Research on Attack Detection Method of Microgrid Central Controller Based on Convolutional Neural Network

Wei Xi¹,², Shengguo He³, Rui Chen³, Yongjun Xu³, Weifan Li³, Guoqi Zhou³, Weiguo Yu³, Hongyan He³, Zhiwei Huang³, Yang Yu¹,², Hao Yao¹,², Hui Liu³, Shengyuan Xiao³, Zhihui Yue³ and Wei Liu⁴

¹Electric Power Research Institute, China Southern Power Grid. Guangzhou 51000, China
²Digital Grid Research Institute, China Southern Power Grid. Guangzhou 51000, China
³CYG SUNRI CO., LTD, Shenzhen 518000, China
⁴Shenzhen Power Supply Bureau Co., Ltd, China Southern Power Grid. Guangzhou 51000, China
Corresponding author e-mail: hsguo@sznari.com

Abstract. The microgrid central controller (MGCC) integrates the functions of control, monitoring, and communication in microgrid system, and has powerful capabilities of information collection and data processing. However, with the development of microgrid system worldwide, the information security management capabilities of the MGCC are poor. If information/network attacks cannot be actively detected and identified, it will easily reduce the reliability of the microgrid system operation. Attackers can use abnormal information or use the MGCC as a springboard to further attack the upper-layer system. Aiming at the above problems, this paper presents an attack detection method based on convolutional neural network, and a detailed design process of attack detection model of the MGCC is proposed. In the attack detection method, the important data streams in the MGCC are used as the input of the convolutional neural network model, then the convolutional neural network model detects or classifies these data streams, finally, intercept the data flow with attack behavior and give a warning prompt, and forward data without attack behaviors normally.

1. Introduction
With the rapid growth of human demand for electricity and the scale of power systems, distributed generation technology has been widely used in clean energy such as photovoltaics and wind power, and has become one of the important topics in the development of power systems in recent years [1-3]. In order to better coordinate the contradictions between distributed units and large power grids, to maximize distributed energy efficiency and comprehensive utility, the concept of microgrid was proposed.

Microgrid is an independent power supply system that integrates distributed generation units, power electronics, energy storage devices, and loads. It can not only supply power to the load independently, but also can be connected to a large power grid to achieve a two-way flow of energy [4-5]. The development of microgrid technology has reduced the burden on large power grids, which can effectively improve the security reliability and flexibility of power systems.

Microgrid control system belongs to the power industry control system. As an important part of the country's key infrastructure, the power industry control system involves distributed power sources and power consumption information collection systems on the user side and in the open environment. If this important information is damaged, it may affect national and social security [6-8]. Especially with
the development of intelligent and information technology, the in-depth application of some information technologies and the development of security forms at home and abroad, the security threats faced by the micro network system cannot be ignored because of its lack of active attack detection ability and attack immunity. In recent years, many of the large-scale power outages in the world have been caused by network attacks or network information security incidents. In addition, there is no lack of cases that interfere with the stable operation of microgrids due to data tampering, and power outages caused by network attacks are still on the rise. Therefore, it is particularly important to improve microgrid's active attack detection capability and self-protection capability [9-10].

The MGCC is in the position of data interaction center and control center in the microgrid system, which can intelligently analyze and judge, issue the optimal microgrid control strategy, and coordinate the stable operation of intelligent devices in the microgrid [11-14]. At this stage, the micro-grid is becoming more intelligent and information-oriented, but the information security protection mechanism of the MGCC is relatively lacking, and it does not have the function of tolerance to faults. Therefore, if the MGCC is subjected to external malicious attacks during the operation of the microgrid [15-17], it may cause the the MGCC to be blocked in the network, communication resources are occupied, and interactive information is tampered with, resulting in equipment failures and then lead to wrong instructions. Attackers can also use the MGCC as a springboard to gradually invade the upper-layer energy management system and upper-layer dispatch center, thereby threatening the safe and stable operation of the entire microgrid system.

Early attack detection was mainly based on methods of expert systems, pattern matching, and statistical analysis [18-20]. The attack detection method based on pattern matching has simple algorithm and high accuracy, but it cannot detect unknown attacks; the expert system-based attack detection method depends on the experience of experts and the completeness of the attack library; attack detection based on statistical analysis depends on the setting of the threshold, but also gives the intruder a chance to slowly adapt to the threshold. However, with the development of high-speed networks and advances in attack methods, traditional methods have the disadvantages of high false positive rates, failure to detect unknown attack behaviors, and occupying too many resources. In addition, most of the existing attack detection methods are based on theoretical and model research, and few have considered the possibility of applying it to specific and complex power system operating conditions, such as a MGCC. In this paper, an artificial intelligence algorithm-based convolutional neural network [21-24] is applied to the MGCC, and a specific attack detection model is designed. This model can realize the active control of the MGCC actively and accurately, thereby ensuring the safe and stable operation of the MGCC in the presence of network attacks.

2. Analysis of Network Attack on MGCC

Figure 1 shows a typical microgrid system structure. Each intelligent device (mainly refers to local controllers such as load controllers, energy storage BMS, environmental monitoring devices, smart circuit breakers, smart meters, and other local controllers that interact with the MGCC for information interaction, as well as upper-level monitoring and energy management systems dispatch center) establish communication with the MGCC through communication. The connection between local controllers such as lower-level loads and micro-source controllers and the MGCC: local controllers such as each load controller and micro-source controller upload real-time operating status information such as power according to the local load and micro-source operating status, the MGCC calculates and analyzes according to the information uploaded by each load and microsource controller, and issues the corresponding microsource output power and load-matching instructions. The connection between the MGCC and the upper-level control system: The MGCC needs to receive instructions issued by the upper-level management system and the dispatching center, such as the power distribution curve issued by the energy management system, and upload all kinds of data required by the upper monitoring and management system.
In the context of high intelligence and informationization, the safe and stable operation of the microgrid depends on the stable communication and coordination of the various devices in the system. However, traditional MGCC may have security vulnerabilities. Attackers often use these known vulnerabilities to penetrate and gain root authority of the MGCC to control or destroy it. For example, an attacker can issue a DoS attack through the MGCC, making the MGCC unable to provide normal communication services; the attacker can embed trojan virus in the MGCC, monitor the MGCC, identify the received data, and carry out specific operations on the target; an attacker can steal and tamper with the network data of the MGCC and the log data, resulting in a series of abnormal events; attackers can also use the MGCC as a springboard to use the connectivity of the network and communications to gradually invade the upper-layer energy management system and dispatch center, thus threatening the stable operation of the entire microgrid system.

Therefore, in order to realize the MGCC to actively identify attacks in the above-mentioned different situations, and to ensure its safe and reliable operation, an attack detection method of MGCC based on convolutional neural networks is proposed.

3. Attack Detection Method of the MGCC Based on Convolutional Neural Network

3.1. Principle of Convolutional Neural Network Attack Detection

The principle of attack detection based on convolutional neural network is shown in Figure 2. The convolutional neural network structure consists of an input layer, a processing layer, and an output layer. The processing layer includes a convolution layer, a pooling layer, and a fully connected layer. Convolutional neural networks with different structures have different numbers of convolutional layers and pooling layers. The training of the convolutional neural network is divided into two stages of forward propagation and backward propagation. First, the convolution operation is performed on the input data; the output of the convolution layer is used as the input of the pooling layer to perform the pooling operation; the output of the pooling layer is passed to the fully connected layer, and the classification operation is performed to obtain the classification model. Then calculate the error between the actual output and the expected output. If the error is greater than the expected value, it enters the back-propagation stage, that is, the error is transmitted back to the network, and calculate the
errors from the fully connected layer, the pooling layer, and the convolutional layer in turn, and distribute the errors to each neuron of each layer, and each layer updates the corresponding weight and threshold according to the error.

**Figure 2.** Principle of attack detection based on convolutional neural network

When the convolutional neural network is applied to the attack detection of the MGCC, the characteristic data or influence factors that can characterize whether the MGCC is attacked are taken as the input of the convolutional neural network, and the input data passes through the layers of the neural network, and finally output the type of attack on the MGCC.

### 3.2. Design of Attack Detection Model

This paper proposes a MGCC attack detection method based on convolutional neural networks. It mainly includes the following: (1) Collecting the data stream; (2) Preprocessing the collected data stream; (3) Training the convolutional neural network, and then inputting the preprocessed data stream to the trained convolutional neural network model, convolutional neural network model detects these data in real time, and outputs classification results; (4) Intercept or forward the data stream according to the classification results; When there is an abnormal class, intercept the abnormal data, and issue corresponding alarm prompts and generate log records; When the classification results are all normal, the data stream is forwarded. The structure of the attack detection system based on convolutional neural network proposed in this paper is shown in figure 3.

**Figure 3.** Structure of attack detection system based on convolutional neural network
The specific design steps of attack detection model for the MGCC based on convolutional neural network are as follows:

Step 1: Collect data flow. The input data of attack detection model of the MGCC based on convolutional neural network includes the received data and sent data of the MGCC, including the received information from the lower layer and upper layer and the information sent by the MGCC to the lower layer and upper layer. For example, the voltage, current, frequency, active power, reactive power and power factor data of the public connection point, the opening and closing information of the opening and closing state of the public connection point switch and the load switching switch, as well as the command signals used to output and control the opening and closing of the public connection point switch and the load switching switch, the power distribution curve from the upper controller, as well as the remote adjustment, remote control and start stop command, load power curve from the lower layer, microsource output power, operation status information, environmental and meteorological data, and other data or factors that can characterize whether the MGCC is attacked;

Step 2: Preprocess the collected data stream. Including missing value filling and numerical processing for data flow; the acquired data has missing value, which is divided into numerical variable and character variable. When missing numerical variable, linear interpolation method is used to complete it:

$$\frac{y-y_0}{y_1-y_0} = \frac{x-x_0}{x_1-x_0}$$

Where $y$ is the missing value, $y_0$ and $y_1$ are the values of the previous sample and the latter sample corresponding to the missing value $y$, and $x_0$ and $x_1$ are the number of rows where $y_0$ and $y_1$ are located. When the character type variable is missing, the character type value that appears the most times in the data stream is used for completion. Numerical processing is to digitize the character variables in the data stream.

Step 3: First, train the convolutional neural network. The samples for training include positive and negative samples of the above data flow, positive samples represent normal received and sent data, and negative samples are attacked received and sent data; The training process of convolutional neural network is divided into forward propagation stage and reverse propagation stage, and the training process is shown in figure 4. The detailed training steps are as follows:

S1: Using uniform distribution function as probability distribution function, the weights, thresholds and learning rate of convolution neural network are initialized randomly;

S2: Select a sample randomly from the training sample as the input of the network, and set the expected value of the expected output;

S3: Samples are propagated forward through convolution layer, pooling layer and full connection layer, and the actual output of convolution layer, pooling layer and output layer is calculated;

S4: Calculate the error between the actual output and the expected output with the log likelihood loss function, and judge whether the error meets the preset expected value, which is 0.02; if yes, go to step S7; otherwise, go to step S5;

S5: Calculate the error term of the output layer:

$$\delta^L = \frac{\partial J(W,b,x,y)}{\partial z^L}$$

Where $J$ is the log-likelihood loss function, which $z^L$ is the inactive linear vector of the output layer; $W$ and $b$ are the output layer weight and threshold respectively; $x$ and $y$ are the input and output of the sample;

S6: Calculate the error of the fully connected layer in the network:

$$\delta^j = (W^{j+1})^T \delta^{j+1} \odot \sigma'(z^j)$$
Where $W^{l+1}$ is the weight of the $l+1$ layer; $\delta^{l+1}$ is the error of the $l+1$ layer; $\otimes$ is the Hadamard product; $\sigma'(z^l)$ is the partial derivative of the activation function to the inactive linear vector; $z^L$ is the inactive linear vector of the output layer; $T$ means transpose.

Convolutional layer error:

$$\delta^{l} = \delta^{l+1} \ast \text{rot180}(W^{l+1}) \otimes \sigma'(z^{l})$$ (4)

Where $\text{rot180}(W^{l+1})$ means first flip $W^{l+1}$ up and down, then flip left and right.

The error of the pooling layer:

$$\delta^{l} = \text{upsample}(\delta^{l+1}) \otimes \sigma'(z^{l})$$ (5)

Where $\text{upsample}(\delta^{l+1})$ means downsampling the error $\delta^{l+1}$ of the $l+1$ layer.

Update the weights and thresholds of the fully connected layer:

$$W^{l} = W^{l} - \alpha \sum_{i=1}^{m} \delta^{l} (a^{l-1})^T$$ (6)

$$b^{l} = b^{l} - \alpha \sum_{i=1}^{m} \delta^{l}$$ (7)

Where $\alpha$ is the learning rate, $m$ is the number of training samples, $W^{l}$ and $b^{l}$ are the weights and thresholds of the fully connected layer, $\delta^{l}$ is the error of the fully connected layer, and $a^{l-1}$ is the output of layers $l-1$ of the fully connected layer;

Update the weights and thresholds of the convolutional layer:

$$W^{l} = W^{l} - \alpha \sum_{i=1}^{m} \delta^{l} * a^{l-1}$$ (8)

$$b^{l} = b^{l} - \alpha \sum_{i=1}^{m} \sum_{u,v} (\delta^{l})_{u,v}$$ (9)

Where $W^{l}$ and $b^{l}$ are the weights and thresholds of the convolutional layer, $\delta^{l}$ is the error of the convolutional layer, $a^{l-1}$ is the output of the $l-1$ layer of the convolutional layer; $\sum_{u,v} (\delta^{l})_{u,v}$ is the sum of the subterms of $\delta^{l}$, $u$ and $v$ represent the ranks respectively;

S7: Determine whether all samples have been learned, and if so, proceed to the next step; otherwise, return to S3 and continue training;

S8: After the training is finished, the connection weights of the nodes in each layer and the thresholds of the nodes in each layer are output as parameters of the convolutional neural network model to obtain a trained model.

After the neural network is trained, the preprocessed data flow is input into the trained convolutional neural network model for real-time detection and classification, and the classification results are output. The classification includes normal types and abnormal types, and the abnormal types includes DoS attack, unauthorized access attack, abnormal detection of interface port, trojan virus attack, message forgery or tampering such as running state and weather.
Step 4: Intercept or forward the data stream according to the classification result. When there are abnormal classes in the classification results, corresponding alarm prompts and log records are generated according to the classification of the data in the abnormal types; when the classification results are normal types, the data flow is forwarded.

**Figure 4.** Training flow chart of convolutional neural network

3.3. Application of Attack Detection Model

In this section, a convolutional neural network classification algorithm is implemented by adding an auxiliary CPU. The auxiliary CPU connects to the main CPU to complete the detection of the data flow of the MGCC. Figure 5 shows the hardware structure of the MGCC. It mainly includes: (1) Clock module: providing reference clock for CPU and convolutional neural network module; (2) Storage module: used to store alarm prompts, log records, control programs, voltage, current and other electrical parameter information of common connection points, public connection point switch, load switching switch, circuit breaker switch and other status information and user information in the microgrid system; (3) Power module: provides working power for CPU, communication module, display/interaction module, input acquisition module, output control module, AC acquisition module, convolution neural network module; (4) Input acquisition module: used to receive public connection point switches, load switching switches in microgrids, circuit breaker switches, etc. and sends it to the attack detection module. (5) Output control module: used to output control signals such as public connection point switches, load switching switches in microgrids, circuit breaker switches; (6) AC acquisition module: used to collect the analog electrical quantities of public connection points, micro sources, energy storage of the system and load, etc., and send them to the attack detection module after conversion from analog to digital; (7) Communication module: It is used for data interaction, receiving
or forwarding status information from lower-level smart devices, and command information from the upper-level micro-network comprehensive monitoring master station and dispatch center, data such as remote signaling, telemetry, power consumption, and remote switching, remote adjustment, start and stop commands, as well as the power distribution curve from the upper controller and the load power curve from the lower layer, as well as micro-source output power, operating status information, and environmental meteorological data; (8) Display/interaction module: used to display the alarm information sent by the processing module and the information for display. The display module can be a display screen or an indicator light, or a combination of the two to display and provide more information, so as to realize better human-computer interaction experience; (9) Processing module (CPU): used to communicate with the upper and lower layers via the communication module and send data to the convolutional neural network module;The CPU also receives alarm prompts, log records, and classification results sent by the convolutional neural network module, and generates alarm information based on the alarm prompts and sends them to the display/interaction module for display, and sends alarm prompts and log records to the upper layer through the communication module; The alarm prompt is to display a corresponding attack classification according to the classification of the data in the abnormal class, and if it is a Dos attack, the display is a Dos attack; the display may be through a display screen and/or an indicator light; when it is a display screen, displaying alarm information, and the alarm information is the type of attack by a network attack; when it is an indicator, you can set the same number of indicators as the network attack classification, and use different color light sources for corresponding display. The log record includes attack time, attack duration, attack mode, transmission protocol type corresponding to the attack, error data segmentation, start and end address information of the error data (that is, source device and target device address information), etc. (10) Convolutional neural network module (detection module): It is used to detect and classify the data sent by the input acquisition module, AC acquisition module, and CPU as a data stream in real time, and output the classification result, and intercept the data stream according to the classification result or forward. When there are abnormal classes in the classification results, corresponding alarm prompts and log records are generated according to the classification of the data in the abnormal classes, and the alarm prompts are sent to the processing module. After receiving the alarm prompt, the processing module generates alarm information according to the alarm prompt, and then displays it through the display/interaction module; when the classification results are all normal, the data stream is sent to the processing module, and the processing module forwards to the upper and/or lower layer through the communication module.

Figure 5. Hardware structure of central controller in microgrid
A typical example of a MGCC active attack detection system based on a convolutional neural network is shown in figure 6. If the MGCC is subject to a message tampering attack, the attack
detection module in the MGCC performs attack detection on the power curve, remote signal telemetry, and weather data to finally identify the type of attack.

\[ \text{Attacker} \rightarrow \text{Message Tampering Attack} \]

\[ \text{Power Curve} \rightarrow \text{Telemetry Telemetry Data} \rightarrow \text{Meteorological Data} \rightarrow \text{MGCC} \rightarrow \text{CPU} \rightarrow \text{AC Acquisition Board} \rightarrow \text{Communication Module} \rightarrow \text{Output Control Board} \rightarrow \text{Attack Detection Module Based on Convolutional Neural Network} \rightarrow \text{Attack Detection Results} \rightarrow \text{Message Tampering Attack} \]

**Figure 6.** Typical case of active attack detection system of the MGCC based on convolutional neural network

### 4. Conclusions
At present, there are security holes in the MGCC. First of all, the monitoring module of the MGCC is limited to the monitoring of the grid switch tripping and closing, current, voltage, power and frequency exceeding limits, and does not consider the monitoring of unreasonable request attacks and false information data attacks; secondly, the MGCC lacks the active attack identification module, and cannot cope with the rapidity of information attacks. In the case of communication delay, when the abnormal state information of the MGCC is uploaded to the microgrid monitoring system, the attacker has made a deeper attack on the power control device, or has gradually invaded the upper-layer system.

Therefore, aiming at the problem of weak information security management capabilities of the MGCC at this stage, a method for detecting the MGCC attacks based on convolutional neural networks is proposed, and gives a detailed design process of attack detection model of the MGCC. That is, the important data streams in the MGCC are used as the input of the convolutional neural network model, then the convolutional neural network model detects or classifies these data streams, finally, intercept the data flow with attack behavior and give a warning prompt, and forward data without attack behaviors normally.

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

[1] Gupta A, Doola S and Chatterjee K 2018 Hybrid ac-dc microgrid: Systematic evaluation of control strategies IEEE Transactions on Smart Grid 9 3830

[2] Brearley B J and Prabu R R 2017 A review on issues and approaches for microgrid protection Renewable and Sustainable Energy Reviews 67 988

[3] Banerji A, Biswas S K and Singh B 2016 Enhancing quality of power to sensitive Loads with Microgrid IEEE Transactions on Industry Applications 52 360

[4] Shafiee Q, Nasirian V, Vasquez J C, Guerrero JM and Davoudi A 2018 A multi-functional fully distributed control framework for AC microgrids IEEE Transactions on Smart Grid 9 3247

[5] Lopes J A P, Moreira C L and Madureira A G 2006 Defining control strategies for microgrids islanded operation IEEE Transactions on Power Systems 21 916

[6] Ashok A, Govindarasu M and Wang J 2017 Cyber-physical attack-resilient wide-area monitoring protection and control for the power grid Proc. IEEE 105 1389

[7] Zhang Y, Wang L, Sun W, Green R C and Alam M 2011 Distributed intrusion detection system in a multi-layer network architecture of smart grids IEEE Transactions on Smart Grid 2 796

[8] Al-Saleh M I, AbuHjeela F M and Al-Sharif Z A 2015 Investi-gating the detection capabilities of antivirus under concurrent attacks International Journal of Information Security 14 387

[9] Stamp J, McIntyre A and Ricardson B 2009 Reliability impacts from cyber attack on electric power systems IEEE Power Systems Conference and Exposition(USA:Seattle, WA) p 1

[10] Jin D, Li Z, Hannon C, Chen C, Wang J, Shahidehpour M and Lee C W 2017 Toward a cyber resilient and secure microgrid using software-defined networking IEEE Transactions on Smart Grid 8 2494

[11] Kaur A, Kaushal J and Basak P 2016 A review on microgrid central controller Renewable Sustain. Energy Rev. 55 338

[12] Mishra S, Mallesham G and Jha A N 2012 Design of controller and communication for frequency regulation of a smart microgrid IET Renew. Power Gener. 6 248

[13] Chen G and Feng E 2015 Distributed secondary control and optimal power sharing in microgrids IEEE/CAA J. Automatica Sinica 2 304

[14] Mahmoodi M, Shamsi P and Fahimi B 2015 Economic dispatch of a hybrid microgrid with distributed energy storage IEEE Transactions on Smart Grid 6 2607

[15] Sedghi H and Jonckheere E 2013 Statistical structure learning of smart grid for detection of false data injection IEEE Power & Energy Society General Meeting (Canada:Vancouver, BC, ) p 1

[16] Zhang H, Cheng P, Shi L and Chen J 2016 Optimal DoS attack scheduling in wireless networked control system IEEE Trans. Control Syst. Technol. 24 843

[17] Fang H, Xu L, Zou Y, Wang X and Choo K-K R 2018 Three-stage stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication IEEE Transactions on Vehicular Technology 67 10788

[18] Denning D E 1987 An intrusion-detection model IEEE Transactions on Software Engineering 13 222

[19] Chen Z, Zhang Y, Chen Z and Delis A 2009 A digest and pattern matching-based intrusion detection engine The Computer Journal 52 699

[20] Ye N, Emran S M, Chen Q and Vilbert S 2002 Multivariate statistical analysis of audit trails for host-based intrusion detection IEEE Trans. Comput. 51 810

[21] Nebauer C 1998 Evaluation of convolutional neural networks for visual recognition IEEE Transactions on Neural Networks 9 685

[22] Lawrence S and Member IEEE 2002 Face recognition: A convolutional neural-network approach IEEE Transactions on Neural Networks 8 98

[23] Fukushima K 1980 Neocognitron: A self-organizing neural network model for a mechanism of pattern recognition unaffected by shift in position Biological Cybernetics 36 193

[24] Lecun Y, Bottou L, Bengio Y and Haffner P 1998 Gradient-based learning applied to document recognition Proceedings of the IEEE 86 2278