On-line Detection of Malicious Activities Based on Edge Computing in Micro-grid System

Wenxin Lei¹, Aidong Xu², Haojie Lin¹, Wenjing Hou¹, Yunan Zhang², Yixin Jiang², Zhongqi Mao¹ and Hong Wen¹

¹School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China
²Electric Power Research Institute, China Southern Power Grid Co., Ltd. Guangzhou, China
Email: sunlike@uestc.edu.cn

Abstract. With the continuous deployment of smart grids, various new smart technologies applied to the power grids have emerged, and the security boundaries of the power systems have gradually blurred, so that the power security protection measures urgently need to be updated. Aiming at the smart micro-grid system based on edge computing, this paper introduces a non-intrusive load monitoring (NILM) method, combined with the advantages of edge computing, and designs an online detection mechanism for malicious activities of terminal devices. This method is dedicated to achieving device-level security assurance.

1. Introduction
In recent years, with the continuous deployment of smart power grids, new equipment in the field of intelligent devices, wireless communications and other new technologies are emerging, and gradually widely used in the construction of electric power communication networks [1]. Micro-grid, as a complete power system, can realize self-control, protection and management, which has become a research hotspot and thus an important embodiment of smart grids deployment [2]. The edge computing technology [3] of the power Internet of things is applied to smart devices near the terminal side of the smart grids. Compared with cloud computing, it brings the nearby processing of data, reduces network transmission bandwidth and response delay, and can be widely used in micro-grid system. At the same time, a high degree of intelligence brings a complex access environment, flexible and diverse access methods, a large number of smart access terminals and other features [4], which will increase the security risks of smart grids. Under this background, the support of computing resources based on the edge computing makes it possible to implement the security protection of the micro-grid system with slightly complex computing methods [5], [6]. Further, in the smart micro-grid system based on edge computing [7], due to the widespread deployment of smart meters [8], the electrical data of the equipment is easy to obtain. It is a better choice to use non-intrusive load monitoring (NILM) [9] to realize the safety protection of the micro-grid system, which reduces additional monitoring equipment costs, additional line deployment costs, and additional time costs.

In this paper, we first discuss the architecture of the smart micro-grid system based on edge computing, and then analysis the NILM method, and propose a method for detecting malicious activities in the smart micro-grid based on the NILM edge computing system.
2. System Architecture

2.1. Micro-grid System
A smart micro-grid is a small-scale, decentralized and independent power system. It is an autonomous system that can realize self-control, protection and management. It can operate with an external power grid or in isolation [10]. It is a small power distribution system that combines distributed power sources, energy storage devices, inverters, related loads and protection devices. Figure 1 is an energy storage-photovoltaic-load topology diagram. The system consists of photovoltaic units, energy storage units, general loads and important loads. The electrical energy of the terminal load is provided by photovoltaic inverters and energy storage devices. When the self-generated energy of the micro-grid cannot meet the demand, the electric power is provided by the commercial grid. The microgrid central controller collects electrical information of devices at all levels for analysis, and realizes the function of controlling the coordinated operation of the entire microgrid.

![Energy storage-photovoltaic-load topology diagram](image)

**Figure 1.** Energy storage-photovoltaic-load topology diagram.

2.2. Edge Computing Module
However, due to the high intelligence of smart micro-grids, the security risks that terminal loads may encounter include: permission attacks, data storage and encryption attacks, vulnerability threats, and remote control [11], [12]. These risks will lead to abnormal activities of the terminal's feedback data [13], allowing the micro-grid central controller to collect wrong information and then make wrong decision-making activities, causing the local or even the entire system of the micro-grid to collapse [14]. In response to this problem, we designed an edge computing module based on NILM for malicious activities detection, and placed it at the same level as the microgrid central controller shown in Figure 1. The edge computing module has the functions of online judgment and instant feedback, which helps to improve the safety performance of the entire system.

3. NILM
Non-intrusive load monitoring (NILM) is designed to monitor a circuit containing a number of devices that are individually switched on and off [15]. By analyzing the waveform of the total load [16], NILM estimated the current moment electrical energy consumption properties and other relevant statistics of a single load.

3.1. Event Detection
The sliding window is taken for event detection of the power sequence. The window power sequence $S = [P_{-N} \cdots P_1 \cdots P_{+N}]$ is taken at the power point $P_i$. $N$ is the length of the windows on both sides of $P_i$ and the total length of the sliding window is $2N+1$. When the load has the event of state change, it is manifested as the sudden activities of power, and then the power sequence appears a large fluctuation, showing a large variance value. The variance of $S$ is $S_{var}$, represents the judgment quantity of power
mutation. In order to avoid the influence of the normal fluctuation range of power when there is no event of state change, the average power of S is expressed as $S_{mean}$, and $\alpha S_{mean}$ is taken as the reference quantity. If $S_{\alpha} \gg \alpha S_{mean}$, where $\alpha$ is the threshold control coefficient, then it is judged that power mutation occurs at this time, that is, load state changes.

3.2. Feature Extraction

The Fourier series expansion was carried out by selecting the time-series samples of the current at steady-state work after the power abrupt transition point. The amplitude of each current harmonic was taken as the load characteristic and denoted as $x = (x_1, x_2, \cdots, x_n)$, among which $n$ was the number of odd harmonics with the maximum amplitude.

3.3. Load Identification

During load identification, test samples are mapped according to the mapping relationship between established load characteristics and terminal load, so as to determine the category of samples to be tested. The specific steps are as follows:

- Training set $X = \{x_1, x_2, \cdots, x_m\}$ is formed according to the characteristic samples of each load, and the corresponding power terminal type label sequence $Y = \{y_1, y_2, \cdots, y_m\}$ is the expected output. Initialize sample weight $D_1 = \{d_{i1}, d_{i2}, \cdots, d_{im}\}$, where $d_{i} = \frac{1}{m}, i = 1, 2, \cdots, m$ and $m$ are the number of load characteristic samples in the training set.

- The weak classifier $h$ with the lowest current error is selected as the $k_1$ basic classifier $H_{k}$, and the sample of misclassification is obtained by comparing the classification result $G_k = \{y_1', y_2', \cdots, y_m'\}$ of the weak classifier $H_k$ with the expected output $Y = \{y_1, y_2, \cdots, y_m\}$. The classification error of $H_k$ is $e_k = \sum_{i=1}^{m} d_i I(H_k(x_i) \neq y_i) = P(H_k(x_i) \neq y_i)$, where $k = 1, 2, \cdots, K$, $K$ is the number of weak classifiers.

- The weight coefficient of the $k_1$ weak classifier $H_k$ is denoted as $\alpha_k = \frac{1}{2} \log \frac{1-e_k}{e_k}$, and the sample weight coefficient of the $k_1$ weak classifier $D(k) = \{d_{i1}, d_{i2}, \cdots, d_{im}\}$. The weight coefficient of the sample centralization corresponding to the $k+1_{th}$ weak classifier $H_{k+1}$ updated is $d_{i+1} = \frac{d_i}{Z_k} \exp(-\alpha_i y_i H_k(x_i))$, where $Z_k$ is the normalization factor, $Z_k = \sum_{i=1}^{m} d_i \exp(-\alpha_i y_i H_k(x_i))$.

- When $K$ weak classifier training is completed, the final strong classifier $f(x) = \text{sign}(\sum_{k=1}^{K} \alpha_i H_k(x))$ is obtained.

- The load characteristic sample $x = (x_1, x_2, \cdots, x_n)$ to be tested is taken as the input. Through the trained load classifier $f(x)$, the output is $y_j$ and the specific type of terminal advice belongs to is obtained.

4. Detection

4.1. Preparation of Parameters

When we detect the state change information of the terminal device in the electrical waveform of the total power outlet and disaggregate the specific state change of the terminal device through NILM, we collect the electricity information of the terminal device. At the moment of state change, the electrical information is exported:

- The steady-state power of the terminal device is extracted and denoted as $p$. 


- Get the time consumed by the start-up process of the device, which refers to the time consumed by the power of the device from 0 to steady state, denoted as $t_{on}$.
- Extract the running time length of the terminal device, which refers to the period of stable operation, denoted as $t_{run}$.
- The electric energy consumed by the device during operation is extracted and denoted as $w$.

Prior to this, the electricity consumption information of the terminal device during normal operation has been recorded in the database, including the steady-state power of parameters recorded as $p'$, start-up time recorded as $t_{on}'$, running time recorded as $t_{run}'$, power consumption recorded as $w'$, etc.

### 4.2. Anomaly Detection

Let $\varepsilon_p$, $\varepsilon_{on}$ and $\varepsilon_w$ be the threshold control coefficient, $t_{run,min}'$ is the shortest time for a single operation of the terminal device, and $t_{run,max}'$ is the longest time for a single operation of the power terminal device. Abnormal activities judgment table show as:

**Table 1. Detection of malicious activities.**

| Parameters | Judgment formula | Threshold | Conclusion |
|------------|-----------------|-----------|------------|
| $p$        | $p \not\in (p' - \varepsilon_p p', p' + \varepsilon_p p')$ | $\varepsilon_p$ | abnormal   |
| $t_{on}$   | $t_{on} \not\in (t_{on}' - \varepsilon_{on} t_{on}' + \varepsilon_{on} t_{on}')$ | $\varepsilon_{on}$ | abnormal   |
| $t_{run}$  | $t_{run} \not\in (t_{run,min}', t_{run,max}')$ | $t_{run,min}', t_{run,max}'$ | abnormal   |
| $w$        | $w \not\in (w' - \varepsilon_w w', w' + \varepsilon_w w')$ | $\varepsilon_w$ | abnormal   |

### 5. Simulation

**Figure 2.** A schematic diagram of event detection through a sliding window.
Figure 3. Load disaggregation of simulation test.

In the following experimental simulation, we collect the historical power data of each terminal load through the edge computing device, and obtain the historical power consumption information of the terminal device load. At the same time, the total power data is collected, and the event detection is performed according to the sequence of the total power. Figure 2 is a schematic diagram of event detection through a sliding window, which can separate events from the total power. Figure 3 is an example of extracting features from the corresponding current sequence and training a classifier to act on three terminal loads. According to the total output power information, the power consumption information of the terminal load can be clearly separated. Then, based on the separated real-time load information, we compare it with our own historical indication information to obtain whether the terminal device is currently operating abnormally.

6. Acknowledgments
This work is supported by the National major R & D program (No. 2018YFB0904900, 2018YFB0904905).

7. References
[1] S. Chen et al., "Internet of Things Based Smart Grids Supported by Intelligent Edge Computing," in IEEE Access, vol. 7, pp. 74089-74102, 2019. doi: 10.1109/ACCESS.2019.2920488
[2] W. Kohn, Z. B. Zabinsky and A. Nerode, "A Micro-Grid Distributed Intelligent Control and Management System," in IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 2964-2974, Nov. 2015, doi: 10.1109/TSG.2015.2455512.
[3] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge Computing: Vision and Challenges," in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.
[4] L. Hu et al., "Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things," in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 219-228, Feb. 2018, doi: 10.1109/JIOT.2017.2778185.
[5] Y. Xie, H. Wen, B. Wu, Y. Jiang and J. Meng, "A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 7, no. 2, pp. 383-391, 1 April-June 2019, doi: 10.1109/TCC.2015.2513388.
[6] L. Hu, H. Wen, B. Wu, J. Tang and F. Pan, "Adaptive Secure Transmission for Physical Layer Security in Cooperative Wireless Networks," in IEEE Communications Letters, vol. 21, no. 3, pp. 524-527, March 2017, doi: 10.1109/LCOMM.2016.2633425.

[7] S. A. Chaudhry, H. Alhakami, A. Baz and F. Al-Turjman, "Securing Demand Response Management: A Certificate-Based Access Control in Smart Grid Edge Computing Infrastructure," in IEEE Access, vol. 8, pp. 101235-101243, 2020, doi: 10.1109/ACCESS.2020.2996093.

[8] G. R. Barai, S. Krishnan and B. Venkatesh, "Smart metering and functionalities of smart meters in smart grid - a review," 2015 IEEE Electrical Power and Energy Conference (EPEC), London, ON, 2015, pp. 138-145, doi: 10.1109/EPEC.2015.7379940.

[9] S. Drenker and A. Kader, "Nonintrusive monitoring of electric loads," in IEEE Computer Applications in Power, vol. 12, no. 4, pp. 47-51, Oct. 1999, doi: 10.1109/67.795138.

[10] Z. Zhaojun et al., "Application of micro-grid control system in smart park," in The Journal of Engineering, vol. 2019, no. 16, pp. 3116-3119, 3 2019, doi: 10.1049/joe.2018.8771.

[11] H. Wen, S. Li, X. Zhu and L. Zhou, "A framework of the PHY-layer approach to defense against security threats in cognitive radio networks," in IEEE Network, vol. 27, no. 3, pp. 34-39, May-June 2013, doi: 10.1109/MNET.2013.6523806.

[12] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," in IEEE Security & Privacy, vol. 7, no. 3, pp. 75-77, May-June 2009, doi: 10.1109/MSP.2009.76.

[13] H. Wen, Y. Wang, X. Zhu, J. Li and L. Zhou, "Physical layer assist authentication technique for smart meter system," in IET Communications, vol. 7, no. 3, pp. 189-197, 12 February 2013, doi: 10.1049/iet-com.2012.0300.

[14] N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014, doi: 10.1109/COMST.2014.2320093.

[15] P. Shenavar and E. Farjah, "Novel embedded real-time NILM for electric loads disaggregating and diagnostic," EUROCON 2007 - The International Conference on "Computer as a Tool", Warsaw, 2007, pp. 1555-1560, doi: 10.1109/EURCON.2007.4400282.

[16] F. Xie et al., "Optimized Coherent Integration-Based Radio Frequency Fingerprinting in Internet of Things," in IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3967-3977, Oct. 2018, doi: 10.1109/JIOT.2018.2871873.