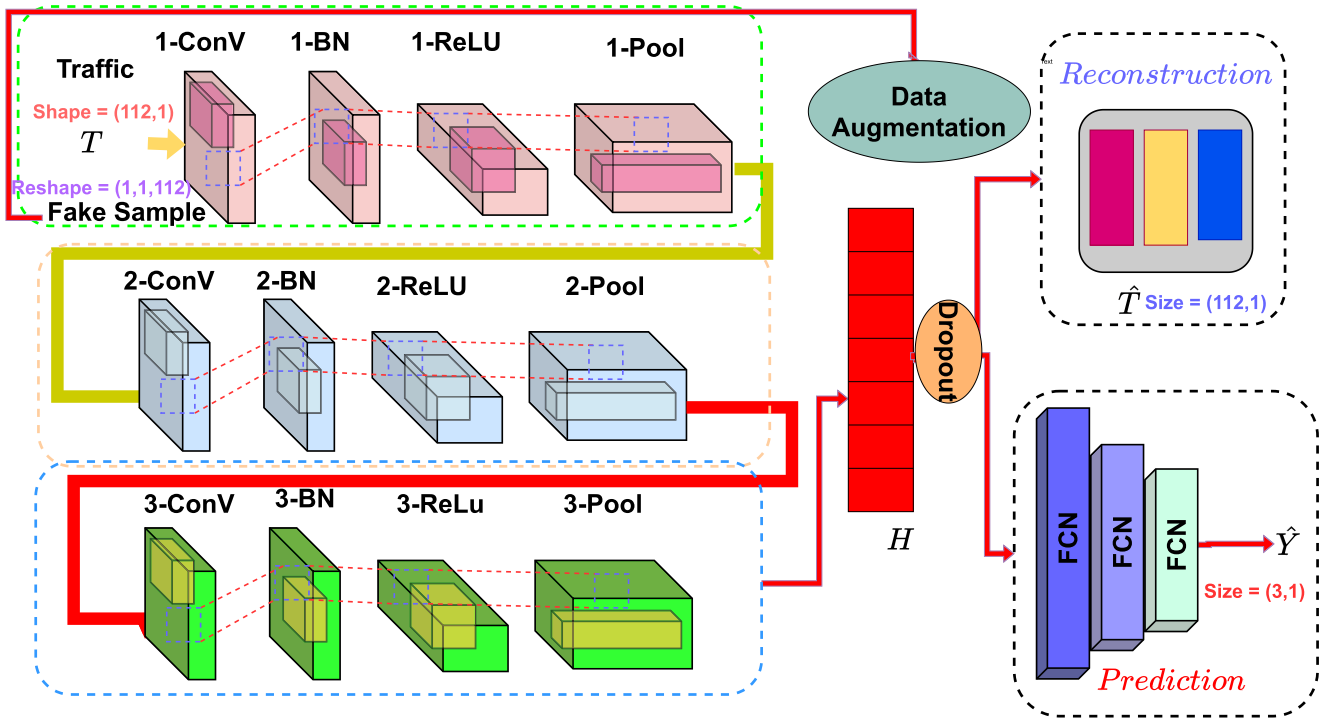


Fig. 2. Framework of the DANTD model proposed in this work for detecting abnormal traffic.

is the category of traffic data, and $\hat{Y}$ is the traffic category predicted by the model.

C. Using GAN Model as Data Augmentation Strategies to Augment the Amount of Abnormal Data

Fig. 3 shows that the DANTD model augments abnormal sample data with a GAN model. The reason for this is as follows. In a real IIoT environment, the amount of normal traffic data is large, while the categories of abnormal traffic data are many but the number of each category is small. In the process of training the model, the lack of abnormal traffic data makes the model unable to fully learn the underlying distribution in the abnormal data. This makes the existing IIoT abnormal detection models biased toward a large amount of normal traffic data. However, the detection effect of the model on a small number of abnormal data is not good.

The DANTD model first uses (9) to input random noise Noise into the generator to produce fake flow data Fake. Then the fake traffic data and the real traffic data are input into the discriminator as shown in (10), so that the discriminator distinguishes the real data from the false data. Through the continuous confrontation training of the generator and the discriminator, it is finally possible to generate fake traffic data that can be confused with the real data. In this work, we use a random generation function in python to generate noise that conforms to a normal distribution. The reason why we use this method of noise generation is that it is simple and fast. The generator is composed of multiple fully connected neural networks, and the discriminator is composed of CNN

$$\text{Fake} = G(\text{Noise}) \tag{9}$$

$$\text{Label} = D(\text{Fake}, T). \tag{10}$$

Algorithm 1 DANTD Model

Input: The traffic data T in the IIoT, T
Output: The predicted detection category $\hat{Y}$ for T, $\hat{Y}$

Feature Extraction Using Deep Convolutional Autoencoders
  The First Layer
  $H_1 \leftarrow ConV(T, C^1)$
  $H_2 \leftarrow BN(H_1)$
  $H_3 \leftarrow ReLU(H_2)$
  $H_4 \leftarrow Pool(H_3)$
  The Second Layer
  $H_1^2 \leftarrow 2 - ConV(H_4, C^2)$
  $H_2^2 \leftarrow 2 - BN(H_1^2)$
  $H_3^2 \leftarrow 2 - ReLU(H_2^2)$
  $H_4^2 \leftarrow 2 - Pool(H_3^2)$
  The Third Layer
  $H_1^3 \leftarrow 3 - ConV(H_4^2, C^3)$
  $H_2^3 \leftarrow 3 - BN(H_1^3)$
  $H_3^3 \leftarrow 3 - ReLU(H_2^3)$
  $H_4^3 \leftarrow 3 - Pool(H_3^3)$
  The Block Function
  $H \leftarrow Block(ConV, Pool, BN, ReLU) + Dropout$
  $\hat{T} \leftarrow ResCon(H)$
  $\hat{Y} \leftarrow Predictor(H)$
Augmenting the Amount of Abnormal data with GAN Model
  $Fake \leftarrow G(Noise)$
  $Label \leftarrow D(Fake, T)$
Return $\hat{Y}$

Finally, we put these generated fake samples into the training set to expand the number of abnormal data. The DANTD model can better learn appropriate parameters by training on the expanded training set, thereby improving the detection accuracy of the minority class. The above parameters are all learned using the Adam optimizer, where the learning rate

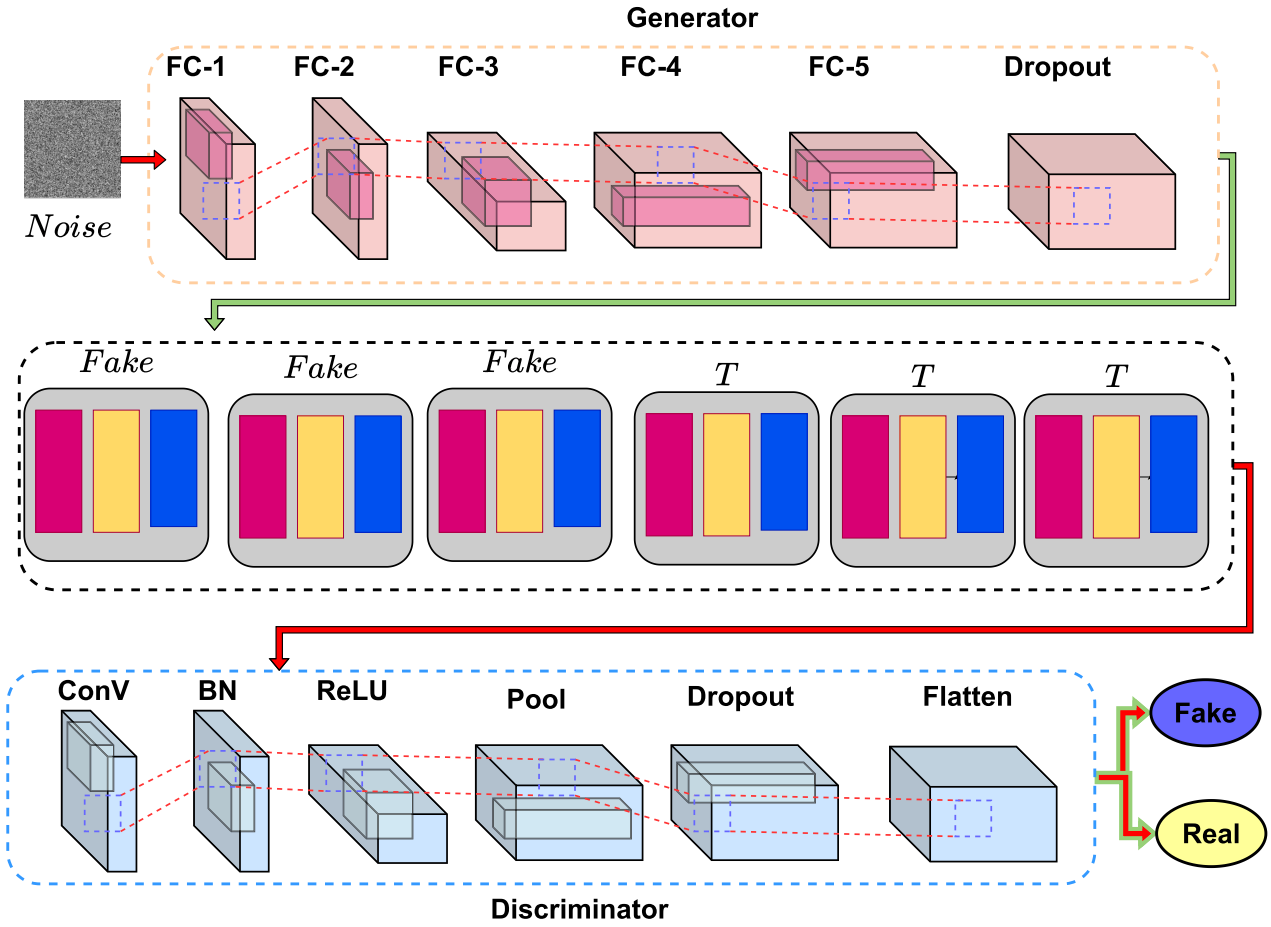


Fig. 3. Data augmentation strategies proposed in the DANTD model.

is used as a hyperparameter to adjust the gradient update rate. The pseudocode of the DANTD model is shown in Algorithm 1.

IV. Results and Discussion

A. Data Set

This work uses a real network security data set, which includes five types of traffic data, including normal network traffic (Normal), denial of service (DOS), remote attack (R2L), detection attack (Probe), and access permission (U2R). A DOS attack works by flooding the target server with traffic, making it inaccessible. The R2L attack is an illegal operation through remote login to a computer. Probe attacks collect network information through various means. The U2R attack is to obtain root authority through illegal means. The numbers of the above types of data are 67 343, 45 927, 11 656, 995, and 52, respectively. Due to the small amount of Probe and U2R data, we only consider Normal, DOS, and R2L data in this work.

B. Experimental Setup

Abnormal traffic detection in this work is actually a multi-classification task. We propose that the input of the model is network traffic, and the output is the type of network traffic. We divide all the traffic data into a training set and a test set in a ratio of 7:3, where the former is used to train the parameters in the model and the latter is used to evaluate the generalization performance of the model. And in order to intuitively show the performance differences between the models, we selected four popular evaluation metrics. The four evaluation metrics are Accuracy, Precision, Recall, and F-Score.

C. Effect of Learning Rate on DANTD Model

The learning rate is a hyperparameter of the DANTD model. We observe the performance of the DANTD model under different learning rates through the following experiments. The details of this experiment are that the learning rate varies within the interval $[0.001, 0.005, 0.01, 0.05, 0.1]$, while the other hyperparameters of the DANTD model remain unchanged. The experimental results are shown in Fig. 4. When we observe Fig. 4, we can find that the effect of the learning rate on the DANTD model is basically the same under the four evaluation metrics. The DANTD model performs best when the learning rate is 0.005. The above results mean that the value of the learning rate should not be too large, which will cause the DANTD model to ignore better parameter values. At the same time, the value of the learning rate should not be too small, which will cause the optimization speed of the DANTD model to be too slow.

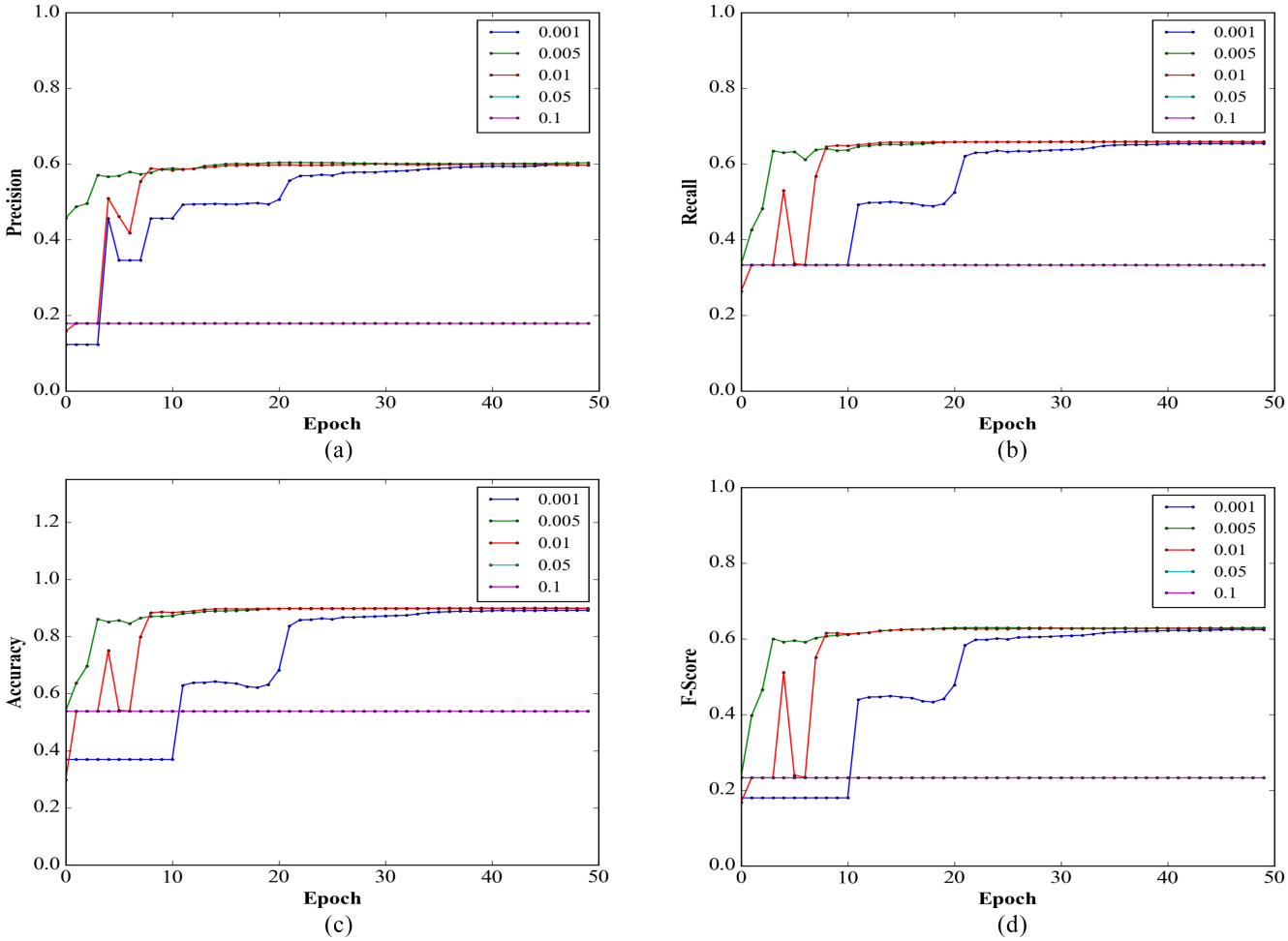


Fig. 4. Effect of learning rate on the DANTD model. (a) Precision. (b) Recall. (c) Accuracy. (d) F-Score.

D. Effect of the Dimension of Latent Feature H on the DANTD Model

In (7), the dimension of H is a hyperparameter of the DANTD model. We observe the performance of the DANTD model in different dimensions of H through the following experiments. The details of this experiment are that the dimensions vary in the interval $[30, 60, 120, 240, 480]$, while the other hyperparameters of the DANTD model are unchanged. The experimental results are shown in Fig. 5.

When we observe Fig. 5, we can find that the influence of the dimension of H on the DANTD model is basically the same under the four evaluation metrics. The DANTD model performs best when the dimension of H is 240, which means that the value of the dimension of H should not be too large, which will cause H to contain too much redundant information, resulting in a decrease in the generalization ability of the DANTD model. At the same time, the value of the dimension of H should not be too small, which will cause H to not contain valuable information, which will also lead to poor generalization performance of the DANTD model.

E. Effect of the Dropout Layer on the DANTD Model

As shown in (5), the DANTD model uses the dropout layer to reduce redundant information. Fig. 6 shows the impact of different dropout layers on the DANTD model. The parameters of the dropout layer vary between the interval $[0.1, 0.3, 0.5, 0.7, 0.9]$. We can clearly observe that different parameters have different effects on the DANTD model. Therefore, we need to learn the optimal dropout parameters on the validation set, so as to enhance the predictive ability of the DANTD model on the test set.

F. Comparison With Three Popular Algorithms

1) *EvolCostDeep [32]:* The EvolCostDeep model combined stacked autoencoders and CNN into a new hybrid model, and optimized parameters in the model with a newly designed cost-dependent loss function.
2) *MCNNF [34]:* The multi-CNN fusion model (MCNNF) is a detection algorithm based on CNN and feature correlation.
3) *CNN [16]:* The CNN model extracts the features through convolution operations, and then uses these features to detect traffic anomalies.

Table I presents the experimental results of the DANTD model with three popular algorithms. The values of the DANTD model under the metrics of Precision, Recall, Accuracy, and F-Score are 0.6, 0.659, 0.899, and 0.628, respectively. The values of the EvolCostDeep model under

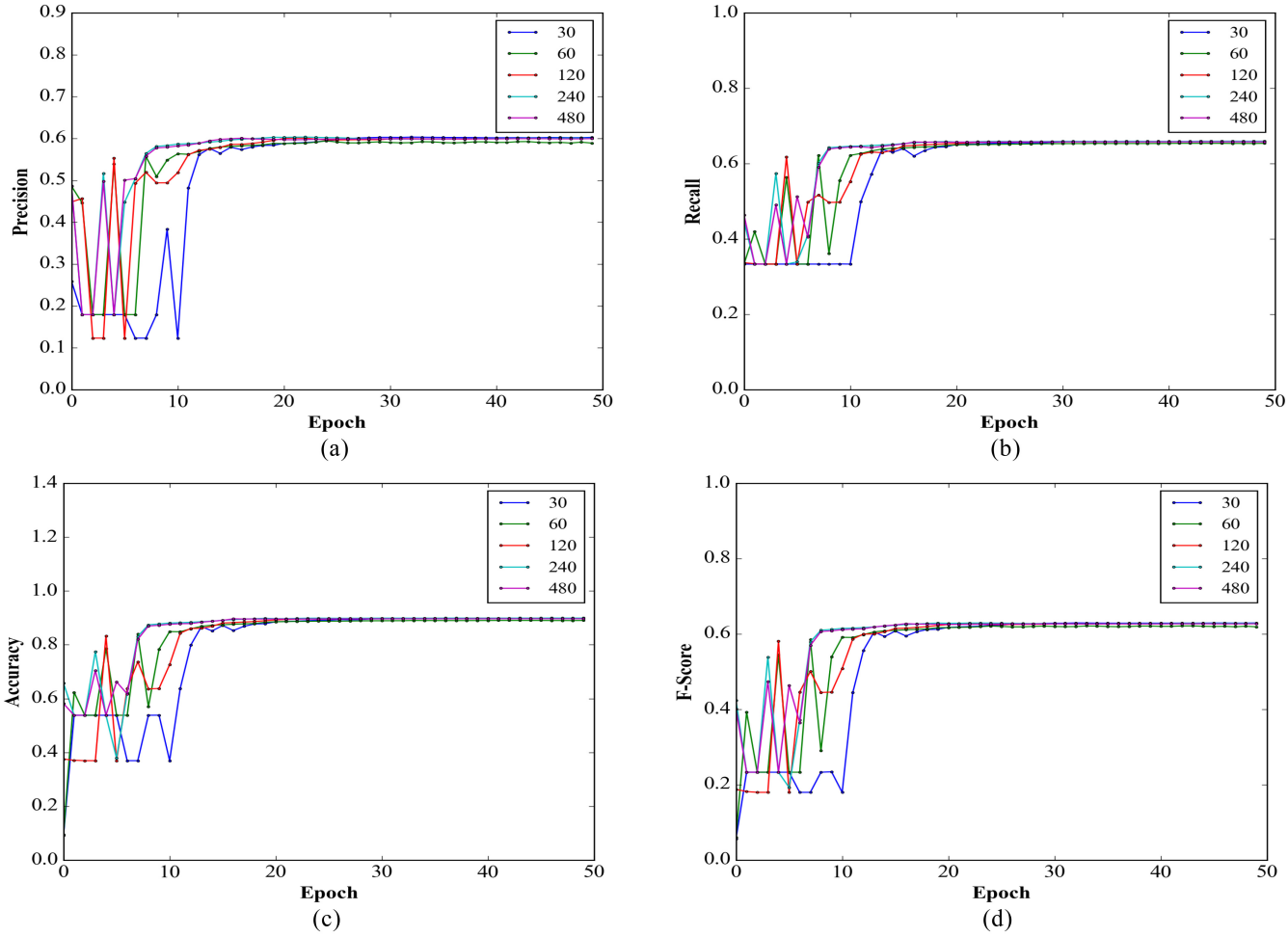


Fig. 5. Effect of the dimension of H on the DANTD model. (a) Precision. (b) Recall. (c) Accuracy. (d) F-Score.

TABLE I
EXPERIMENTAL RESULTS OF THE DANTD MODEL AND BENCHMARKS

Methods	Precision	Recall	Accuracy	F-Score
CNN	0.568	0.631	0.855	0.594
MCNNF	0.588	0.641	0.876	0.613
EvolCostDeep	0.594	0.645	0.882	0.618
DANTD	**0.6**	**0.659**	**0.899**	**0.628**

TABLE II
EXPERIMENTAL RESULTS OF THE DANTD MODEL WITH DIFFERENT LEARNING RATES (MAXIMUM VALUE)

Methods	Precision	Recall	Accuracy	F-Score
DANTD-0.001	0.598	0.654	0.891	0.624
DANTD-0.005	0.603	0.659	0.899	0.629
DANTD-0.01	0.599	0.658	0.897	0.627
DANTD-0.05	0.179	0.333	0.538	0.233
DANTD-0.1	0.179	0.333	0.538	0.233

the Precision, Recall, Accuracy, and F-Score metrics are 0.594, 0.645, 0.882, and 0.618, respectively. The values of the MCNNF model under the Precision, Recall, Accuracy, and F-Score metrics are 0.588, 0.641, 0.876, and 0.613, respectively. The values of the CNN model under the Precision, Recall, Accuracy, and F-Score metrics are 0.568, 0.631, 0.855, and 0.594, respectively. We can easily find that the DANTD model achieves the best performance under all metrics, which shows the effectiveness of the improvement points in this work. Tables II–IV and Figs. 7–9 show the detailed performance of the DANTD model based on the above hyperparameter experiments. The above figures and tables can more directly observe the performance of the DANTD model under various hyperparameters.

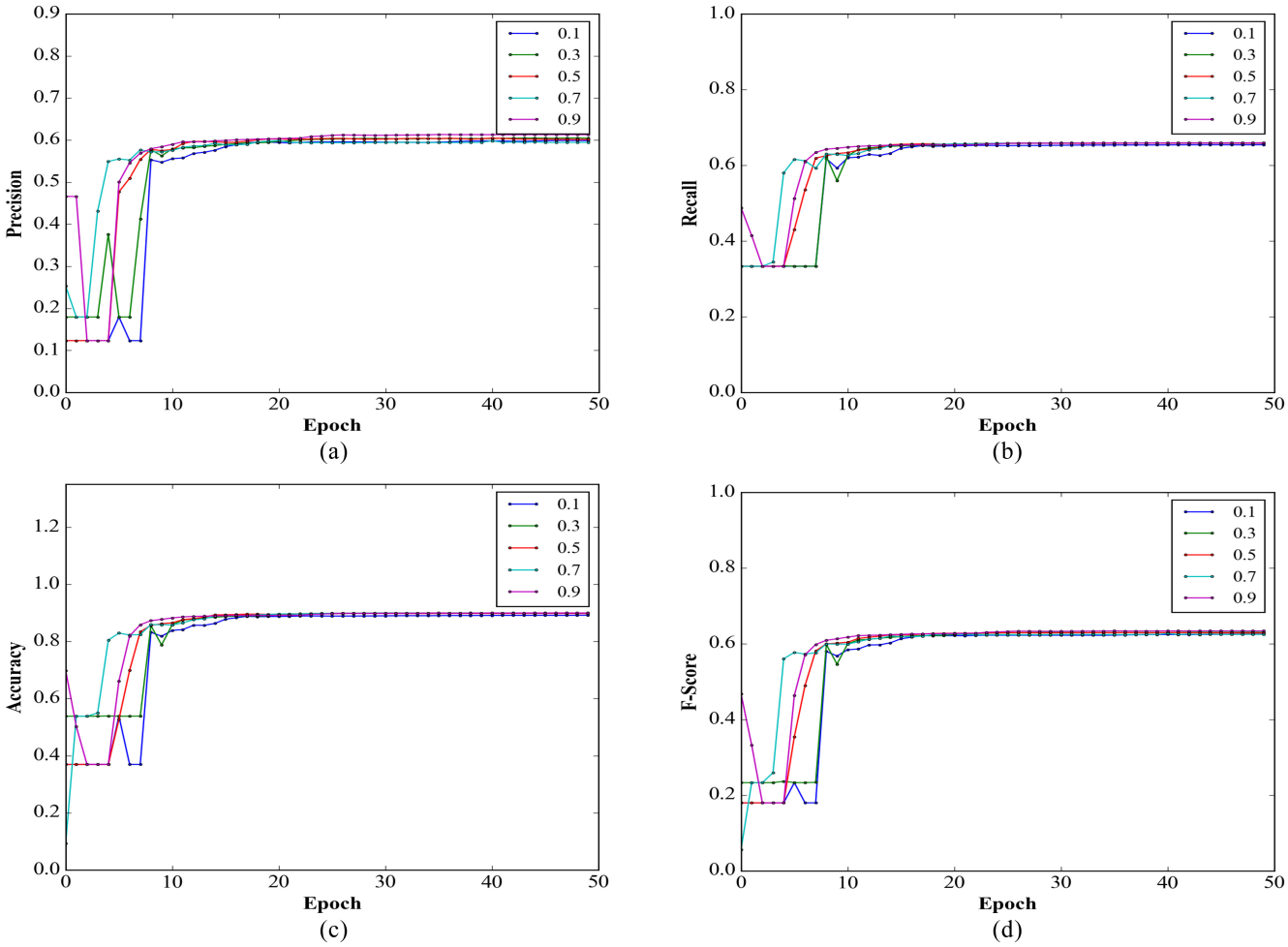


Fig. 6. Effect of dropout layer on the DANTD model. (a) Precision. (b) Recall. (c) Accuracy. (d) *F*-Score.

TABLE III
EXPERIMENTAL RESULTS OF THE DANTD MODEL WITH DIFFERENT *H* (MAXIMUM VALUE)

Methods	Precision	Recall	Accuracy	F-Score
DANTD-30	0.603	0.659	0.898	0.629
DANTD-60	0.594	0.653	0.89	0.621
DANTD-120	0.601	0.659	0.899	0.628
DANTD-240	0.603	0.659	0.899	0.629
DANTD-480	0.6	0.657	0.896	0.627

TABLE IV
EXPERIMENTAL RESULTS OF THE DANTD MODEL WITH DIFFERENT DROPOUT (MAXIMUM VALUE)

Methods	Precision	Recall	Accuracy	F-Score
DANTD-0.1	0.599	0.654	0.891	0.625
DANTD-0.3	0.604	0.659	0.899	0.63
DANTD-0.5	0.604	0.658	0.897	0.629
DANTD-0.7	0.599	0.659	0.899	0.627
DANTD-0.9	0.613	0.659	0.899	0.634

The reason why the DANTD model can achieve good prediction performance is that it uses a deep convolutional autoencoder to extract representative latent features from high-dimensional traffic data, enabling it to have better prediction performance. And the DANTD model uses the GAN model to expand the amount of abnormal data, so that the amount of each type of traffic data reaches a balanced state, thereby improving the performance of the DANTD model. The validity and practicability of the DANTD model are verified by discussing the above experimental results.

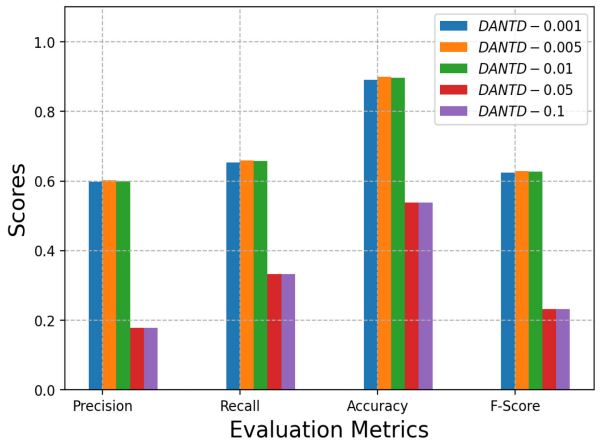


Fig. 7. Experimental results of the DANTD model with different learning rates (maximum value).

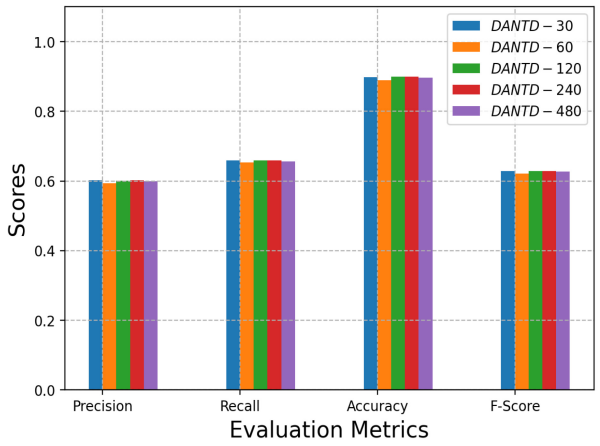


Fig. 8. Experimental results of the DANTD model with different H (maximum value).

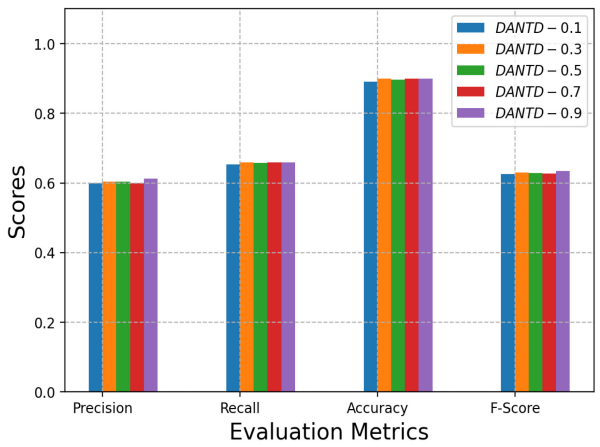


Fig. 9. Experimental results of the DANTD model with different dropout (maximum value).

V. Conclusion

In this work, we propose a DANTD for the security of the IIoT using high-order features and novel data augmentation strategies. The DANTD model relies on a deep convolutional autoencoder to extract the high-order latent features of high-dimensional traffic, enabling it to better represent the original data and, thus, have the better discriminative ability. And the DANTD model generates fake abnormal samples by means of the GAN model, which balances the data distribution to a certain extent, making the model less susceptible to the interference of abnormal points. However, due to the long training time and many model parameters, the DANTD model does not meet the real-time requirements of real-world scenarios. Therefore, in future work, how to lighten the architecture of the DANTD model is the focus of the work. Besides, we will explore how to combine the IIoT platform and blockchain technology to protect the security of private data.

References

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[2] P. K. Malik et al., "Industrial Internet of Things and its applications in industry 4.0: State of the art," *Comput. Commun.*, vol. 166, pp. 125–139, Jan. 2021.

[3] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 2985–2996, May 2021.

[4] W. Z. Khan, M. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial Internet of Things: Recent advances, enabling technologies and open challenges," *Comput. Elect. Eng.*, vol. 81, Jan. 2020, Art. no. 106522.

[5] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on Industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.

[6] A. Bahga and V. K. Madisetti, "Blockchain platform for Industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, 2016.

[7] S. Zhao, S. Li, and Y. Yao, "Blockchain enabled Industrial Internet of Things technology," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1442–1453, Dec. 2019.

[8] X. Li, M. Xu, P. Vijayakumar, N. Kumar, and X. Liu, "Detection of low-frequency and multi-stage attacks in Industrial Internet of Things," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8820–8831, Aug. 2020.

[9] M. A. Alsoufi et al., "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," *Appl. Sci.*, vol. 11, no. 18, p. 8383, 2021.

[10] J. Long, W. Liang, K.-C. Li, Y. Wei, and M. D. Marino, "A regularized cross-layer ladder network for intrusion detection in Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1747–1755, Feb. 2023.

[11] L. Cui et al., "Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3492–3500, May 2022.

[12] E. Gyamfi and A. Jurcut, "Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 22, no. 10, p. 3744, 2022.

[13] D. Wu, Z. Jiang, X. Xie, X. Wei, W. Yu, and R. Li, "LSTM learning with Bayesian and Gaussian processing for anomaly detection in Industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5244–5253, Aug. 2020.

[14] X. Wang et al., "Toward accurate anomaly detection in Industrial Internet of Things using hierarchical federated learning," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7110–7119, May 2022.

[15] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, "A survey of convolutional neural networks: Analysis, applications, and prospects," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 12, pp. 6999–7019, Dec. 2022.

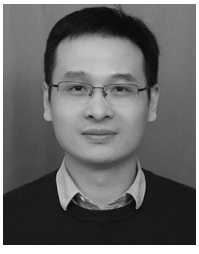
[16] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[17] B. Krawczyk, "Learning from imbalanced data: Open challenges and future directions," *Progr. Artif. Intell.*, vol. 5, no. 4, pp. 221–232, 2016.

[18] H. He and E. A. Garcia, "Learning from imbalanced data," *IEEE Trans. Knowl. Data Eng.*, vol. 21, no. 9, pp. 1263–1284, Sep. 2009.

[19] I. Goodfellow et al., "Generative adversarial networks," *Commun. ACM*, vol. 63, no. 11, pp. 139–144, 2020.

[20] Z. Cai, Z. Xiong, H. Xu, P. Wang, W. Li, and Y. Pan, "Generative adversarial networks: A survey toward private and secure applications," *ACM Comput. Surveys*, vol. 54, no. 6, pp. 1–38, 2021.
[21] H. Gao, B. Qiu, R. J. D. Barroso, W. Hussain, Y. Xu, and X. Wang, "TSMAE: A novel anomaly detection approach for Internet of Things time series data using memory-augmented autoencoder," *IEEE Trans. Netw. Sci. Eng.*, early access, Mar. 29, 2022, doi: 10.1109/TNSE.2022.3163144.
[22] J. Lan, X. Liu, B. Li, J. Sun, B. Li, and J. Zhao, "MEMBER: A multi-task learning model with hybrid deep features for network intrusion detection," *Comput. Secur.*, vol. 123, Dec. 2022, Art. no. 102919.
[23] Y. Zhang, C. Yang, K. Huang, and Y. Li, "Intrusion detection of Industrial Internet of Things based on reconstructed graph neural networks," *IEEE Trans. Netw. Sci. Eng.*, early access, Jul. 1, 2020, doi: 10.1109/TNSE.2022.3184975.
[24] W. Ullah et al., "Artificial intelligence of things-assisted two-stream neural network for anomaly detection in surveillance big video data," *Future Gener. Comput. Syst.*, vol. 129, pp. 286–297, Apr. 2022.
[25] X. Zhou, Y. Hu, J. Wu, W. Liang, J. Ma, and Q. Jin, "Distribution bias aware collaborative generative adversarial network for imbalanced deep learning in Industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 570–580, Jan. 2023.
[26] W. Zhang, X. Dong, H. Li, J. Xu, and D. Wang, "Unsupervised detection of abnormal electricity consumption behavior based on feature engineering," *IEEE Access*, vol. 8, pp. 55483–55500, 2020.
[27] X. Xie, B. Wang, T. Wan, and W. Tang, "Multivariate abnormal detection for industrial control systems using 1D CNN and GRU," *IEEE Access*, vol. 8, pp. 88348–88359, 2020.
[28] X. Li et al., "CAN bus messages abnormal detection using improved SVDD in Internet of Vehicles," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3359–3371, Mar. 2022.
[29] D. Yun-Mei et al., "The abnormal detection of electroencephalogram with three-dimensional deep convolutional neural networks," *IEEE Access*, vol. 8, pp. 64646–64652, 2020.
[30] H. Wei, Y. Xiao, R. Li, and X. Liu, "Crowd abnormal detection using two-stream fully convolutional neural networks," in *Proc. 10th Int. Conf. Meas. Technol. Mechatronics Automat. (ICMTMA)*, 2018, pp. 332–336.
[31] W. Liang, Y. Hu, X. Zhou, Y. Pan, I. Kevin, and K. Wang, "Variational few-shot learning for microservice-oriented intrusion detection in distributed Industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 8, pp. 5087–5095, Aug. 2022.
[32] A. Telikani, J. Shen, J. Yang, and P. Wang, "Industrial IoT intrusion detection via evolutionary cost-sensitive learning and fog computing," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 23260–23271, Nov. 2022.
[33] M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty, and M. Ryan, "Deep-IFS: Intrusion detection approach for Industrial Internet of Things traffic in fog environment," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7704–7715, Nov. 2021.
[34] Y. Li et al., "Robust detection for network intrusion of Industrial IoT based on multi-CNN fusion," *Measurement*, vol. 154, Mar. 2020, Art. no. 107450.
[35] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 3469–3477, May 2021.



Guolong Shi received the B.S. degree from Hohai University, Nanjing, China, in 2010, the M.Sc. degree from the University of Science and Technology of China, Hefei, Anhui, China, in 2013, and the Ph.D. degree from Hefei University of Technology, Hefei, in 2019.

He is currently an Associate Professor with Anhui Agricultural University, Hefei, and a Postdoctoral Researcher with Wuhan University, Wuhan, Hubei, China. His research interests mainly are intelligent sensor signal processing, IoT technology implementation, and pattern recognition algorithm.

Xinyi Shen received the B.S. degree from Anhui University, Hefei, Anhui, China, in 2020. She is currently pursuing the postgraduate degree with Anhui Agricultural University, Hefei.

Her research interests mainly are signal processing and pattern recognition algorithm.

Fuke Xiao received the B.S. degree from Anhui Agricultural University, Hefei, Anhui, China, in 2021, where he is currently pursuing the postgraduate degree.

His research interests mainly are signal processing and pattern recognition algorithm.

Yigang He received the M.Sc. degree in electrical engineering and automation from Hunan University, Changsha, China, in 1992, and the Ph.D. degree in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 1996.

In 1990, he joined the College of Electrical and Information Engineering, Hunan University and was promoted to an Associate Professor and a Professor in 1996 and 1999, respectively. From 2006 to 2011, he was the Director of the Institute of Testing Technology for Circuits and Systems, Hunan University. He was a Senior Visiting Scholar with the University of Hertfordshire, Hatfield, U.K., in 2002. In 2011, he joined Hefei University of Technology, Hefei, China. In 2017, he joined Wuhan University, Wuhan, China, where he is currently the Vice Dean of the School of Electrical Engineering. He has authored over 200 journal and conference papers in the aforementioned areas and several chapters in edited books. His current research interests include the areas of circuit theory and its applications, testing and fault diagnosis of analog and mixed-signal circuits, electrical signal detection, smart grid, radio frequency identification technology, and intelligent signal processing.

Dr. He was a recipient of a number of national and international awards, prizes, and honors. He has been serving on the Technical Program Committee of a number of international conferences.