Hindawi
Mobile Information Systems
Volume 2022, Article ID 4184941, 11 pages
https://doi.org/10.1155/2022/4184941

*Research Article*

# Safe Operation Management of Urban Smart Grid Based on Deep Learning

**Huimin You**

*Secretariat, Jiangsu Computer Society, Nanjing 210000, Jiangsu, China*

Correspondence should be addressed to Huimin You; huimin.you@utesting.cn

Received 1 June 2022; Revised 25 July 2022; Accepted 30 July 2022; Published 24 August 2022

Academic Editor: Imran Shafique Ansari



The smart grid in the twenty-first century is constantly innovated by the big data technology and the Internet of Things (IoT) technology. As the second generation of a power network, the smart grid keeps developing towards automation and intelligence, driving the energy conversion rate, power utilization rate, and energy supply rate to increase. However, in the smart grid, the power terminal has a pivotal role in controlling, monitoring, and regulating the production process of electricity, which is currently facing many security challenges. The most critical aspect of smart grid security management is to ensure the security of power terminals. Existing solutions generally monitor power terminal devices by monitoring power terminal traffic; however, such security policies can only monitor attacks with characterization properties at the traffic level and cannot be used to monitor power terminal devices directly. Based on this, this paper reviewed the literature on intelligent operation and maintenance and deep learning at home and abroad and comprehensively analyzed the research progress of intelligent operation and maintenance, and in the comparative analysis of deep learning methods, because the convolutional neural network has fewer connections and parameters and can control the capacity by controlling its depth and width, it is convenient to establish a model with larger learning capacity, so a convolutional neural network is chosen for data analysis. In this study, we choose to use the convolutional neural network to analyze the data, combine the monitoring, management, and fault location of operation and maintenance work organically through some deep learning algorithms, reduce the number of model layers through a deep learning-based security monitoring technology for electric power terminals to improve the training speed and efficiency, and achieve all-round protection for electric power terminals at the device level and the network level. The management of urban smart grid dispatching operation also requires strict implementation of relevant technical standards to ensure the standardized operation and enhance the safety and stability of grid operation.

## 1. Introduction

Electricity production is characterized by a high degree of automation, with many power plants, transmission lines, substation and distribution facilities, and power-using equipment forming a power network, interlocking and mutually constraining joint operation, and constituting a very large and complex process of power production, circulation, distribution, and consumption. In this process, power generation, supply, and consumption are carried out simultaneously, and production, transmission, and consumption are balanced at all times. These intrinsic characteristics of power production require that the operation of the power grid must be very stable and reliable, and any accident in any one link, such as not dozens of exclusion, may bring a chain reaction, resulting in serious damage to the main equipment or a large area blackout, and may even cause a catastrophic accident of the entire network collapse. At present, China's electric power industry has entered a new stage of "large units, large power plants, large power grids, high parameters, high voltage, high automation" as the main hot spots, which brings new issues to the production of electric power safety and puts forward higher and newer requirements.

Through the extensive application of intelligent technologies and information technology, such as the Internet of Things, big data, cloud computing, blockchain, mobile Internet, artificial intelligence, and edge computing, and the

pooling of resources from all aspects, the system can achieve human-computer interaction and interconnection of all aspects of the power system and provide a smart service system with efficient information processing, comprehensive state awareness, and convenient and flexible application. The system used in Japan is mainly based on Toshiba's Grid Control Monitoring System, which consists of Toshiba Group's Integrated Smart Meter Management System, Meter Data Management System, and Toshiba Solutions Corporation's Customer Information Management System. The Korea Smart Grid Association is launching a national programme to encourage and support the development of smart grid patents that meet international standards. The association supports companies, universities, and research institutes that apply for international patents and hosts the development of technologies and standards that can be translated into patents in the future.

The sensor structure of the IoT-based electrical safety management system uses structural sensors as a means of receiving signals from the safety management system in real time. The signals are analyzed and processed through a database system to ensure the safety and stability of the system and to reduce the risk to staff. If a worker is not working in accordance with the relevant regulations of the State Grid Corporation of China, the sensors in the safety management system will send out an alarm signal, which will be transmitted to the management center in the background. With regard to China's national strategy, the State Grid launched the first pilot projects for automated urban power distribution in August 2009, which were implemented in central areas (or parks) in Beijing, Hangzhou, Yinchuan, and Xiamen. It is a nonprofit, loose, and open trade federation organization. It is also the first strategic alliance in the field of smart distribution networks in China. It promotes the development of smart grids in China. The main objectives of the pilot project are to adopt a rational distribution automation configuration scheme based on different reliability requirements, to form a smart distribution network with self-built systems, user interaction, and efficient operation, to develop customer-specific performance, and to provide flexible access to decentralized production. The second pilot will build the second phase on the basis of the first phase of distribution automation in the first pilot cities, focusing on expanding technical support for distributed network access, improving the construction of an integrated technical support platform for advanced applications and supervision of the distribution network, and realizing integrated management of distribution network dispatch, operation, and control.

*1.1. Research Status.* There are a large number of power terminals in the business system of the smart grid, and the data acquisition and monitoring control system (SCADA) in the smart grid is used to monitor and control the operating power terminals, and perform telemetry, telematics, remote control, and remote regulation, i.e., "four remotes." RTU (remote terminal unit) and FTU (feeder terminal unit) are important components of the SCADA, among which RTU is a typical embedded system, located in the remote device of substation equipment, which is mainly responsible for collecting power parameters of equipment, communicating with the master station, and responding to the request of the master station. Many domestic and foreign scholars have already studied the protection of power terminals in order to improve the safety performance of power terminals.

Jiang et al. proposed to build a security assessment model for electric power terminals by assessing the hardware security, network security, system security, application security, and management security of electric power terminals in response to international information security risk assessment specifications [1]. By assessing the security of power terminals, the literature realizes quantitative analysis of terminal security assessment, thus guiding us to protect power terminals with higher risk after assessment more reasonably, allocate computing resources in the power grid reasonably, and improve the efficiency of protection for power terminals. Nan et al. investigate the access control of power terminals and protect them from the network level. The power communication network is an important part of the power secondary system, which plays the role of scheduling, protection, and transmission of marketing data in power production, and the power terminal realizes the demand response to the main station by accessing the power communication network [2]. Therefore, building a safe and reliable power communication network, conducting security analysis and device authentication for the power terminals that are connected to the network, and providing access control for the power terminal devices are conducive to the security protection of the power industrial control network.

In the security protection of electric power terminals, accurate and effective identification of attacks is a necessary condition for security protection of electric power terminals. Only by accurately locating and identifying the attacks on electric power terminals can the damage caused by attacks be minimized and targeted protection be provided. So far, many scholars have conducted research on the identification of attacks on power terminals. Fang et al. researched an intrusion detection system based on protocol parsing technology to detect attacks that invade electric power terminals [3]. Meanwhile, Cao et al. studied the network protection wall system and the industrial intrusion detection system (IDS) for information networks and organically combined them to propose a new approach that incorporates both of these security strategies [4]. Yang et al. implemented a security detection system that learns novel attack behaviors by extending the GHSOM (Growing Hierarchical Self-Organizing Map) neural network model [5]. The paper addresses the problems that arise in common cluster analysis algorithms deployed in IDSs: The first is the use of the random method to determine the initial cluster centroids, its algorithm is sensitive to the initial values, and different initial values will make the final convergence of the algorithm inconsistent [6]; and the second is the use of the hill climbing method that cannot solve the problem of local optimum, and so, an improved cluster analysis method is proposed that can solve the problem of local optimum to some extent, so as to improve the intrusion. The article

optimizes the intrusion detection based on the BP neural network algorithm using a genetic algorithm, which improves the performance of the intrusion detection system to a certain extent [7]. The article takes TCP data messages transmitted by power terminals as observations and combines neural networks and hidden Markov models by adjusting the structures of hidden Markov models and neural networks to achieve the optimization of intrusion detection systems [8].

### 1.2. Contents and Methods

*1.2.1. Main Idea.* This paper is dedicated to improving the security of the smart grid and designing a comprehensive security monitoring system for power terminals to realize the security protection of terminal devices. In designing protection strategies for power terminals, a comprehensive power terminal protection strategy is designed from the power terminal device level and the power terminal network level. In the power terminal device-level security protection, this paper uses the characteristics of the power terminal itself, which has a single function and a single structure cylinder and often executes specific business instructions, to monitor the state of the device using the power terminal equipment side-channel information. To this end, a security monitoring strategy for power terminals based on device power consumption information is designed to achieve nonintrusive security monitoring of power terminals through data collection, feature extraction, and training of neural network models for power terminal power consumption information. This method can detect power terminal information attacks that cannot be detected at the network level and improve the security performance of power terminals. In the network-level security protection of electric power terminals, we propose a network-level attack detection method for electric power terminals. By capturing the communication messages between electric power terminals and the master station, we extract the key segments in the messages of electric power terminals, and then train the security detection model of electric power terminals through feature engineering and data enhancement to realize the network-level security protection of electric power terminals. This method can effectively detect attacks on power terminals launched from the network level, and the model also has good robustness and generalization performance, which can well improve the security performance of power terminals. The main contributions of this research can be summarized as the following four points:

(1) A device-level security protection method and a network-level security protection method for power terminals are proposed, which provide security protection for power terminals from the device level and the network level, respectively, and can effectively improve the security performance of power terminal devices and guarantee smart grid security.

(2) A safety monitoring method of power terminal based on power consumption information of power terminal is proposed, which monitors the power consumption information of side channel of power terminal in a nonintrusive way and maps the power consumption of power terminal equipment to its operation status.

(3) A deep neural network-based information attack detection method for power terminals is proposed, which achieves information attack security detection for power terminals through data mining and analysis, feature extraction, data enhancement, and model optimization of communication messages of power terminals.

(4) A laboratory simulation environment was built to simulate and verify our proposed security monitoring technology for power terminals. The test results show that the device-level power terminal security protection technology and the network-level power terminal security protection technology can effectively monitor the working status of the power terminal and can effectively protect the power terminal equipment.

The safety management system for power field operations is based on the IoT technology for server design. Its main purpose is to solve the problems between information processing and the human-machine interface in the Chinese national grid. The apparatus- and personnel safety-based servers deliver the data collected during fieldwork to the fieldwork fault detection server, the staff summary server, and the environmental monitoring server for processing.

*1.2.2. Experiment Procedures.* Section 1 is Introduction. On the basis of reading-related literature, the information attacks suffered by smart grid intelligence and the major accidents occurred are summarized, and the security monitoring method and the attack identification method for power terminals adopted in this paper are briefly introduced.

Section 2 is Algorithm Model. This model is divided into three parts: the cloud-centric layer, the edge layer, and the field layer to achieve nonintrusive monitoring of power terminal devices and protect them at the device level.

Section 3 is Conclusions and Optimization Suggestions. It discusses how the model implements security protection in urban smart grids and effective monitoring of power terminals without affecting their normal operation.

Section 4 is Conclusion. In this paper, we propose a device-level and a network-level security monitoring strategy for power terminals in smart grids. We summarize our work as follows:

(1) We propose a device-level security protection method for power terminals based on edge channel, which achieves a device-level security monitoring of power terminals by collecting edge channel information from power terminals and mapping the edge channel timing information to the working state of power terminals using an LSTM neural network. The method has good accuracy and noninvasiveness, and can better realize the safety monitoring of power terminals.

(2) We propose a network-level security protection method for electric power terminals based on deep learning, which realizes network-level security monitoring of electric power terminals by data mining and feature extraction of communication messages of electric power terminals and the data enhancement method based on an adversarial generative neural network.

(3) We built a DTU security monitoring simulation platform to test the edge channel-based device-level security protection method. The experimental results show that the method can accurately detect the abnormal state of DTU.

## 2. Algorithm Model

The network and power terminal security detection method proposed in this paper first requires collecting normal messages and attack messages from power terminals, performing data cleaning and feature extraction on the data after data enhancement based on adversarial generative neural networks, and finally learning the messages through stacked self-encoders, so as to achieve detection of information attacks on power terminals and achieve security monitoring of power terminals at the network level. Purpose power terminals are widely used in the smart grid. In the distribution automation system and the power monitoring system, RTU, PLC, DTU, and other power terminals are widely used, which not only make the power grid more informative and intelligent, but also bring many risks to the smart grid [9]. Research shows that there are a lot of security risks and vulnerabilities in embedded power terminal devices, and a large number of power terminal devices still have security problems such as command injection and hard coding. Attackers can take advantage of the vulnerabilities of these power terminals to tamper with the control commands and operations of power terminals without authorization, thus causing power outages.

Based on the current situation, this paper proposes a security monitoring method based on the bypass signals of power terminals and protects them accordingly at the power terminal device level. The method collects power consumption information (positive samples) of power terminals with normal operation history and power consumption information (negative samples) when they are under attack, feature-engineers them, extracts the combination of features that can characterize the working state of power terminals, and then learns the features through an LSTM neural network to train the security monitoring model of power terminals to achieve the purpose of device-level security monitoring of power interruptions.

*2.1. RNN.* A RNN is called a "recurrent neural network," its structure is a network of network nodes connected into a ring, and it learns time series information through its internal recurrent structure [10].

In the formula, $x$, $s$, $U$, $V$, and $o$ are the parameter vectors in the neural network. $x$ is the vector of the input layer of the neural network, $s$ is the input vector of the hidden layer of the neural network, $U$ denotes the weight matrix of the input layer, $V$ denotes the weight matrix of the output layer, and $o$ denotes the vector of the output layer, as shown in Figure 1. In particular, the input vector $s$ of the hidden layer in the RNN is the key to its ability to learn time series signals. Unlike conventional neural networks, its value depends not only on the vector $x$ of the input layer, but also on the input vector $s$ of the hidden layer at the previous moment. The weight matrix $W$ is the value of the weights of the hidden layer at the previous moment, i.e., $s_t = s_{t-1} \times W$.

As shown in Figure 2, after the RNN has received input $x_t$ at moment $t$, the value of the hidden layer is $s_t$ and the output value is $o_t$, where the value of $s_t$ is jointly determined by $x_t$ and $s_{t-1}$.

The output and hidden layers of the RNN are computed as follows:

$$o_t = g(Vs_t), \tag{1}$$

$$s_t = f(Ux_t + Ws_{t-1}). \tag{2}$$

Equation (1) is the formula for the output layer. $V$ is the weight matrix of the output layer, and $bg$ is the activation function. The output vector of the output layer is a function of the product of the vector $s_t$ corresponding to the hidden layer and the output weight matrix $V$. It is activated by the activation function of the fully connected layer, which varied linearly or nonlinearly, and then output as $o_t$.

Equation (2) is the formula of the hidden layer. In the RNN, the implicit layer, i.e., the recurrent layer, is the most important component of the network. The output $s_t$ of the implicit layer at the current moment $t$ is the product of the input vector $x_t$ and the input weight $U$ of the current input layer, and the sum of the product of the output $s_{t-1}$ of the implicit layer and the weight matrix $W$ of the implicit layer at the previous moment $t-1$. In the formula, the output $s_{t-1}$ of the previous moment is in turn a function of the output of the previous moment, thus going forward to any previous moment $t'$. Thus, the RNN can learn the historical features of the data.

The specific formula is as follows:

$$\begin{aligned} o_t &= g(Vs_t)Vf(Ux_t + Ws_{t-1}), \\ &= Vf(Ux_t + Wf(Ux_{t-1} + Ws_{t-2})), \\ &= Vf(Ux_t + WVf(Ux_t + Wf(Ux_{t-1} + Wf(Ux_{t-1} + Wf(Ux_{t-2} + Ws_{t-3})), \\ &= Vf(((Ux_t + Wf(Ux_{t-1} + Wf(Ux_{t-2} + Wf(Ux_{t-3} + Ws_{t-4}))))), \\ &= \ldots \end{aligned} \tag{3}$$

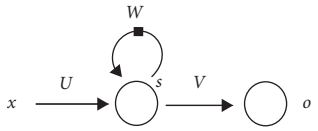


Figure 1: RNN structure diagram.

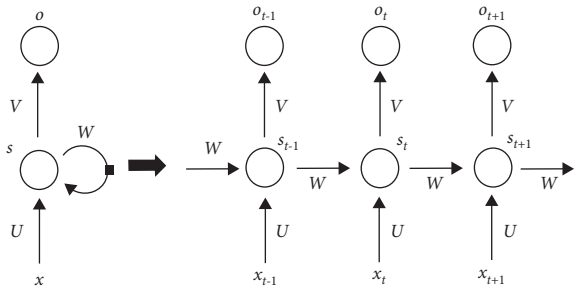


Figure 2: RNN structure unfolding diagram.

*2.2. LSTM Neural Network.* RNNs have problems in practical applications such as gradient disappearance and gradient explosion, where gradient disappearance makes the time series information learned by the neural network shorter [11]. To solve the problem, a new type of network structure is proposed: an LSTM neural network.

An LSTM neural network is called "long short-term memory neural network," which is a recurrent neural network, similar to the RNN, and is also suitable for processing time series information.

From Figure 3, the input vectors of the LSTM at moment $t$ are as follows:

(1) The input vector of the LSTM network at the current moment $x_t$

(2) The output vector of the LSTM at the previous moment $h_{t-1}$

(3) The cell state vector of the previous moment $c_{t-1}$

The outputs of the LSTM network are as follows:

(1) The LSTM output vector at the current moment $h_t$

(2) The unit state vector at the current moment $c_t$

The LSTM neural network algorithm is implemented primarily by opening and closing doors. In an LSTM neural network, the gate can be considered as a fully connected layer, where the input to the gate is a vector and the output is a real number between 0 and 1, indicating the degree of opening and closing of the gate.

The opening and closing of the door are represented as follows:

$$g(x)\sigma(Wx + b). \tag{4}$$

In the formula, $W$ is the weight of the gate and $b$ is the bias term. The opening and closing of a gate are determined by the combination of the gate's weight $w$ and the gate's input vector $x$ plus the bias term $b$. Since the gate outputs through the fully connected layer and its activation function is a sigmoid function, the output value of the gate is a value

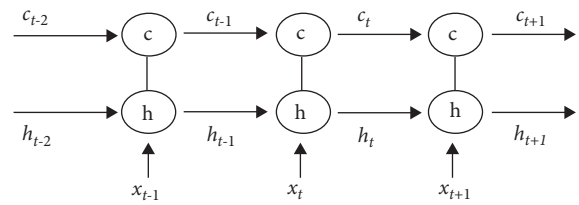


Figure 3: LSTM neural network structure diagram.

between 0 and 1. When the gate output is 0, no information can pass through the gate into the neural network unit and the gate discards that information; similarly, when the gate output is 1, any information can pass through the gate into the neural network unit and the gate keeps that information. However, due to the nature of the sigmoid function, all gates cannot be fully opened or closed, so the gates will filter all information and partially retain or discard it.

The most important of the LSTM neural network unit states are the forgetting gate and the input gate. The forgetting gate controls the neural network unit state, choosing which part of the unit state content from the previous moment is forgotten, i.e., choosing part of the unit content $c_{t-1}$ to go to the next moment. The input gate controls the relationship between the input vector $x_t$ of the neural network unit state and the unit state $c_t$, i.e., how much of the input unit vector is fed into the unit state. In addition to this, the LSTM uses an output gate to regulate the proportion of the unit state $c_t$ output to the current output value $h_t$ of the LSTM.

The formula for the forgetting gate is as follows:

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right). \tag{5}$$

In the formula, $W_f$ is the weight matrix of the forgetting gate, $[h_{t-1}, x_t]$ denotes the splicing of vector $h_{t-1}$ and vector $x_t$, $b_f$ is the bias term, and $\sigma$ is the binary sigmoid activation function.

The dimensionality of the weight matrix can be calculated using the dimensionality of each cell inside the LSTM neural network. The dimension of the weight matrix $W_f$ is expressed as follows:

$$d_c \times (d_h + d_x). \tag{6}$$

In the formula, $d_x$ denotes the dimension of the forgetting gate, $d_h$ denotes the dimension of the implied layer, and $d_c$ denotes the dimension of the cell state.

The weight matrix is a combination of $W_{fh}$ and $W_{fx}$, and in the formula, $W_{fh}$ corresponds to the input $h_{t-1}$ at the previous moment in the hidden layer, and $W_{fx}$ corresponds to the input vector $x_t$. $W_f$ is denoted as follows:

$$\begin{aligned}\left[W_f\right]\begin{bmatrix} h_{t-1} \\ x_t \end{bmatrix} &= \left[W_{fh}\, W_{fx}\right]\begin{bmatrix} h_{t-1} \\ x_t \end{bmatrix} \\ &= W_{fh}h_{t-1} + W_{fx}x_t.\end{aligned} \tag{7}$$

Input gate is expressed as follows:

$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t] + b_i\right). \tag{8}$$

In the formula, the parameters of the input gate are $W_i$ and $b_i$. $W_i$ is its weight matrix, and $b_i$ is the bias term.

The input state $\tilde{c}_t$ is obtained from a linear combination of the previous output and the current input by the calculation of the activation function:

$$\tilde{c}_t = \tanh\left(W_c \cdot \left[h_{t-1}, x_t\right] + b_c\right). \tag{9}$$

The current state $c_t$ is derived from a linear combination of the previous cell state $c_{t-1}$ and the current input cell state $\tilde{c}_t$:

$$c_t = f_t \circ c_{t-1} + i_t \circ \tilde{c}_t. \tag{10}$$

In the formula, the symbol $\circ$ denotes multiplication by elements. From equation (10), it can be seen that, the new memory unit $c_t$ is a combination of $\tilde{c}_t$ and $c_{t-1}$. The LSTM neural network can preserve previous time series information through forgetting gates, while controlling the entry of currently unimportant information through output gates.

Output gate is expressed as follows:

$$o_t = \sigma\left(W_o \cdot \left[h_{t-1}, x_t\right] + b_o\right). \tag{11}$$

The final output of the LSTM network is obtained by multiplying the output gate and cell state elements as follows:

$$h_t = o_t \circ \tanh\left(c_t\right). \tag{12}$$

*2.3. Data Enhancement Method Based on an Adversarial Generative Neural Network.* The collected communication messages of electric power terminals have different percentages of different attack types, among which DoS (denial-of-service) attacks account for 61% of the proportion of all messages; however, U2R attacks account for only 0.37% of all messages. In learning the communication message patterns of power terminals, in order to get better generalization performance of the model, we need to attack as many samples of various types of messages as possible; however, there are some attack messages for which the data are very sparse in the normal operation of power systems [12]. Therefore, in order to improve the accuracy of the detection model of the power terminal information attack, a large number of new attack sample data are generated by adversarial generative neural network simulation as a way to make the detection model more stable and reliable.

When using the adversarial generative neural network to generate samples, the selection of the generator and discriminator parameters is the key, as shown in Table 1.

By continuously optimizing the generator and the discriminator, the generator and the discriminator continuously play and learn, and finally generate new attack samples through the generator. In the specific training process of the adversarial generative neural network, the generator is first fixed, then the discriminator is optimized, and then the discriminator is updated; then, the discriminator is fixed again, the generator is updated, and the cycle is repeated; and finally, a complete adversarial generative neural network is trained.

Table 1: Parameters of the antagonistic generative neural network.

| Parameters | Values | |
|---|---|---|
| | Generator | Discriminator |
| Input cell dimension | 9 | 9 |
| Output cell dimension | 9 | 1 |
| Activation function | Linear | Sigmoid |
| Number of layers of the network | 3 | 3 |
| Number of hidden layer cells | 9, 32, 9 | 9, 32, 1 |
| Optimization goals | RMSE | Logloss |

Then, the attack samples of power terminal messages are generated by the trained adversarial generative neural network. Based on the 3,495,079 negative samples collected previously, 400,000 new negative samples are generated by the adversarial generative neural network method, which is used to increase the data sample set.

## 3. Conclusions and Optimization Suggestions

*3.1. Power Terminal Security System Experiment.* Simulation tests are conducted on the power terminal security monitoring system through the power terminal security detection simulation platform, including the normal operation of the power terminal and abnormal operation, to obtain samples of the power terminal side channels.

*3.1.1. Experimental Setup.* In this paper, there are four kinds of attacks on the DTU equipment used: (1) DTU distribution switch attack, (2) information acquisition attack, (3) DTU monitoring road number attack, and (4) DTU overload attack. Among them, DTU distribution switch attack refers to the DTU control distribution switch to continuously open and close operations; such attacks will affect the stability of the power grid and at the same time will significantly reduce the service life of the distribution switch; information acquisition attack refers to significantly increase the collection frequency of the DTU, while ensuring that the frequency of DTU information uploaded to the main station and substation of distribution automation does not change, so as to evade the detection mechanism; DTU monitoring road number attack refers to reducing the number of monitored switch paths, such as changing the previous 8 paths to 2 paths, and significantly reducing the amount of data collected and transmitted, thus affecting the power consumption; and DTU overload attack means increasing the computation capacity of DTU so that the legitimate service does not get a timely response, which has a similar effect as DoS attack [13].

The dataset includes several parts:

(1) Training set: Simulation of the operation state of the electric power terminal is performed on the simulation platform, and the normal and abnormal power consumption information of the device is collected for four days, from which 9600 power consumption information of the electric power terminal is obtained, and each power consumption information is labeled.

(2) Test set: Simulation of the operation state of the power terminal is carried out on the simulation platform, and the power consumption information of the device on the fifth day is collected as the test set for model training, with a total of 2400 power consumption information. The model will learn the power consumption behavior of the first four days to predict the power consumption information on the fifth day.

*3.1.2. Experimental Analysis.* The LSTM neural network model is built by the Keras library in Python. The performance of the power terminal security monitoring model is evaluated by accuracy, TPR (true-positive rate), and FPR (false-positive rate), which are defined as follows:

$$\begin{aligned} \text{Accuracy} &= \frac{\text{TP} + \text{TN}}{\text{P} + \text{N}}, \\ \text{TPR} &= \frac{\text{TP}}{\text{TP} + \text{FP}}, \\ \text{FPR} &= \frac{\text{FP}}{\text{FP} + \text{TN}}. \end{aligned} \tag{13}$$

First, the label separability of several abnormal attacks is analyzed, and the mean power consumption and peak power consumption of power terminal devices under normal operation and abnormal operation are extracted, respectively, and 12,000 power consumption samples are collected; the results are shown in Figure 4.

From the figure, it can be seen that the attacks on DTU have more obvious distinguishability in the dimension of power consumption and over zero-point value, and they can be clustered in different areas separately, which indicates that the monitoring of the working state of the power terminal can be achieved in the perspective of power consumption through data mining and feature extraction, and lays the foundation for using the LSTM neural network for classification afterwards.

The safety monitoring model is trained by learning some of the features in turn, and the accuracy of the safety monitoring model is compared to evaluate the features. The results are shown in Figure 5.

As can be seen from the figure, the accuracy of the model is relatively low when only a few features are used to learn the model, and the accuracy of the model is gradually improved as the number of feature dimensions continues to increase. Because the LSTM neural network is divided into linear combinations of features and learns the characteristics of the combined features, these characteristics can better express the safety state of the power terminal, thus achieving higher accuracy.

The TPR and FPR values of the power terminal security monitoring model are calculated, where TPR is the true-positive rate, which refers to the ratio of positive instances identified by the model to all positive instances, and FPR is the false-positive rate, which refers to the ratio of negative instances identified by the model to all negative instances. The ROC curves of the model are shown in Figure 6.

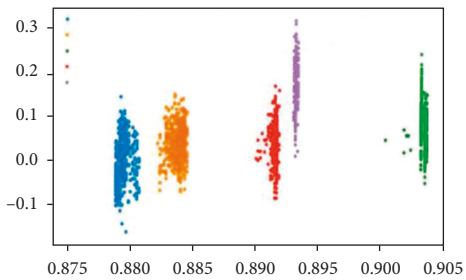


Figure 4: Separability analysis of DTU attacks.

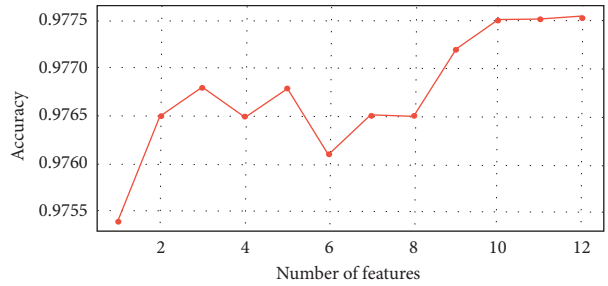


Figure 5: Effect of the number of features on model performance.

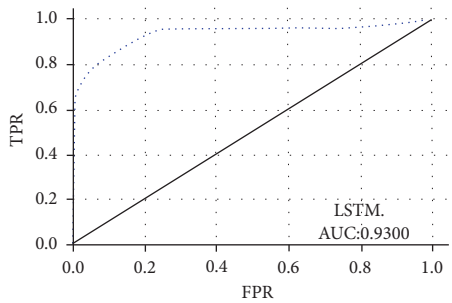


Figure 6: ROC curve.

As can be seen from Figure 6, the model proposed in this paper has good generalization performance. In the experiment, 9600 samples are selected as training data and 2400 samples as test data. Through the model test, the AUC value of the power terminal security monitoring system is calculated to be 0.9300, which indicates that the power terminal security monitoring model can monitor the operation status of DTU well and also can improve the security performance at the device level.

### 3.2. Power Terminal Information Attack Detection Experiment

*3.2.1. Experimental Setup.* The power I&C message data generated based on an adversarial generative neural network are divided into four datasets: (1) the original dataset, (2) the original dataset plus some newly generated small dataset, (3) the original dataset plus some newly generated medium dataset, and (4) the original dataset plus some newly generated large dataset, as shown in Table 2.

Table 2: Power industrial control message dataset.

| No | Dataset type | Size of the newly generated dataset | Total dataset size |
|---|---|---|---|
| 1 | Original dataset | — | 4599799 |
| 2 | Original dataset + partial small dataset | 40000 | 4599799 |
| 3 | Original dataset + partial medium dataset | 160000 | 4719799 |
| 4 | Original dataset + partial big dataset | 400000 | 4959799 |

Table 3: Fifty-fold cross-validation dataset.

| Parameters | Values | Parameters | Values |
|---|---|---|---|
| Optimizer | SGD | Learning rate | 0.01 |
| Batch size | 32 | Number of training rounds | 10 |
| Number of neural network layers | 5 | Input units | 86 |
| Hidden layer units | 128, 64, 32 | Dropout | 0.1 |
| Activation functions | Tanh | Pretraining optimizer | SGD |

The neural network model is built through the TensorFlow library in Python, in which the model is tested using the fivefold cross-validation method, and its model parameters are shown in Table 3.

*3.2.2. Experimental Results and Analysis.* First, the similarities and differences between the proposed power terminal security monitoring party and traditional machine learning methods are compared in this paper. The similarities and differences between the proposed deep neural network (DNN) and the random forest (RF) model, the linear regression (LR) model, and the K-nearest neighbour (KNN) model performance on the original dataset were first compared. The results are shown in Figure 7.

From Figure 7, it can be seen that the proposed model has good performance on the original dataset, where the accuracy of the KNN model is 0.8521, the accuracy of the RF model is 0.9201, the accuracy of the *L* model is 0.8211, and the accuracy of the DNN model is 0.9431. The poor performance of the LR model is mainly due to the generalization performance of the LR model. The generalization performance of the LR model is mainly determined by feature engineering. For communication messages from power terminals, there are limitations in improving the generalization performance of the model through feature engineering; therefore, the LR model has the worst performance. The performance of the random forest model is better than that of the linear model because the random forest model is able to improve the generalization performance of the whole model by bagging multiple models and complementing the strengths of each base model. However, the tree model is unable to extract the deeper information of the power terminal messages. However, the DNN model can extract the deep attack patterns of the attack messages through the nonlinear action of neurons, so the deep neural network approach can better mine the deep information in the power message samples [14]. Therefore, the model achieves a higher accuracy rate.

To overcome the problem of small number of attack samples, adversarial generative neural networks are used to generate more attack samples. Depending on the number of attack samples generated, they are divided into attack samples for small datasets, attack samples for medium datasets, and attack samples for large datasets. In order to compare the performance improvement of the newly generated attack samples on the power terminal security measurement system, the performance of the power terminal security monitoring model was compared with the original dataset plus the newly generated dataset, and the results are shown in Figure 8.

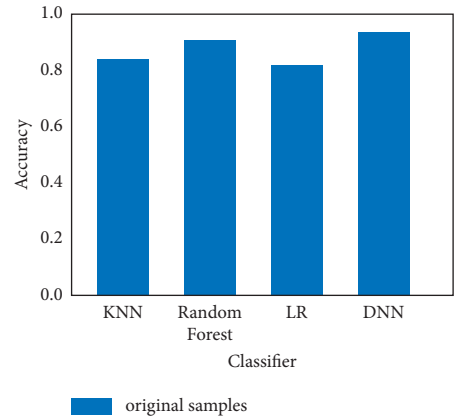


Figure 7: Accuracy comparison of the four classifiers.

As can be seen from Figure 8, the accuracy of the model improved with the addition of the newly generated attack message samples. This is due to the fact that the DNN model requires more training samples than the other linear models or tree models. Neural networks need to capture the patterns of attack messages by mining the samples for deeper information. The performance of the DNN model was enhanced by the samples generated by the GAN, and the RF model was improved by increasing the number of samples from 0.9201 to 0.9271, but the performance of the model was not overly dependent on the size of the dataset due to the bagging strategy.

### 3.3. Discussion

First, it provides a method to quickly obtain knowledge points in test set for the huge amount of resources,

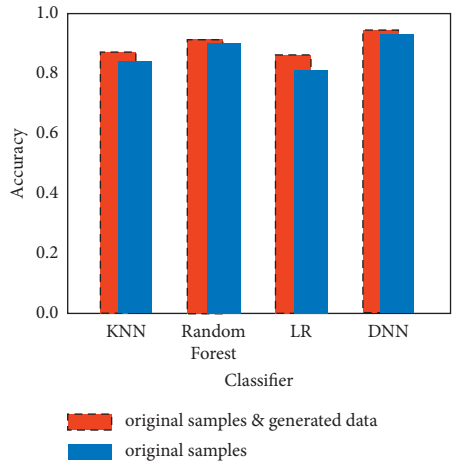


Figure 8: Accuracy of the four classifiers on different datasets.

provides comprehensive and effective knowledge points for teachers, students, teaching resource developers, etc., and solves the problem of comprehensive and effective extraction of knowledge points from a large amount of resources.

Second, it enhances the quantification of the organization form of the knowledge structure of materials, provides more objective, reasonable, and comprehensive references to the organization form of the knowledge structure of materials for material developers, etc., satisfies the scientific knowledge structure of materials in terms of rich content and compact knowledge structure of materials, and solves the difficult problem of organizing the knowledge structure of a large number of materials.

Third, this paper proposes and designs an electrical safety management system based on the IoT technology, which is mainly applied to field operations. Relying on the hardware and software design of the safety management system, it is possible to realize the improved research in this paper. The data of simulation experiments show that compared with the initial system, the risk factor of field operation obtained by the safety management system designed in this paper is lower, which can more effectively guarantee the safety of fieldworkers and the working instruments required for field operation.

## 4. Conclusion

The large-scale interconnection of power grids has led to an increase in the voltage level of power system operation, and the increasing standard of living has led to higher requirements for the stability of power grid operation, which has significantly increased the power supply capacity of urban power grids and increased the risk of safety operation and management. Through the previous study, urban smart grid safety operation management can focus on grid scheduling, fault diagnosis, and risk prediction and evaluation [15].

First, grid dispatch in urban smart grid security operation management involves locations, places, and behaviors. Due to the complexity of power grid operations with diverse characteristics, in order to effectively implement the corresponding supervision and management work, it is necessary to combine the content of enterprise operations and related work requirements in an orderly manner to carry out specific control behavior. On the one hand, the causes of dangerous accidents should be summarized in a centralized analysis of the danger points and effectively anticipate their development. On the other hand, it is necessary to supervise the factors and related problems that are easy to generate dangerous points in an integrated manner, and effectively avoid sudden changes of dangerous points. The power system is a very complicated system; its complexity not only includes the structure of the system, but also includes the composition of the grid components of the diversity, the grid operation mode diversity, the grid in the environment of the diversity, and the grid received by the load of the variety of risk factors [16]. This diversity leads to the diversity and complexity of the risks faced by the grid. The establishment of the index system is to differentiate the different risks to the grid operation caused by safety incidents. Both the State Grid Corporation and the Southern Power Grid Corporation have graded the grid risk accidents. The size of the grid risk is an important basis for the staff to take preventive and management measures. The grading of the grid risk is very important for the scientific evaluation of the grid operation risk and for the grid staff to have a more comprehensive understanding of the actual operation of the grid [17].

Second, the random forest algorithm (Bootstrap) can be used for grid fault diagnosis in urban smart grid security operation management to shorten fault handling time and improve grid reliability. The random forest algorithm is a repetitive sampling technique, in which a new set of training samples is generated from the original training sample set by repeatedly drawing a random sample, and then, a random forest of decision trees is generated based on the self-help samples. Each tree in the forest has the same distribution, and the classification error depends on the classification ability of each tree and the correlation between them. The random forest algorithm is used in the study of grid fault diagnosis, although the random forest algorithm is a black box model with no control over the internal operation, and can only be tried continuously between different parameters and random seeds [18]. However, the algorithm has a powerful learning generalization ability, which can better solve the learning problem of the neural network algorithm itself, the problem of falling into local optimal solution, and the correlation between sample attributes by the plain Bayesian network algorithm [19]. In addition, the random forest algorithm also has the advantages of balancing errors on unbalanced data and fast training speed, which can well solve the problem of unbalanced fault data types.

Finally, the next research step of urban smart grid safety operation management focuses on grid risk prediction and evaluation based on risk theory. Random failures of equipment in the system are often beyond the normal human ability to predict, and there are many uncertain risk factors that make it difficult for grid operators to intuitively make accurate judgments about risk. With the large-scale interconnection of power grids, the contradiction between the risk of power grid operation and the level of economic and social development and people's daily life requirements is becoming more and more prominent. In the power market environment, the input and output of electric energy are closely related to the rapidly changing market demand. The operating cost of power generation and transmission is a key factor that grid companies must consider, and in order to reduce operating costs, they often not only fail to build new transmission lines in time, but also often make the grid operate at its limit, which brings great risk to the stable operation of the power system [20]. In order to ensure the stable operation of the power grid and guarantee the reliable level of social power supply, it is necessary to further strengthen the management process of the power grid, standardize the risk analysis of the power grid, optimize the risk assessment and control workflow, effectively evaluate and prevent the potential risk factors of the power grid, so as to systematically deal with the existing safety hazards and weak links of the power grid, reasonably carry out maintenance and transformation, and thus realize the prevention of power grid accidents in advance. This will enable us to prevent grid accidents in advance.

## Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

## Conflicts of Interest

The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

## Acknowledgments

This work was supported by the Jiangsu Province Policy Guidance Program (International Science and Technology Cooperation)—Key National Industrial Technology Research and Development Cooperation Project (Project Title: Joint Research and Development of Smart Power Grid Topology Stability System Architecture based on DSM, Project Number: BZ2021033).

## References

[1] Z. W. Jiang, D. Wang, and H. Y. Wang, "power smart terminal security assessment model[J]," *Computer Engineering and Design*, vol. 35, no. 1, pp. 6–10, 2014.

[2] Q. Nan, Y. Q. Lei, and B. Y. Huang, "Research on power terminal communication access architecture under smart grid [J]," *Power System Communication*, vol. 33, no. 1, pp. 74–77, 2012.

[3] X. Fang, Y. Wan, and X. Wen, "Research on the method of DDoS attack in network intrusion detection system based on protocol analysis technology[J]," *Information Network Security*, vol. 4, pp. 20–30, 2012.

[4] Z. J. Cao, Y. F. Zhao, and X. F. Rong, "Network intrusion detection and firewall linkage platform design[J]," *Information Network Security*, vol. 9, pp. 32–40, 2012.

[5] Y. A. Yang, H. Z. Huang, and Q. N. Shen, "Research on intrusion detection based on incremental GHSOM neural network model[J]," *Journal of Computer Science*, vol. 37, no. 5, pp. 1216–1224, 2014.

[6] T. Verschueren, W. Haerick, K. Mets, C. Develder, F. D. Turck, and T. Pollet, "Architectures for smart end-user services in the power grid," *IEEE/IFIP Network Operations and Management Symposium Workshops*, vol. 2010, pp. 316–322, Article ID 5486557, 2010.

[7] J. L. Yang, S. H. Xiao, L. W. Liang, and C. L. Philip Chen, "Cyber security and privacy issues in smart grids.[J]," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 156–168, 2012.

[8] W. Lee, X. Lin, R. Schober, and W. S. W. O. N. G. Vincent, "Direct electricity trading in smart grid: a coalitional game analysis.[J]," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 74–85, 2014.

[9] S. D. Beigvand and H. Abdi, "Optimal power flow in the smart grid using direct load control Program[J]," *Journal of Operation and Automation in Power Engineering*, vol. 3, no. 2, pp. 85–92, 2015.

[10] S. Li and X. D. Wang, "Cooperative change detection for voltage quality monitoring in smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 86–99, 2016.

[11] R. Pal and V. Prasanna, "The STREAM mechanism for CPS SecurityThe case of the smart grid[J]," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 4, pp. 34–42, 2017.

[12] T. Yalcin and M. Ozdemir, "Computational intelligence methods for identifying voltage sag in smart grid[J]," *Advances in Science, Technology and Engineering Systems*, vol. 2, no. 3, pp. 125–134, 2017.

[13] X. Y. Wang, Y. F. Huang, H. J. Zhu, and H. F. Jiang, "Study on variable lane control method application in ITS[J]," *Basic and Clinical Pharmacology and Toxicology*, vol. 10, pp. 14–22, 2019.

[14] Z. Y. Feng, Q. Li, T. A. Gulliver, and P. Zhang, "Priority-based dynamic spectrum management in a smart grid network environment.[J]," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 5, pp. 101–105, 2015.

[15] P. L. Fevre, "Is your smart grid secured? [Expert view][J]," *IEEE Power Electronics Magazine*, vol. 3, no. 4, pp. 86–96, 2016.

[16] C. Zhong, J. Li, B. Ding, and S. Y. Guo, "Investigation of directional wide-beam radial line slot antenna for smart grid fault detector," in *Proceedings of the 11th International Conference on Computer Engineering and Networks(CENet2021)*, pp. 617–624, NY City, July 2021.

[17] J. G. Lu, J. J. Fu, J. Zhang, and K. Q. Zhang, "Multi-machines and multi-tasks scheduling for UAV power inspection in smart grid," *Proceedings of the 11th International Conference*

*on Computer Engineering and Networks(CENet2021)*, vol. 40, pp. 733–741, 2021.

[18] P. J. F. Torres, L. Ekonomou, and P. Karampelas, "The correlation between renewable generation and electricity demand: a case study of Portugal," *Energy Syst*, pp. 119–151, 2016.

[19] B. A. Ugale, P. Soni, T. Pema, and A. Patil, "Role of cloud computing for smart grid of India and its cyber security," *NUiCONE 2011-Conference Proceedings*, vol. 2011, Article ID 6153298, 2011.

[20] R. Zafar, A. Mahmood, S. Razzaq, W. Ali, U. Naeem, and K. Shehzad, "Prosumer based energy management and sharing in smart grid," *Renewable and Sustainable Energy Reviews*, vol. 82, pp. 1675–1684, 2018.