Research on Deep Belief Network of Wind Power Control Management Unit Based on Attack Identification

Wei Liu¹, Zhiwei Huang², Rui Chen², Kai Ding², Xiaofan Zhu², Junfeng Zhou², Guoqi Zhou², Shengguo He², Hongyan He², Shengyuan Xiao², Feng Lu², Guoyou Wang², Baifeng Ning¹ and Qing Ding¹

¹Shenzhen Power Supply Bureau Co., Ltd, China Southern Power Grid. Shenzhen 51800, China
²CYG SUNRI CO., LTD, Shenzhen 518000, China
Corresponding author e-mail: hzw@sznari.com

Abstract. With the continuous improvement of the level of economic development and the increasingly serious environmental problems, countries around the world are focusing more on renewable energy. Wind energy is an important category of renewable energy because of its advantages. However, wind power is very dependent on the climate environment. It operates in an open operating environment, and its communication depends on the network interaction method. With the proposal of the Internet of Everything, the power grid is developing in the direction of information and intelligence. There are more and more attacks, and the security and stability of wind power interface devices have been threatened. As the power grid involves many areas and households, once the power outage occurs, the economic losses will be huge and even cause major security accidents. This paper proposes a deep belief network research of wind power control management unit based on attack recognition to improve the safety and operational reliability of wind power generation.

1. Introduction

With the rapid economic growth and all-round social progress, China's energy supply has caused great concern at home and abroad. The relationship between supply, demand and supply of coal, electricity, oil and transportation has obviously tightened. Among them, the situation of power shortage is increasingly prominent. Insufficient energy supply has become an important factor restricting China's sustainable economic development. Therefore, the development and utilization of new and renewable energy sources[1-4] is one of the important strategic measures to solve China's energy and environmental protection problems.

In addition to hydropower, wind power[5-8] is the most mature technology, the largest scale development and commercial development prospects in the development and utilization of renewable energy in the world. Resolving the outstanding role of residents in remote areas, etc., has shown good prospects for development and is one of China's important follow-up energy sources.

At the current stage, China's research on wind energy is continuously increasing, and the state's support policies for the wind power industry have been continuously issued, so that the wind power technology continues to be improved. As a typical renewable resource, its reserves are far greater than the total amount of other energy sources. In this context, the wind power industry has an inestimable development prospect as a new industry. However, wind power is very dependent on the climatic environment, and power generation is unstable and indirect. Therefore, when a large number of wind turbines are connected to the power grid, their operating status information needs to be obtained in a
timely and accurate manner and uploaded to the superior dispatching center through the wind power interface. On the other hand, with the proposal of the interconnection of all things, the power grid is developing in the direction of information and intelligence, and various network attacks[9-12] are also facing more and more. Wind power interface devices in open operating environments The security and stability of the power grid have been threatened. Because the power grid involves many areas and households, once a power outage occurs, the economic losses will be huge and even cause major security accidents. In the past few years, many cases have occurred in the world due to the time of large-scale power outages caused by cyber attacks, so it can be seen that the importance of security precautions is becoming increasingly prominent.

2. Development Status

Figure. 1 is a diagram of an application scenario of the prior art. It can be seen from Figure 1 that the inverters of multiple wind turbines are generally connected to the wind power management system, receive control of the wind power control system and receive wind power data, and the wind power management system is connected to the central controller. The wind power data of the transformer is collected and uploaded to the central controller. The central controller adjusts and controls the inverter according to the wind power data. The wind power management system implements the inverter of the wind power generation device under the active interactive control and coordination framework of the power distribution network. Coordinate with local control on the network side. The wind power management system can first evaluate the operating status of the inverter and accept the control instructions of the upper-level control unit of the active power distribution network. The wind power generation device has fluctuations. The active control of the inverter is based on the derating control based on the maximum power that can be generated. The wind power management system can obtain the maximum adjustable within one or several control cycles in the future through ultra-short-term wind prediction. The generated power is fed back to the upper-level central controller to realize the predictive control of the wind power generation device. Of course, the wind power management system is also connected to the lower-level micro-source controller and intelligent circuit breaker to collect corresponding data. The wind power management system is an important bridge to realize the communication between the lower-level wind turbines and the upper-level dispatch center. Today, with the intelligent development of the power grid, its communication depends on the network interaction method. However, due to the development of network information, there are various as long as there is a security loophole in the fan, the attacker will use this as a breach to attack the device, causing the device to fail to work properly, and even using the loophole to further invade the entire large power grid and cause a large-scale power outage. Therefore, this paper combines actual work and research data to analyze the current shortcomings of wind power generation. Here, a deep belief network[17-20] study of wind power control management units based on attack recognition[13-16] is proposed to improve wind power. Power generation safety and operational reliability.
3. Attack Recognition Model

This paper proposes a deep belief network research device model for wind power control management unit based on attack recognition. As shown in Figure 2, it includes a power supply unit, a main control unit, a data processing unit, a USB interface, a touch screen, an input acquisition unit, an output control unit, and a network. Communication unit and LED running status light. The main control unit is connected to the network communication unit, USB interface, output control unit, touch screen, and data processing unit. The power supply unit is connected to the main control unit and data processing unit. The data processing unit is also connected to LEDs. Operation status light, AC sampling unit, input acquisition unit, the main control unit is connected to the upper layer (central controller) through a network communication unit, and the data processing unit is connected to the lower layer (inverter, inverter, Micro-source controller, intelligent circuit breaker) to collect data.

Among them: the main control unit is used to complete the coordinated control function of other units, receive the upper-level control instructions, switch the working state of the wind turbine, and process the real-time wind power data according to the classification results sent by the data processing unit. When anomalous data of the network attack type is issued, an attack alarm is intercepted and the data of the network attack is intercepted and a log record is generated. At the same time, the normal data belonging to the normal class is forwarded through the network communication unit; the USB interface is used to pass the external device. The main control program of the wind power management system is upgraded; the input acquisition unit is used to receive part of the wind power data of the inverter connected to the wind power. The data stream is obtained from the inverter and then transmitted to the data processing unit; output the control unit is used to send output instructions issued by the main control unit to the lower layer for coordinated control; the touch screen is used for human-computer interaction and display information, including attack alarms and operation history data viewing; LED operating status lights are used to display whether the current data processing unit is normal work; network communication unit is used for data transmission between the main control unit and the upper central controller (that is, the wind power data collected by the inverter obtained by the wind power management system and uploaded to the central controller). It can be configured with multiple communication protocols and the wind turbine operation monitoring.
master station. Time synchronization between messages; AC sampling unit is used to collect the current and voltage analog quantity as part of the wind power data and send it to the data processing unit; the data processing unit is used to obtain real-time wind power data through the trained deep belief network Real-time detection of real-time wind power data, classification of real-time wind power data, generation of classification results, and transmission to the main control unit.

Figure 2. Internal structure of the wind power

4. Implementation Steps

4.1. Overall Implementation Steps
The purpose of the present invention is to provide an attack identification method and a wind power management system based on a deep belief network. The technical problem to be solved is to be able to implement active defense against unknown attacks and improve the information security and operational reliability of wind power generation. The overall implementation steps are shown in Figure 3.

Figure 3. Attack recognition overall implementation steps
Step 1: Collect normal data and abnormal data after being attacked by the network, then integrate the normal data and abnormal data according to different types of attacks, and classify the abnormal data of the same label into the same one. In the abnormal classification, all the classifications are used as training samples to obtain a training database; the normal wind power data includes ambient temperature, wind speed, wind direction, air density, air pressure, fan blade speed, fan number, fan status, generated power, fan output power, generator voltage, current, etc.; abnormal data can be collected through abnormal wind power data (as described above) generated by network attack on normal data; the classification includes normal class, network attack class, the network attack Classes include DOS (denial of service attack), R2L attack, U2R attack, power stealing attack, DDoS (distributed denial of service) attack, unauthorized access attack, Trojan horse attack, detection and scanning attack, etc.

Step 2: Train the deep belief network, input the reference database to the deep belief network, and obtain the trained deep belief network through deep learning;

Step 3: Obtain real-time wind power data of the wind turbine, perform real-time detection of real-time wind power data through the trained deep belief network, classify the real-time wind power data, and generate a classification result. When the wind power data is classified, all the data belong to the normal category. When the wind power data is classified, there is abnormal data belonging to the network attack class, it is determined that there is a network attack, and the abnormal data with the network attack is performed at the same time as the alarm is issued. Intercept and generate log records, and send attack alarms and log records up to the superior central controller.

4.2. Specific Algorithm Implementation Steps
In the second step, the following network structure (shown in Figure 4) is adopted for the deep belief network, which includes an input layer, a hidden layer, and an output layer, where the hidden layer is composed of three layers of restricted Boltzmann machines (RBM). Each RBM has two layers of neurons. One is the dominant layer (dominant layer), which is composed of dominant neurons (dominant cells). It is responsible for inputting training data, and the other is a hidden layer (hidden layer). Neurons (cryptons) are composed as feature detectors. In RBM, there is a weight W between any two connected neurons to indicate their connection strength, and each neuron itself has an offset coefficient b (for the explicit element) and c (for the hidden element) to represent its self weight.

![Figure 4. Schematic diagram of a deep belief network algorithm](image)

The training of the deep belief network in step two is implemented by the following steps (see Figure 5):
Enter reference database

Standardize the S-excitation function for each hidden element

Calculate the probability of the hidden element being activated

Calculate the probability that an explicit element will be activated

Use the reconstructed explicit element to calculate the probability of the hidden element being activated, and obtain a new hidden layer

Determine the weight and offset of RBM1, and then use its hidden layer as the obvious layer of the second RBM2

Repeat (2)-(5) until all RBM training is completed

Set up a back-propagation neural network at the last layer of the deep belief network

Get a trained deep belief network model

Figure 5. Implementation steps of the deep belief algorithm

1. Enter the reference database into the deep Belief Network (DBN);
2. Train RBM in deep belief networks, including:
   (1) Normalize each hidden element with the S excitation function, and change the probability value of them to being active, S excitation function is

\[
\delta(x) = \frac{1}{1 + e^{-x}}
\]

Where: \( x \) represents the value passed by the explicit layer multiplied by the weight plus the deviation of the hidden layer; the value passed by the explicit layer is the sample data in the input training sample, and the weight is the connection between neurons;

(2) Calculate the probability that the hidden element is activated:
\[
P\left( h_j^{(0)} = 1 \mid v^{(0)} \right) = \delta \left( c_j + \sum_{i=1}^{m} W_{i,j} v_i^{(0)} \right)
\]

Among them: \( p \) is the probability of the hidden element being activated, \( h_j^{(0)} \) is the \( j \)-th activated hidden element, \( v^{(0)} \) represents the initial display layer, and \( v_i^{(0)} \) represents the \( i \)-th Display elements, each of which is the value of the sample data of the training samples in the training database, \( W_{n \times m} \) is the weight between the explicit layer and the hidden layer, and \( m \) is the total number of explicit layers. \( n \) is the total number of hidden elements in the hidden layer, \( j \) is the \( j \)-th hidden element, \( c_j \) is the offset of the \( j \)-th hidden element, and the initial offset \( c \) of the hidden layer is 0; The weight is the connection between the explicit layer and the hidden layer. The initialization of the weight \( W \) comes from the random number of the normal distribution \( N(0, 0.01) \);

Each node in the neural network accepts the input value and passes the input value to the next layer, and the input node directly passes the input attribute value to the next layer. In neural networks, there is a functional relationship between the inputs and outputs of the hidden layer and output layer nodes. This function is called the excitation function;

(3) Calculate the probability that the explicit element is activated:

\[
P\left( v_i^{(1)} = 1 \mid h^{(0)} \right) = \delta \left( b_i + \sum_{j=1}^{n} W_{i,j} h_j^{(0)} \right)
\]

Among them: \( p \) refers to the probability of activation of the explicit element, \( v_i^{(1)} \) represents the \( i \)-th activated element after reconstruction, \( h^{(0)} \) represents the hidden layer, and \( h_j^{(0)} \) represents the \( j \)-th hidden layer element. \( W_{n \times m} \) is the weight between the hidden layer and the hidden layer, \( n \) is the total number of hidden-layer hidden elements, \( i \) is the \( i \)-th hidden element, and \( b \) is the offset of the hidden element. The apparent layer offset is initialized as \( b_i = \log \frac{p_i}{1-p_i} \), where \( p_i \) is the proportion of samples in the training sample whose \( i \)-th feature is activated, and the feature is the training database. Sample data of training samples; The hidden layer represents activated features;

(4) Then use the reconstructed explicit element to calculate the probability of the hidden element being activated again, and obtain a new hidden layer \( h^{(1)} \);

\[
P\left( h_j^{(1)} = 1 \mid v^{(1)} \right) = \delta \left( c_j + \sum_{i=1}^{m} W_{i,j} v_i^{(1)} \right)
\]

Among them: \( p \) refers to the probability of the hidden element being activated, \( h_j^{(1)} \) represents the \( j \)-th hidden element activated by the reconstruction layer after the reconstruction, \( v^{(1)} \) represents the reconstruction layer after the reconstruction, \( v_i^{(1)} \) represents the \( i \)-th display element, the \( i \)-th display is the value of the reconstructed display element. \( W_{n \times m} \) is the weight between the display layer and the hidden layer, and \( m \) is the display layer. The total number of meta-elements, \( n \) is the total number of hidden-layer hidden elements, \( j \) is the \( j \)-th hidden element, and \( c_j \) is the offset of the \( j \)-th hidden element; The weight between the explicit layer and the hidden layer is the apparent layer and The connection between hidden layers;

(5) Update the offset and weight. The update formula is:

\[
\Delta W = [ P(h^{(0)} = 1 \mid v^{(0)}) v^{(0)T} - P(h^{(1)} = 1 \mid v^{(1)}) v^{(1)T} ]
\]

\[
W_{\text{new}} = W + \alpha \Delta W \tag{6}
\]

\[
b_i = b_i + \alpha (v_i^{(0)} - v_i^{(1)}) \tag{7}
\]

\[
c_j = c_j + \alpha [ P(h^{(0)} = 1 \mid v^{(0)}) - P(h^{(1)} = 1 \mid v^{(1)}) ] \tag{8}
\]

Where \( \Delta W \) represents the difference between the reconstructed display element and the input value, \( \alpha \) is the learning efficiency value of 0.01, \( W \) is the weight before the update, and the initialization of the weight \( W \) comes from the normal distribution \( N(0, 0.01) \) \( v^{(0)} \) is the initial apparent layer, \( v^{(0)T} \) is the transpose of \( v^{(0)} \), and \( h^{(0)} \) is the activated layer after activation.
layer, \( \psi^{(1)} \) is the reconstructed visible layer, the reconstructed visible layer maps the value to the hidden layer, and the hidden layer is activated to get \( h^{(1)} \); the layer is the sample data of the training samples in the training database;

(6) After one RBM is fully trained, determine the weight and offset of the RBM, and then use its hidden layer as the dominant layer of the second RBM;

(7) Repeat (1)-(6) until all RBM training is completed;

(8) After all RBM training is completed, a back propagation neural network is set at the last layer of the deep belief network, and the weight is fine-tuned using the back neural network;

(9) The trained deep belief network model is finally obtained.

Further, after step (9), a deep belief network model can also be tested, and data from any wind power data can be input to the trained deep belief network model for model verification. When the output result does not meet expectations, then after modifying the weight and offset, repeat steps (2)-(8) until the output result meets the expectations and ends.

5. Conclusions

With the society's emphasis on clean energy, wind power has played an increasingly important role in clean energy, but its work is in a development environment, and with the development of smart grids, the grid is moving towards information and intelligent, the direction of development is facing more and more various network attacks. The security and stability of wind power interface devices in open operating environments are threatened. Because the power grid involves many areas and households, once a power outage occurs, the economic loss is huge and may even cause major security accidents. The present invention performs active immunity based on a deep belief network. Therefore, this paper proposes a deep belief network study of a wind power control management unit based on attack recognition. By using layer-by-layer training, it solves the optimization problem of deep neural networks, and gives the entire network a good initial weight through layer-by-layer training, which allows the entire neural network to generate training data according to the maximum probability, so that the network can achieve the optimal solution as long as it is fine-tuned compared with current technology, it can do different attacks and identifying alert function, thereby enhancing information security, and operational reliability of wind power.

6. Acknowledgment

This work was by Supported by the National Key R&D Program of China (2018YFB0904900, 2018YFB0904903).

7. Reference

[1] Carrasco, J. M., Franquelo, L. G., Bialasiewicz, J. T., Galvan, E., Guisado, R. C. P., & Prats, M. A. M., et al. (2006). Power-electronic systems for the grid integration of renewable energy sources: a survey. IEEE Transactions on Industrial Electronics, 53 1002.

[2] Barton, J. P., & Infield, D. G. (2004). Energy storage and its use with intermittent renewable energy. IEEE Transactions on Energy Conversion, 19 441.

[3] Liserre, M., Sauter, T., & Hung, J. Y. (2010). Future energy systems: integrating renewable energy sources into the smart power grid through industrial electronics. IEEE Industrial Electronics Magazine, 4 18.

[4] Bull, S., R. (2001). Renewable energy today and tomorrow. Proceedings of the IEEE, 89 1216.

[5] Thomas Ackermann. (2003). Wind power in power systems. IEEE Power Engineering Review, 22 23.

[6] Wang, J., Shahidehpour, M., & Li, Z. (2008). Security-constrained unit commitment with volatile wind power generation. IEEE Transactions on Power Systems, 23 1319.

[7] Hetzer, J., Yu, D. C., & Bhattarai, K. (2008). An economic dispatch model incorporating wind power. IEEE Transactions on Energy Conversion, 23 611.

[8] Karki, R., Hu, P., & Billinton, R. (2006). A simplified wind power generation model for reliability evaluation. IEEE Transactions on Energy Conversion, 21 533.
[9] Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber–physical system security for the electric power grid. *Proceedings of the IEEE, 100* 210.

[10] Hahn, A., Member, S., IEEE, Member, S., & IEEE. (2011). Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid, 2* 835.

[11] Soltan, S., Yannakakis, M., & Zussman, G. (2017). React to cyber attacks on power grids. *IEEE Transactions on Network Science & Engineering, 99* 1.

[12] Bruno, C., Guidi, L., Lorite-Espejo, A., & Pestonesi, D. (2015). Assessing a potential cyberattack on the italian electric system. *Security & Privacy, IEEE, 13* 42.

[13] Pasqualetti, F., Dorfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control, 58* 2715.

[14] Ameli, A., Hooshyar, A., El-Saadany, E. F., & Youssef, A. M. (2018). Attack detection and identification for automatic generation control systems. *IEEE Transactions on Power Systems, 99* 1.

[15] Ashok, A., Govindarasu, M., & Wang, J. (2017). Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proceedings of the IEEE, 1* 19.

[16] Sahoo, S., Mishra, S., Peng, C. H., & Dragicevic, T. (2018). A stealth cyber attack detection strategy for dc microgrids. *IEEE Transactions on Power Electronics, 1* 1.

[17] Chen, Y., Zhao, X., & Jia, X. (2015). Spectral–spatial classification of hyperspectral data based on deep belief network. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 8* 1.

[18] Bu, S., Liu, Z., Han, J., Wu, J., & Ji, R. (2014). Learning high-level feature by deep belief networks for 3-d model retrieval and recognition. *IEEE Transactions on Multimedia, 16* 2154.

[19] Zhang, C., Lim, P., Qin, A. K., & Tan, K. C. (2017). Multiobjective deep belief networks ensemble for remaining useful life estimation in prognostics. *IEEE Transactions on Neural Networks and Learning Systems, 28* 2306.

[20] Chang, G. W., & Lu, H. J. (2018). Integrating grey data preprocessor and deep belief network for day-ahead pv power output forecast. *IEEE Transactions on Sustainable Energy, 1* 1.