Sensors and Materials, Vol. 36, No. 1 (2024) 323–336
MYU Tokyo

S & M 3521

Power Load Prediction Based on Multi-IoT Monitoring Sensors and Protection Detection Response Recovery Network Security Model

Yiming Zhang,[1] Qi Huang,[2*] Shaoyang Yin,[3] Xin Luo,[4] and Shuo Ding[2]

[1]Metrology Center, Yunnan Power Grid Co., Ltd., Kunming 650500, P.R. China
[2]Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650500, P.R. China
[3]Qujing Power Supply Bureau, Yunnan Power Grid Corporation Limited, Kunming 650500, P.R. China
[4]Dehong Power Supply Bureau, Yunnan Power Grid Corporation Limited, Kunming 650500, P.R. China

(Received August 3, 2023; accepted January 4, 2024)

Keywords: Internet of Things, load prediction, deep learning, security monitoring

With the expansion and deployment of smart metering in power grid management and control, the need for security protection in the power system is continuously growing. However, the current construction of a comprehensive defense system for terminal data is inadequate. In this paper, we report a study on power loads to address the security challenges facing grid management, using the protection detection response recovery (PDRR) network security model as the basis. Firstly, we design an end-to-end security perception architecture using IoT technology and develop an optimization model for monitoring sensor information. In addition, we construct a data aggregation model that improves adversarial domain adaptation and incorporates deep convolutional neural networks to extract features. The proposed model enhances short-term load forecasting by combining linear predictions from autoregressive models with the nonlinear trend analysis capabilities of deep learning models. The performance of the proposed method is compared with those of the Adam and stochastic gradient descent (SGD) optimizers. Experimental results confirm that the proposed method ensures reliable data transmission, facilitates effective classification aggregation of heterogeneous data, and yields fast and accurate load forecasting results. Furthermore, the proposed method enhances the robustness of the model.

1. Introduction

The development of the power industry is crucial to a country's economic strength and overall development. However, with the increasing adoption of information management systems in this industry, there is a growing concern about network security threats. In response to these Cyber Attacks affecting electricity security, the US Department of Defense (DoD) has proposed the PDRR network security model, which consists of four elements: Protection,

*Corresponding author: e-mail: 2541209269@qq.com
https://doi.org/10.18494/SAM4650

ISSN 0914-4935
https://myukk.org/

Detection, Response, and Recovery.[1,2] Among these elements, security detection is a proactive defense measure that requires security monitoring to address the vulnerabilities caused by unforeseen security threats. By employing various technological means to collect and analyze data from the power grid, it is possible to achieve a sense of situational awareness regarding the security of the distribution network.

Currently, there is a need for research on deep networks that are more suitable for domain adaptation to overcome the limitations of deep learning. Convolutional neural networks (CNNs) were originally proposed by LeCun in France for postal code recognition.[3] Baid *et al.* improved the structure of one-dimensional CNNs and introduced the temporal convolutional network (TCN), an algorithm designed for time series data prediction.[4] Moreover, there are other deep learning networks such as recurrent neural network (RNN), long short-term memory (LSTM), and gated recurrent unit (GRU). Deep domain adaptation enhances the traditional deep classification network structure by introducing adaptive layers to achieve the goals of data distribution adaptation. This method was initially introduced in the domain adaptive neural network (DaNN).[5–8] Subsequently, numerous researchers have been influenced by generative adversarial networks (GANs),[9] which consist of generating networks and discriminating networks, and have made advancements in adaptive methods. [10] While these techniques of data aggregation and analysis are mature, they still encounter challenges in handling substantial amounts of diverse security data. Therefore, there is a pressing need for innovations using the IoT technology proposed.[11] With the popularization of IoT technology, it is particularly important to set up appropriate sensors in the field of power.[12,13] However, the research on the modeling of wireless sensor transmission in power systems is not perfect.

In this study, we first construct a monitoring sensor optimization model to improve communication channels and design a distribution network security data aggregation model based on adversarial domain adaptation networks. Data is effectively classified through reasonable feature extraction. Secondly, we use real data from smart grid terminals to build a load prediction model based on AdaBelief optimization. The accuracy and robustness of the model are verified through simulation experiments.

2. Optimization Model for Terminal Monitoring Sensors

Firstly, a smart safety monitoring system is designed for the power distribution network using IoT technology.[14–16] It consists of the end-point perception layer, information access layer, and cloud platform computing layer. To enhance the network security monitoring performance of the intelligent measurement network, we propose an optimization model for monitoring sensor information in the perception layer. This model improves the information interaction capability of the safety monitoring system and meets the requirements of high-dimensional, large-scale, and multinode data access in the smart grid system. Additionally, it resolves the issue of data format differences caused by various sensor technologies.

2.1 Design of the optimization model

To obtain the complete analysis of information in the PDRR model, the communication framework of a wireless sensor is constructed in this study. It uses its communication model to capture accurate and complete information in real time. The detailed steps for designing the data model of the perception layer sensing devices in the distribution grid monitoring system by integrating and unifying the data from sensors of different specifications are as follows.

1) Basics and standards of intelligent transducer electronic data sheets (TEDS): The term "basics" pertains to the essential requirement of having TEDS for carrying out data source tasks and acquiring pertinent information from the sensor nodes. The term "standards" refers to the IEEE 1451.4 standard, which evaluates the TEDS technology and mandates that the electrical connections, content, and data formats be standardized and stored in TEDS templates in electronic form.
2) Security protection: The monitoring sensors of the system detect abnormal data. Upon the occurrence of a fault or threat, the data information is uploaded to the IoT cloud, and the processor issues instructions and backs up data to ensure the real-time security of the smart power IoT. TEDS technology facilitates the use of data templates for various sensor types, allowing for the transmission of sensor parameters and calibration dates, and providing a means for modifying calibration through small incremental data adjustments.
3) Deployment strategy: To tackle the complexity of information interaction resulting from inconsistent sensor data models, we propose the construction of a sensor information model with unified semantics and data formats in the design of the data aggregation control module. This approach allows for easy integration and compatibility of sensors. Moreover, the advanced TEDS circuit design enables smart sensors to seamlessly switch between reading and measurement states, while the support for multiple wiring methods enhances the versatility of sensor applications in various scenarios.

In Fig. 1, the structure of the terminal perception layer framework built in the paper is shown.

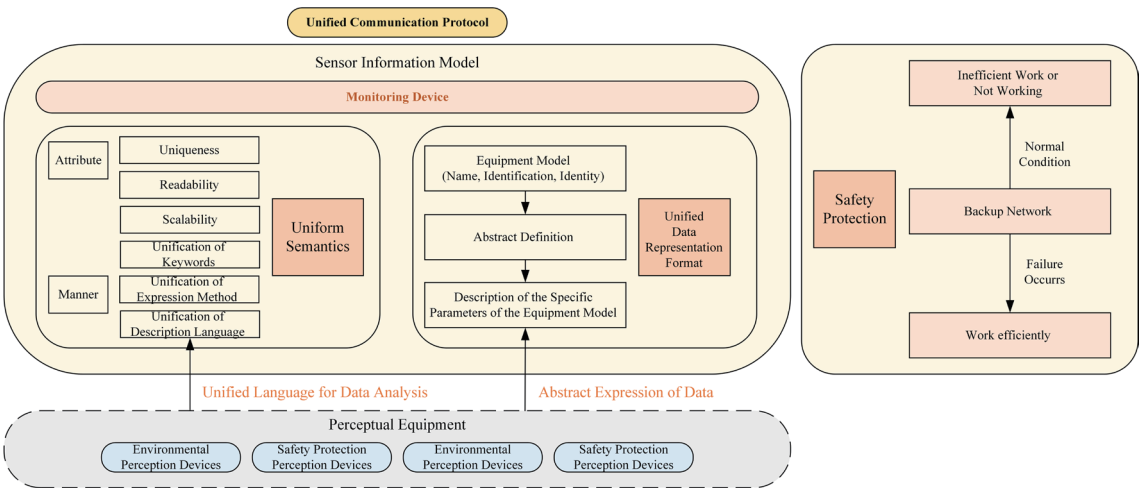


Fig. 1. (Color online) Terminal perception layer framework.

2.2 Optimization model algorithm

To effectively reduce the error rate of information transmission and improve the speed of information transmission, a precise IoT channel model is proposed. Taking the complex conditions of multipaths into consideration, the IoT transmission channel model is formulated as follows.

$$|c(f)| = A\sqrt{\frac{1}{2k}\left\{\left[cv_1 + cv_2\right]^2 + \left[sv_1 + cv_2\right]^2\right\}}, \tag{1}$$

where $|c(f)|$ represents transfer function of the channel, and v_1 and v_2 express the values of the input and output signals, respectively.

By quantitatively decomposing multiple independent fading channels, the following quantized balanced transmission channel model can be obtained.

$$R_q^i(k) = E[q_i(k)q_i^T(k)] \le \text{diag}\left\{\frac{\Delta_i^2(k,1)}{4}, \frac{\Delta_i^2(k,2)}{4}, \ldots, \frac{\Delta_i^2(k,p)}{4}\right\} = \overline{R}_q^i(k), \tag{2}$$

where $\Delta_i^2(k,1)$ represents the quantized equilibrium value.

Considering the interference among multipaths and the deployment pattern of complex sensors, the signal reception model for mutual sensing between sensor nodes in the IoT is given as

$$x_m(t) = \sum_{i=1}^{I} s_i(t)e^{j\varphi_{mi}} + n_m(t), -p+1 \le m. \tag{3}$$

This results in higher data transmission accuracy, significantly reduced average hop count of data packets, and reduced time delay.

2.3 Experimental simulation and analysis

In the hardware environment for model development and experimental simulation, the operating system used is Windows 10 Ultimate Edition. The optimization model for monitoring sensor information in the perception layer is executed on the Optimum Network Performance (OPNET) simulation platform. This platform allows for improved system response speed, enabling the validation of the sensor optimization system's performance. By using the principle of perceptual similarity, the perception layer is simulated using the OPNET platform, with the specific parameters given in Table 1.

Table 2 shows the highest improvement percentage in the two scenarios. Here, Scene 1 represents the traditional IoT power system, and Scene 2 represents the ubiquitous IoT system proposed in this section. To show the superiority of the proposed method, we compare the performance of the two scenarios.

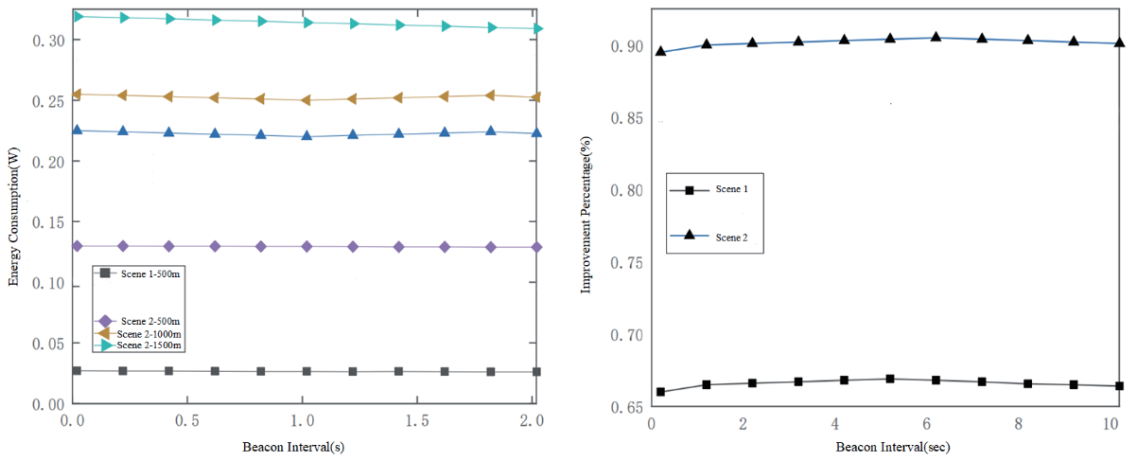
According to Fig. 2, the system presented in this section, ubiquitous power IoT (UPIoT), exhibits a reduction in the average hop count and time delay in comparison with the traditional

Table 1
Simulation parameters.

Simulation Scene	Sensor deployment nodes	Deployment range (km)	Routing protocol	Available channels	Transmission distance (m)
Scene 1	50	3 × 10	AOD	1	500
Scene 2	50	3 × 10	AODV	3	500/1000/1500

Table 2
Highest improvement percentage in two scenes.

Simulation Scene	Percentage
Scene 1	66.8
Scene 2	90.6



(a) (b)

Fig. 2. (Color online) Average transmission results of data. (a) Energy consumption and (b) improvement percentage.

mode. This suggests an enhancement in the response speed of the sensor information optimization model proposed in this paper. The data presented in Table 2 indicates that UPIoT demonstrates an improvement of 23.8% in interaction efficiency compared with previous systems.

3. Load Data Aggregation Model Using Adversarial Domain Adaptation Network

3.1 Load data preprocessing

The available data consists of load values of a specific region over two months, encompassing parameters such as three-phase voltage, three-phase current, active power, reactive power, power factor, and other interval values recorded every 15 min. To evaluate the distribution of current within the system, the degree of imbalance in three-phase currents is often employed as a metric. The equation describing this indicator is presented below:

$$I_{ub} = \frac{\max\{I_A, I_B, I_C\} - \min\{I_A, I_B, I_C\}}{\max\{I_A, I_B, I_C\}} \times 100\%, \tag{4}$$

$$E = P_{useful} \times 0.25. \tag{5}$$

I_A, I_B, and I_C respectively represent the current of each phase of the three-phase generator, and Eq. (4) indicates the unbalance of the three-phase current.

1) The original load data is imported into the SPSS (a data processing tool) software for data preprocessing. Initially, the median absolute deviation (MAD) method is employed to detect and replace any outliers that are identified with the mean value. MAD is calculated as the median of the absolute deviations from the median. The deviations can have both positive and negative values in a univariate sequence.

$$MAD = median\left(\left|X_i - median(X)\right|\right) \tag{6}$$

Assuming the data follows a normal distribution, the outliers should fall outside the 50% probability, while the normal values should fall within the middle 50% region, i.e.,

$$P\left(\left|X - \mu\right| \le MAD\right) = P\left(\frac{\left|X - \mu\right|}{\sigma} \le \frac{MAD}{\sigma}\right) = P\left(Z \le \frac{MAD}{\sigma}\right) = 0.5. \tag{7}$$

Under a normal distribution, ±0.6749 covers 50% of the area, 1/0.6749 ≈ 1.4826, so

$$MAD_c = 1.483 \cdot MAD. \tag{8}$$

2) To eliminate the influence of different data units on the result analysis, the min–max normalization method is used for normalization; this centralizes the dimensionless data values in the range (0, 1). The specific equation is

$$x_{i,j}^{*} = \frac{x_{i,j} - x_j^{min}}{x_j^{max} - x_j^{min}}, \tag{9}$$

where x_j^{max} and x_j^{min} represents the maximum and minimum values of the column.

3.2 Experimental simulation and analysis load data aggregation analysis based on adversarial domain adaptation

GANs utilize the concept of a zero-sum game,[14,15] which revolves around cooperation and competition between the generator and the discriminator. The generator, referred to as the generative network, creates samples that closely resemble real data by utilizing random noise. On the other hand, the discriminator, known as the discriminative network, classifies the generated samples in order to differentiate between real and fake data. Through this adversarial

game, both networks engage in training and enhance their performance through dynamic interactions. The design process of GAN is shown in Fig. 3 and Table 3.

The theoretical implementation of GAN is mainly accomplished using the following three equations.

1) Mathematical expectation of a continuous function:

$$E(x) = \int xf(x)dx \tag{10}$$

2) KL divergence:

$$KL\left(P \| Q\right) = \int p(x) \log \frac{p(x)}{q(x)} dx \tag{11}$$

3) JSD divergence:

$$JSD\left(P \| Q\right) = \frac{1}{2} KL\left(P \| M\right) + \frac{1}{2} KL\left(P \| Q\right) \tag{12}$$

By incorporating the adversarial mindset of GAN and domain adaptation, an adversarial domain adaptation is formed. Overall, the three optimization objectives form a stubborn loss function for adversarial domain adaptation, as follows:

$$L(\theta_f, \theta_y, \theta_d) = \frac{1}{n_s} \sum_{x_i \in B_s} L_y\left(G_y\left(G_f\left(x_i\right)\right), y_i\right) - \frac{\lambda}{n_s + n_t} \sum_{x_i \in (B_s \cup B_t)} L_d\left(G_d\left(G_f\left(x_i\right)\right), b_i\right), \tag{13}$$

where x_i is the input sample, $G_f\left(x_i\right)$, $G_y\left(G_f\left(x_i\right)\right)$, and $G_d\left(G_f\left(x_i\right)\right)$ are the outputs of the feature extractor, the label classifier, and the domain discriminator, respectively, y_i is the class label of the actual sample, and b_i is the domain label of the actual sample.

The loss function of the label classifier is calculated using cross-entropy loss and is expressed as

$$L_y = \frac{1}{n_s} \sum_{x_i \in B_s} \sum_{t=1}^{T} P_{x_i \to t} \log G_y\left(G_f\left(x_i\right)\right), \tag{14}$$

where $P_{x_i \to t}$ is the probability that the input sample x_i belongs to class t. After learning and training, the parameters of the three modules can be represented as

$$\left(\hat{\theta}_f, \hat{\theta}_y\right) = \text{argmin}_{\theta_f, \theta_y} L\left(\theta_f, \theta_y, \theta_d\right), \tag{15}$$

$$\left(\hat{\theta}_d\right) = \text{argmax}\, L\left(\theta_f, \theta_y, \theta_d\right). \tag{16}$$

According to the T-SNE algorithm designed in this paper, the clustering results before and after optimization were obtained, as shown in Fig. 4.

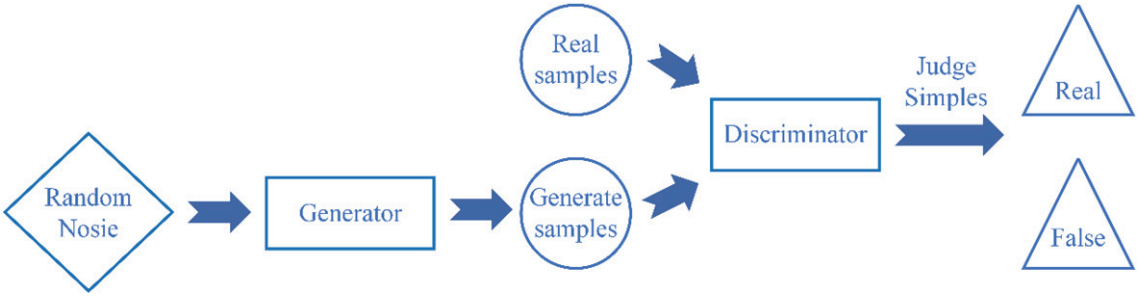
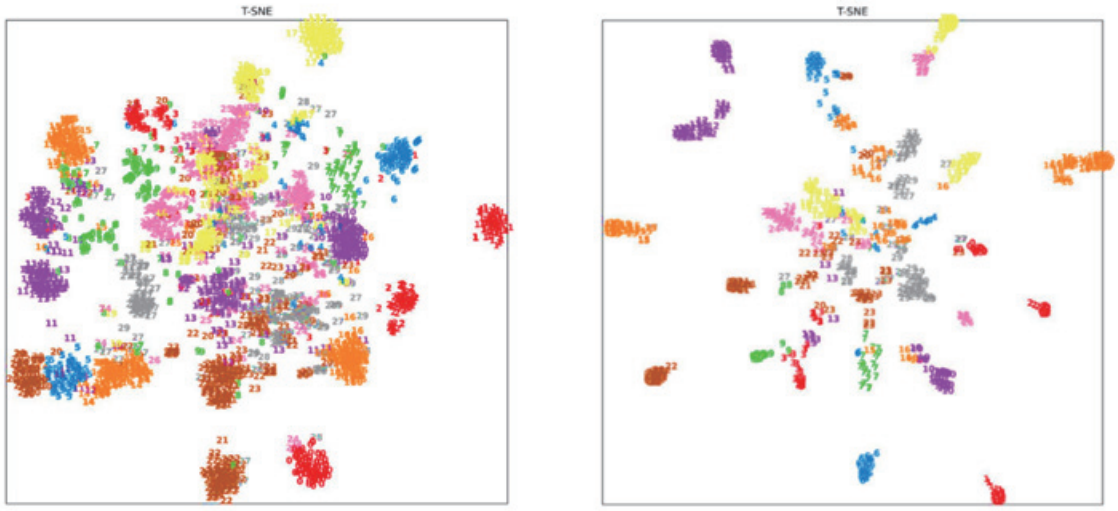


Fig. 3. (Color online) Algorithm flow of generative adversarial network (GAN).

Table 3
Specific functions of each module.

Specific function	Module		
	Feature extractor	Label Classifier	Domain Discriminator
Course of events	Extract features to map to feature space, obfuscate data sources as much as possible	Classify aligned source and target domain features, identify the right label	Discriminate domain of features to discern the source of data
Purpose	To maximize the loss L_d to learn the parameter θ_f	To minimize the loss L_y to learn the parameter θ_y	To minimize the loss L_d to learn the parameter θ_d



(a) (b)

Fig. 4. (Color online) Data aggregation visualization based on T-SNE: (a) before aggregation and (b) after aggregation.

3.3 Experimental simulation and analysis

Next, we implemented the model establishment and experimental simulation using Python 3.9.7. The preprocessed data was divided into the source domain (A) and the target domain (B).

To evaluate the effectiveness of the adversarial domain adaptation data aggregation model, we performed feature visualization and convergence verification. We used 60% of the samples in the target domain as the training set, 20% as the validation set, and the remaining samples as the test set. The results of the experiment are presented in Fig. 5.

1) Feature Visualization: According to the figure, the aggregated classification boundaries are distinct, indicating effective aggregation and alignment of data distributions between the source and target domains.
2) Convergence Verification: The accuracy curve and loss function curve of the model as the number of iterations increases are shown in Fig. 6.
   From the analysis of the accuracy and loss curves, it is evident that the model's accuracy levels off and reaches a stable point as the number of iterations increases. This finding suggests that the experimental results exhibit accurate aggregation and consistent training performance.

4. Short-term Load Forecasting based on AdaBelief Optimization

Previous studies have revealed that short-term load time series data displays substantial randomness and nonlinear properties. Accurate and prompt short-term load forecasting is vital to guarantee the secure and dependable operation of the power system. Taking into consideration the current state of research both domestically and internationally, in this section, we put forward a solution for enhancing and refining deep learning techniques in the realm of short-term load forecasting. The key aspects of this proposal involve optimizing a deep learning module through the utilization of the AdaBelief optimizer and incorporating autoregressive algorithms for improved assistance.

4.1 Improved load forecasting framework based on deep learning

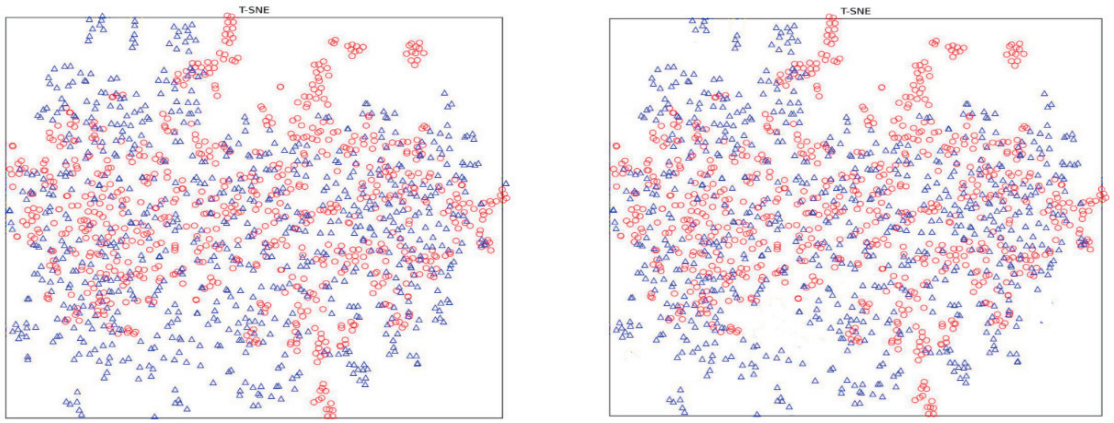
The data that has undergone feature selection is imported into the improved deep learning prediction model. The model is composed of two components. The first is an optimized deep learning module, which can be embedded in any deep learning method. In this paper, a TCN model is chosen as the optimization algorithm on the basis of previous research findings. The second is a linear trend analysis prediction model based on autoregressive (AR) models. The specific framework is depicted in Fig. 7.

Here, the prediction result of the TCN model is y^o, and the prediction result of the AR model is y^r. The AR model learns the linear patterns of multiple time series, and its equation is

$$y^r = \sum_{k=0}^{n} H_k y_{t-k} + c, \tag{17}$$

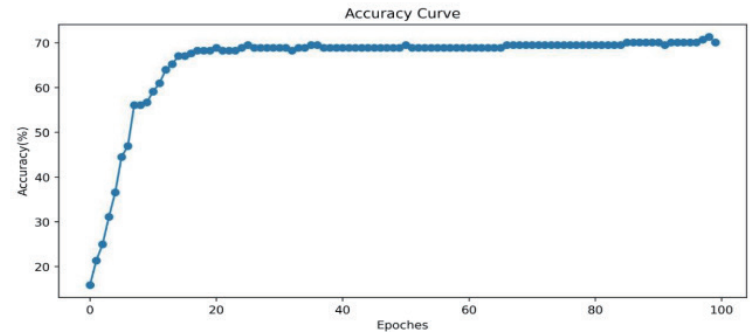
where $H_k \in \mathbb{R}^D$ and $c \in \mathbb{R}$ represent the coefficients of the model and n is the order of the model.

The final prediction result in this section is the combination of the nonlinear trend and the linear trend components, which is obtained as

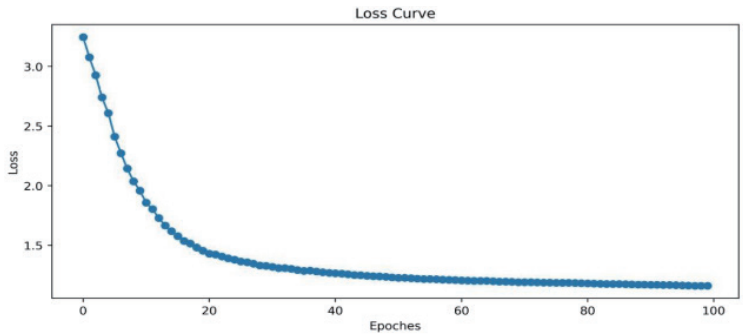


(a) (b)

Fig. 5. (Color online) Feature distribution of source domain and target domain: (a) before and (b) after aggregation.



(a)



(b)

Fig. 6. (Color online) (a) Accuracy and (b) loss function curves of the aggregation model.

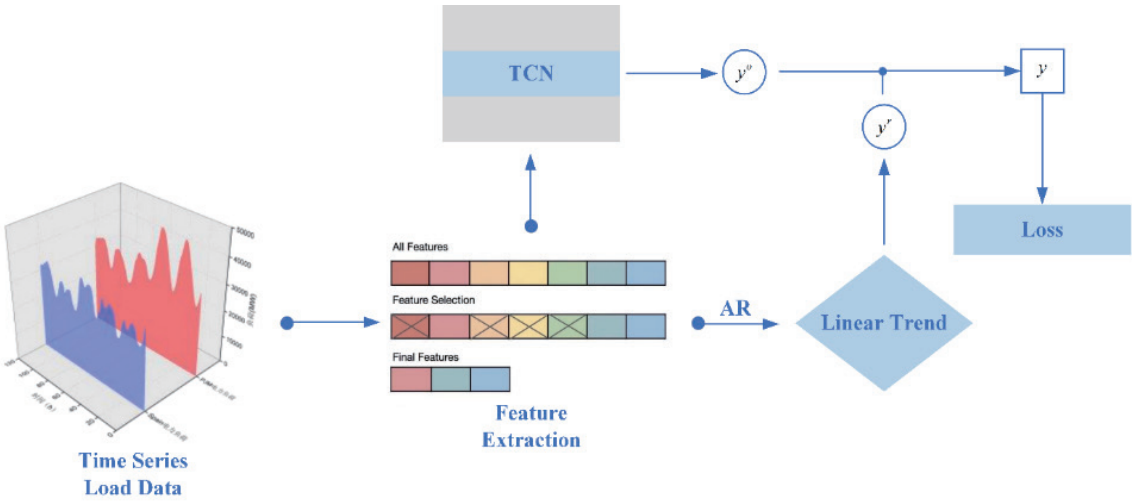


Fig. 7. (Color online) Load prediction framework.

$$y = \alpha y^r + (1 - \alpha) y^o, \tag{18}$$

where α is the optimal weight coefficient obtained through multiple repeated experiments. The AR model has an auxiliary role of dealing with the phenomenon that deep learning is insensitive to changes in data scale.

4.2 Results and analysis of experiment

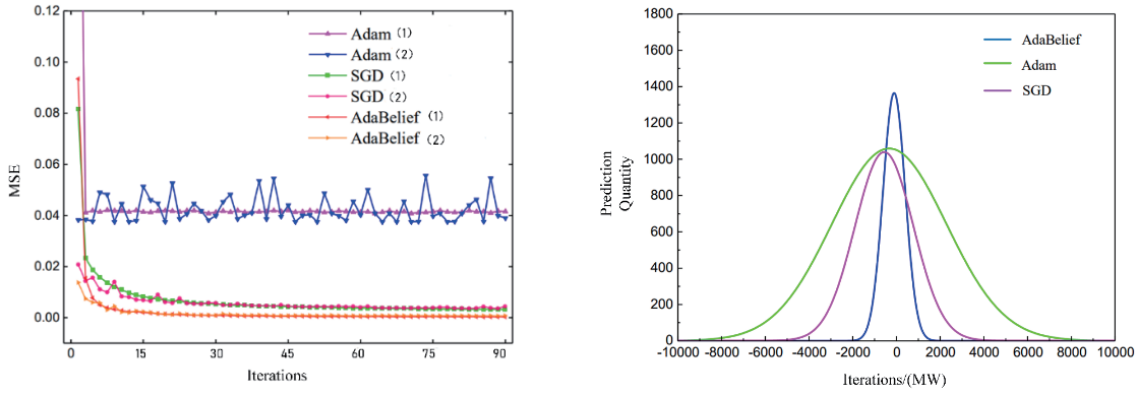
The algorithm implementation described in this paper is based on the Python language, and open-source programs on Github related to deep learning are utilized for learning. To handle the dataset, 80% of the data is utilized as the training set, while 10% is allocated as the validation set and another 10% is allocated as the test set for purposes such as training, parameter tuning, and measuring prediction accuracy. The TCN model adopts the default parameters provided by the Keras library® to ensure the generality of the framework design.

1) Validation of effectiveness of AdaBelief optimizer

In this section, a unified learning rate ($Rate_{learning} = le - 2$) and the number of iterations ($n = 90$) are set, and the losses of the TCN network under the AdaBelief, Adam, and SGD optimization algorithms are compared. The mean square error (*MSE*) is used as the loss function for performance comparison.

$$Loss = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - Y_i\right)^2 \tag{19}$$

In Fig. 8, (a) represents the training loss, and (b) represents the validation loss. It can be seen that the training and validation losses of the AdaBelief optimization algorithm are both lower than those of the other two algorithms, and it also has the highest learning speed.



(a) (b)

Fig. 8. (Color online) MSE loss functions and errors for three optimization algorithms. (a) MSE loss and (b) prediction quantity.

Table 4
Results of prediction.

Optimizer Type	*RSE*	*CORR*	Iteration time per Step (s)
AdaBelief	0.1023	0.9987	92
Adam	0.5799	0.8151	127
SGD	0.3268	0.9623	102

The AdaBelief optimization technique dynamically adjusts the learning rate during each step of training to ensure that the decreasing trend of the two losses remains consistent. This adjustment helps to meet the requirements for good training without the need to manually tune parameters to improve prediction performance. Additionally, it prevents issues such as overfitting or training instability. y_i and Y_i represent the actual load values and predicted load values in the model, and N represents the total number of samples.

The AdaBelief optimization technique dynamically adjusts the learning rate during each step of training to ensure that the decreasing trend of the two losses remains consistent. This adjustment helps to meet the requirements for good training, without the need to manually tune parameters to improve prediction performance.

Figure 8 shows that the AdaBelief optimization algorithm has the highest number of predictions within a small error range, with an absolute error of less than 2000 MW. In comparison with Table 4, its RSE value is significantly smaller than the other two optimization algorithms, and the CORR value is close to 1. These results indicate that the method described in this section considerably improves the prediction accuracy of the deep learning model. Additionally, the iteration time is better than those of the other methods, demonstrating a faster response.

5. Conclusions

Research results intuitively provide decision support for the monitoring and management of the distribution IoT. Our proposed research method combines the PDRR model with IoT

technology to optimize the information transmission performance of end sensors and promote the load data aggregation and prediction performance in the distribution grid. By improving the information transmission speed of the perception layer and the efficiency of the sensor system, the optimized model of end monitoring sensors enhances the overall performance of the secure data of the distribution IoT. This ensures the reliability and accuracy of the subsequent data analysis. To solve the limitations of traditional deep learning algorithms for multidomain heterogeneous data, a data aggregation model based on adversarial domain adaptation was proposed in this paper. The model achieves accurate data aggregation with good convergence, while suitable features can be extracted for analysis. The visualization of data analysis presents the research results in a clear and intuitive manner. This supports decision-making for the monitoring and management of the distribution IoT. Overall, an optimized research method that improves the security and efficiency of data transmission and analysis in the distribution IoT is presented in this paper. The proposed models and techniques offer valuable insights for the practical implementation of secure data monitoring and management in IoT systems.

Acknowledgments

This work was supported by the Science and Technology Project of Yunnan Power Grid Co., Ltd., under Grant No. YNKJXM20220010 and the National Key Research & Development Program of China under Grant No. 2023YFB2407300.

References

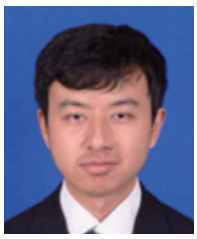
1 A. J. Titus, E. van Opstal, and M. Rozo: Health Security **4** (2020) 310. https://doi.org/10.1089/hs.2020.0007
2 L. Xie, Q. Dai, and H. Yang: J. University of Science and Technology of China **10** (2011) 915. https://doi.org/10.1155/2023/6545323
3 K. Wu, R. Cheng, H. Xu,and J. Tong: Int. Tra. Electr. Energy Syst. **1** (2023) 1.
4 Y. Baid,J. He, J. Chen, X. Wang, and B. Du: Elect. Power Syst. Res. **215** (2023) 109016. https://doi.org/10.1016/j.epsr.2022.109016
5 A. Pasdar and H. H. Mehne: Int. J. Electr. Power Energy Syst. **33** (2011) 693. https://doi.org/10.1016/j.ijepes.2010.11.019.
6 S. Hochreiter, J. Schmidhuber: Neural Comput. **9** (1997) 1735. https://doi.org/10.1162/neco.1997.9.8.1735
7 T. Yang,F. Zhai,Y. Zhao: Eng. Sci. Technol. II **43** (2019) 9.
8 M. Ghifary, W. B. Kleijn, and M. Zhang: Domain Adaptive Neural Networks for Object Recognition-13th Pacific Rim Int. Conf. Artificial Intelligence (PRICAI, 2014) 898.
9 S. J. Bai, J. Z. Kolter, and V. Koltun: Arxiv **3** (2018) 1. https://doi.org/arXiv:1803.01271
10 I. J. Goodfellow: Generative Adversarial Nets-28th Conf. Neural Information Processing Systems (NIPS), (Montreal 2014) 2672.
11 I. Averbuch: Thoracic Cancer **14** (2017) 1589.https://doi.org/10.1111/1759-7714.14902
12 L. Peng, J. Yan, Q. Lu: Eng. Sci. Technol. II **19** (2020) 150. https://doi.org/10.19768/j.cnki.dgjs.2020.19.05
13 L. Li, B. Lu, W. X. Xu, Z. H. Gu, Y. S. Yang, and D. P. Tan: Mech. Syst. Signal Process **189** (2023) 110058. https://doi.org/10.1016/j.ymssp.2022.110058
14 H. Shi, L. Wang, R. Scherer, M. Wozniak, and W. Wei: Eng. Sci. Technol. II Ser. **1** (2022) 1. https://doi.org/10.27733/d.cnki.gsxlg.2022.000195
15 L. Li, B. Lu, W. X. Xu, Y. F, Tan, Z. H. Gu, Y. S. Yang, J. G. Yang, and D. P. Tan: Acta Phys. Sin. **72** (2023) 034702. https://doi.org/10.7498/aps.72.20221991
16 S. Mohammadjafari, O. Ozyegen, M. Cevik, E. Kavurmacioglu, J. Ethier, and A. Basar: Neural Comput. Appl. **33** (2021) 11309. https://doi.org/10.1007/s00521-020-05656-2

About the Authors

Yiming Zhang was born in 1990 in Yunnan Province and graduated from Kunming University of Science and Technology in 2014 and is now an engineer at the Metering Center (Power Load Control Technology Center) of Yunnan Power Grid Co. His main research directions are grid digitization, power metering automation, and network security for power monitoring systems. (zhangyiming01@im.yn.csg)

Qi Huang was born in 2002 in Kunming County, Yunnan Province. Currently, she is a student at the College of Civil Aviation and Aeronautics Engineering, Kunming University of Science and Technology, pursuing a bachelor's degree in mechanical engineering. Her main interests lie in operations research, traffic management, and mechanical theory. (2541209269@qq.com)

Yin Shaoyang was born in 1983 in Yunnan Province. He is currently working as a senior engineer in the Marketing Department, Measurement and Project Management Unit of Qujing Power Supply Bureau, Yunnan Electric Power Company Limited. He graduated from Yunnan University with a bachelor's degree in computer science and technology. His research focus is on smart electricity and power metering. (yinshaoyan@qj.yn.csg.cn)



Luo Lin was born in 1994 in Dali Prefecture, Yunnan Province. He graduated from Chengdu Institute of Technology, majoring in computer science and technology, and now works at Yunnan Power Grid Co., Ltd. as the class leader and safety officer of the electric energy data class in the power supply service center. His research interests are in power marketing and metering electricity. (luoxin03@im.yn.csg)

Shuo Ding was born in 2003 in Changchun City, Jilin Province. He is presently a junior student in the School of Civil Aviation and Aviation of Kunming University of Science and Technology and is working toward a bachelor's degree in transportation. His main research interests are data analysis, data mining, operations research, and machine learning. (911517473@qq.com)