Safety Protection Technology of Power Monitoring System Based on Feature Extraction Algorithm

Che Xiangbei*, Ouyang Yuhong, Kang Wenqian and Su Jing

Shenzhen Power Supply Bureau Co., Ltd. Shenzhen, Guangdong, 518000, China
E-mail: chexiangbei@163.com
**Corresponding Author*

Received 15 July 2021; Accepted 17 August 2021;
Publication 09 November 2021

Abstract

The network security protection technology of power monitoring systems is of great significance. Aiming at the power network monitoring and protection technology problem, the paper proposes an active monitoring and protection strategy based on a feature extraction algorithm. The algorithm can calculate the transfer degree of security incidents based on evidence theory. First, the paper obtains a specific state transition diagram based on the security topology of a generalized random power communication network. Then, we analyze the relationship between power system information security and engineering security based on the system's operating results and feature extraction algorithms. The experimental results demonstrate the rapid effectiveness of this method.

Keywords: Power monitoring network, evidence theory, feature extraction algorithm, security protection technology.

Distributed Generation & Alternative Energy Journal, Vol. 37_2, 311–326.
doi: 10.13052/dgaej2156-3306.37211

1 Introduction

The power monitoring system covers the entire process of "generation, transmission, transformation, distribution, and use" of electric energy from generation to use. The system mainly includes the computer network business system, basic communication system, intelligent equipment, data network, dispatching system, etc., involved in the whole process of electric energy from generation to use [1]. All links in the power system involve or include power monitoring. Therefore, once the power monitoring system receives a malicious attack, it will inevitably bring security risks to the regular operation of the power grid.

Some researchers have proposed an optimized video transmission method based on frame similarity for remote video monitoring of electric power operations. These methods improve the transmission quality of video decoding. Second, some scholars have designed a power monitoring system based on compressed sensing and wireless networks, simplifying power monitoring data to a certain extent [2]. Third, some scholars have proposed an improved page algorithm to solve efficient information interaction in the power monitoring system. Finally, some scholars have proposed a solution based on the probability and statistics model to solve the problem that the power IT monitoring software cannot abnormally warn the object characteristics.

At present, research on power monitoring is mainly focused on data interaction, video image processing, etc., while research on power monitoring network security is relatively small [3]. Based on this, we take the power monitoring network security as the research object and propose a new active detection and protection strategy for the conventional detection technology that can detect and protect multiple types of network attacks effectively. We hope to provide a valuable reference for the safe operation of the power grid.

2 Power Monitoring Network Security

As one of the critical facilities of the power industry, the power monitoring network provides the virtual network environment and network data for the regular operation of the power. Therefore, whether the power monitoring network is safe will directly affect the security and stability of the power system, which in turn affects national security and social stability [4]. The overall framework of a typical power monitoring network is shown in Figure 1.

The power monitoring network is mainly divided into two parts: (1) Production control area. This area is divided into a controlled area and a

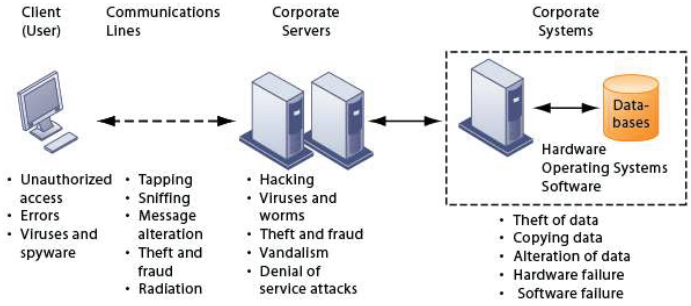

Figure 1 The overall framework of power monitoring network security.

non-controlled area. Use logical isolation between each other. (2) Management information area. This area can be divided into several business security zones according to different functional requirements. The production control area and the production control area adopt dedicated line encryption authentication and vertical encryption authentication to realize data communication. Safety isolation is adopted between the production control area and the management information area to realize information interconnection. Information protection is implemented between the management information area and the management information area through a firewall. Security protection is implemented between the management information area and the external public network through a firewall.

In Figure 1, the dispatching system uses D5000. It mainly includes three parts: the control system, man-machine terminal, and computer network system. The functional units mainly include SCADA, AGC, EDC, and network security deployment to realize the "five remote" functions. The distribution automation system realizes the "remote control," "remote measurement," "remote signaling," and "remote viewing" of the distribution automation master station and the intelligent feeder terminal through the computer system and network communication [5]. Wired optical fiber is conventionally used, and the 101/104 communication protocol has complied. The business of the management information area mainly refers to the electricity information collection system. The front server mainly adopts RS485 communication protocol or power carrier technology to realize the data collection of electric energy terminals. Data transmission from the power terminal data to the background data service area is realized through an optical fiber dedicated line, dedicated wireless network, or other methods.

At present, power monitoring network security mainly adopts special power isolation devices, security monitoring devices, network intrusion

detection, anti-virus software, firewalls, etc. [6]. This guarantees the safe operation of the power monitoring network to a certain extent. However, these measures cannot guarantee that all network attacks can be effectively protected, especially for malicious intrusion code detection, warning information protection, compound attack protection, situation assessment, etc. Therefore, further research on the security of power monitoring networks is needed.

3 Active Defense Algorithm for Compound Attacks on Power Monitoring Network

Attack detection is designed to analyze the network traffic or operating behaviors presented during network operation. We extract representative attack features and judge the security and stability of system operation [7]. Currently, network attacks against power monitoring systems mainly present composite attacks, and traditional single threat source detection methods are not sufficient to detect multiple types of composite attacks. This makes the detection results appear unitary, and the detection effect is not ideal. Because the information transmission and instruction acquisition of the power monitoring system is periodic and the business data flow is relatively fixed. This makes various security incidents caused by cyber attacks on power monitoring systems have a certain periodicity. As a result, security events have a specific correlation with each other.

Conventional attack detection methods for power monitoring systems are mainly based on two methods: network traffic detection and protocol analysis detection. These two methods can effectively detect a single source of network attacks but only consider a single security factor without considering multiple security factors for compound attacks [8]. This is not effective in dealing with multiple types of network attacks with frequent activities.

Based on this, we propose an improved active defense strategy for compound attacks based on D-S evidence theory [9]. The method integrates and detects the correlation between network security accidents of the power monitoring system and realizes the active detection and protection of compound attacks.

3.1 D-S Evidence Theory

D-S evidence theory is a conventional multi-source data fusion algorithm based on Bayesian inference. This method is mainly used in network security situation fusion, target positioning, and so on. The basic steps are as follows:

3.1.1 Define identification framework Θ

$$\Theta = \{A_1, A_2, \ldots, A_n\} \tag{1}$$

The formula A_i represents the proposition in the identification frame Θ. Each proposition corresponds to a probability. Thus, we get that the probability distribution function ($mass$ function) satisfies $m(\varphi) = 0, \sum_{A \subset \Theta} m(A) = 1$.

3.1.2 Forming a combination rule

If each proposition of the identification framework is orthogonal, the orthogonal sum of the mass function can be calculated:

$$\begin{aligned} m(A) &= m_1(A) \oplus m_2(A) \oplus \cdots \oplus m_n(A) \\ &= \frac{1}{1-K} \sum_{\cap A_i = A} \prod_{1 \le j \le n} m_j(A_i) \end{aligned} \tag{2}$$

Where K is the normalization factor.

$$K = \sum_{\cap A_i = \emptyset} \prod_{1 \le j \le n} m_j(A_i) \tag{3}$$

3.1.3 Calculating likelihood function and trust function

Each proposition may obtain multiple mass functions under different discriminators or different samples. Then the likelihood function and trust function are:

$$Pl(A) = \sum_{B \cap A = \emptyset} m(B) \tag{4}$$

$$Bel(A) = \sum_{B \subset A} m(B) \tag{5}$$

Equation (4) expresses that the likelihood function is the orthogonal sum of the $mass$ function of a particular proposition and the intersection of multiple propositions. Equation (5) represents the orthogonal sum of multiple $mass$ functions for a specific proposition of the trust function.

Equation (4) is based on the trust function and likelihood function obtained in step (3). This formula determines the upper limit and lower limit of the trust degree of each proposition in the identification framework. In combination with the discriminator, we can get the final judgment result.

3.2 Improvement of D-S Evidence Theory

The core ideas of active detection of power monitoring network attacks based on traditional D-S evidence theory are as follows: (1) The article extracts several security events that characterize the power monitoring network security as feature quantities. (2) We define each type of network attack as a proposition of the identification framework. The security events corresponding to each type of cyber attack constitute evidence to form an identification framework. (3) According to statistical theory, we obtain the mathematical mapping relationship between each network attack and historical security event and set the mass function based on this relationship. (4) Calculate the trust function and the likelihood function to get the upper limit of the trust degree and the lower limit of the trust degree. (5) Combine the discriminator to get the judgment result. Because each piece of evidence has the same weight on the judgment result, the traditional D-S evidence theory cannot effectively distinguish between different security incidents on the judgment result [10]. This affects the discrimination accuracy. In addition, when different network attacks coincide, the related security events may be aliased. This is prone to discriminative ambiguity and conflicts of evidence. Therefore, the article proposes an improvement plan based on the traditional D-S evidence theory. The specific process is shown in Figure 2.

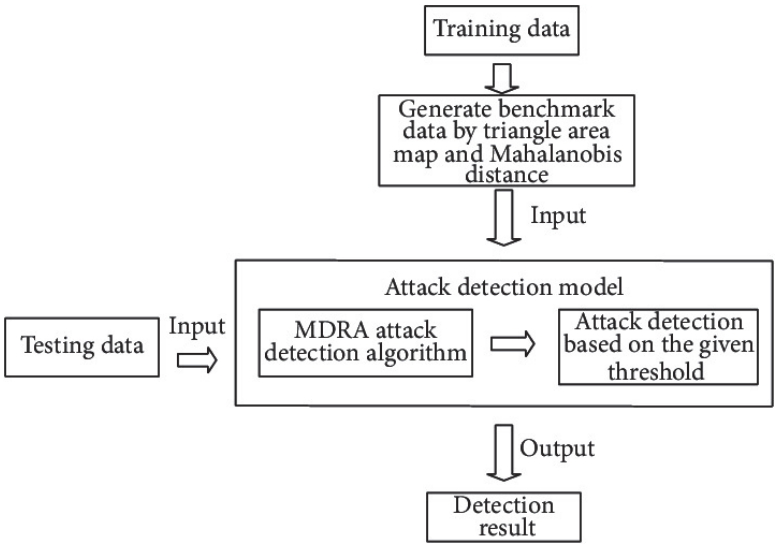

Figure 2 Power monitoring network security compound attack detection process.

In summary, the linear weighting improvement idea based on the deviation value can judge whether the operating state caused by a single attack source is a normal state or an abnormal state according to the magnitude of the deviation value. This can effectively judge the running status and facilitate decision-makers to make different coping strategies based on the deviation results.

3.2.1 Improvement 1

The standard security events corresponding to the regular operation of the power monitoring system are periodic. The system monitoring workflow is fixed. Therefore, we can use regression analysis to fit the operating law of everyday security events and compare and analyze it with the attribute values of abnormal security events. We calculated the degree of deviation between the two [11]. Generally, the greater the degree of deviation, the greater the possibility that the current security event deviates from the standard security event. The greater the possibility that the current security event is an abnormal attack. Therefore, we can use a weighting method to weight the security events corresponding to the deviation degree, which can accurately characterize the impact of abnormal security events on the detection conclusion.

Definition 1:

(1) The power monitoring network security event sequence collected in a period T is $X = \{x_i, t_i | i = 1, 2, \ldots, n\}$. Where x_i, t_i represents the security event attribute value of each collection point in period T and the collection time point T, respectively. (x_i, t_i) represents the value of the security event attribute.

(2) The security event sequence of multiple periods is $D = \{X_j | j = 1, 2, \ldots, m\}$, X_j which represents the security event sequence of the j period. D represents the property value of a standard security event that changes with time in multiple sampling periods. Here, regression analysis can be used to fit it.

(3) The sequence of multiple security events co-occurring at the time t_i' in a cycle T is $X' = \{x_i', t_i' | i = 1, 2, \ldots, n\}$. Therefore, after repeated verifications, we use the local weighted linear regression analysis method to fit the attribute values of everyday security events over time.

Definition 2:

The locally weighted linear regression equation is $x = at+b$. At the sampling point t_p', the cost function $J(a, b)$ of the security event attribute value can be

obtained according to formula (6).

$$\begin{cases} J(a,b) = \sum\limits_{(x_i,t_i)\in D} \omega_i(x_i - at_i - b) \\ \\ \omega_i = \exp\left(\dfrac{|t_i - t'_p|}{-2k^2}\right) \end{cases} \tag{6}$$

The formula ω_i, k represents the weight of the security event attribute value at each time point. They satisfy the parameters of the Gaussian function of $k \sim [0,1]$. The closer to t'_p, the larger ω_i is. We use the gradient descent method to optimize the parameter a, b of $J(a,b)$. Then at G and $x'_p = at'_p + b$, we can get the deviation degree at t'_p according to Equation (7).

$$\theta = \frac{x' - x'_p}{x'_p} \tag{7}$$

If $|\theta|$ is greater than the deviation threshold θ', it indicates that the current security event is an abnormal state. Therefore, according to the above calculation results, we set different weights for security events according to the degree of deviation.

Definition 3:

$\{\theta_1, \theta_2, \ldots, \theta_n\}$ is the deviation degree corresponding to n security events, and the corresponding security event weight is $\{\omega_1, \omega_2, \ldots, \omega_n\}$.

$$\begin{cases} \theta_{\max} = \max\{|\theta_1|, |\theta_2|, \ldots, |\theta_n|\} \\ \theta_{\min} = \min\{|\theta_1|, |\theta_2|, \ldots, |\theta_n|\} \end{cases} \tag{8}$$

Through the above formula, we can calculate the maximum and minimum deviation of each security event. Then, we use equation (9) to normalize the maximum and minimum deviations.

$$\omega_i = \frac{|\theta| - \theta_{\min}}{\theta_{\max} - \theta_{\min}} + 1 \tag{9}$$

According to formula (9), we can get the value range of $[1,2]$ when the deviation is the largest. Perform weighting processing on the $mass$

function of each security event to obtain the weighted $mass$ function as $\{m'_1, m'_2, \ldots, m'_n\}$

$$m'_i(A) = m_i(A)^{\omega_i} \tag{10}$$

Then the weighted combination rule based on D-S evidence theory is:

$$\begin{aligned} m(A) &= m'_1(A) \oplus m'_2(A) \oplus \cdots \oplus m'_n(A) \\ &= \frac{1}{1-K} \sum_{\bigcap A_i = A} \prod_{1 \le j \le n} m_j(A_i)^{\omega_i} \end{aligned} \tag{11}$$

Typically, if the network attack is independent, the corresponding $mass$ function only represents one type of network attack. For example, when the trust function and the likelihood function remain unchanged, the calculation result $m(A)$ of equation (11) can represent the trust degree of the network attack A. If $\{A_i | m(A_i) > m_\varepsilon\}$ (m_ε the threshold of trust degree) is satisfied, the maximum trust degree corresponds to the type of network attack currently occurring. On the other hand, if the trust of all network attacks is less than the threshold, no network attacks have occurred.

3.2.2 Improvement 2

When multiple network attacks coincide, it is straightforward to cause aliasing of security events, which will cause conflicts of evidence and lead to wrong judgments. The conventional method of resolving conflicts of evidence is reconciliation. However, the disadvantage of this type of method is that it cannot effectively solve the conflict of compound attack evidence caused by multiple types of network attacks co-occurring. Therefore, we propose a new method for resolving conflicts of evidence [12]. The basic idea of the method based on evidence classification is as follows:

1. In the identification framework, the functional distance between two pieces of evidence is defined as:

$$\begin{cases} d(m_1, m_2) = \sqrt{\dfrac{1}{2}(\langle \vec{m}_1, \vec{m}_1 \rangle + \langle \vec{m}_2, \vec{m}_2 \rangle - 2\langle \vec{m}_1, \vec{m}_2 \rangle)} \\ \langle \vec{m}_1, \vec{m}_2 \rangle = \displaystyle\sum_{i=1}^{2^{|\Theta|}} \sum_{j=1}^{2^{|\Theta|}} m_1(A_i) m_2(A_j) \frac{|A_i \bigcap A_j|}{|A_i \bigcup A_j|} \end{cases} \tag{12}$$

2. In the formula, $\vec{m}_1, \vec{m}_2$ represents the vector of m_1, m_2 respectively.

3. According to step (1), we can calculate the distance between all the pieces of evidence. In this way, the distance matrix R is formed,

$$R = \begin{cases} d(m_1, m_1) & d(m_1, m_2) & \cdots & d(m_1, m_n) \\ d(m_2, m_1) & d(m_2, m_2) & \cdots & d(m_2, m_n) \\ \vdots & \vdots & \ddots & \vdots \\ d(m_n, m_1) & d(m_n, m_2) & \cdots & d(m_n, m_n) \end{cases} \tag{13}$$

4. Based on hierarchical clustering, we judge the pair of evidence whose distance is less than the threshold value as similar. This can be summarized into one category. Otherwise, they are classified as independent collections separately;
5. According to the method mentioned above, we calculate the distance between the re-clustered evidence sets.
6. This cycle is executed until all the evidence sets are independent and cannot be combined.

The distance D between the two sets of evidence after re-clustering is calculated using Equation (14):

$$D = \frac{\sum_{i=1}^{|M|} \sum_{j=1}^{|N|} d(m_i, m_j)}{|M| \times |N|} \tag{14}$$

In the formula, m_i, m_j respectively represents the D function of the evidence set i in the evidence set M after the deviation degree is calculated and weighted. The $mass$ function of the j evidence in the evidence set N after the deviation degree is calculated and weighted. We set the threshold as d_Θ. If the minimum value $D_{\min}$ of $mass$ is less than d_Θ, similar evidence sets are merged. Otherwise, it is not merged. Thus, it is an independent collection. In this way, the combined evidence set can be obtained, and then the security event weighting method in the improvement as mentioned above 1 can be used. Thus, we can identify the most dangerous attack possible when multiple types of network attacks exist simultaneously.

4 Experimental Results and Analysis

1. The experimental environment is the actual simulation environment of the project. We are equipped with power distribution master stations, intelligent terminals, and simulated attack sources. The simulated attack

Table 1 Security events and mass function table

	Network Throughput/ (%)	CPU Utilization Rate/ (%)	Network Connection Volume/(%)	Business Data Failure Volume/(%)	Business Data Session Volume/(%)	The Number of Identity Authentication Failures/(%) A1
A1	3	3	2	39	16	15
A2	81	7	2	10	0	0
A3	2	4	35	0	5	15
A4	10	7	50	10	0	0

source is equipped with the $Kali-Linux$ attack toolset. It can simulate various common types of network attacks. To better reflect the pros and cons of the proposed scheme, we designed a combined experiment where multiple types of cyberattacks exist at the same time and analyzed the results;

2. Starting from the stability of security events, the security events we choose mainly include: network throughput, network connection volume, CPU usage rate, business data failure volume, business data session volume, and identity authentication failure volume. Part of the network attack $mass$ function is $BufferOverflow(A_1)$, $UDPStorm(A_2), Nmapscan(A_3), Land(A_4)$. The specific data is shown in Table 1.

4.1 Single Source Cyber Attack

If only considering a single threat source to attack the power monitoring network, there is no need to distinguish evidence conflicts based on evidence classification. We only need to compare the proposed improvement 1 with the traditional D-S evidence theory.

Before the experimental verification of a single attack source, according to improvement 1, the security events corresponding to the attack type are linearly weighted based on the deviation value of the time series. We take the parameter k of the Gaussian function $= 1$. The discrimination threshold is selected as 0.15, and the standard value of the time sampling point corresponding to the security event of a single attack type is calculated. Taking the CPU utilization rate (%) as an example, the discriminating effect of improved D-S evidence theory and traditional D-S evidence theory is shown in Figure 3.

It can be seen from Figure 3 that after calculating the deviation degree of various security events of the power monitoring system, the local linear

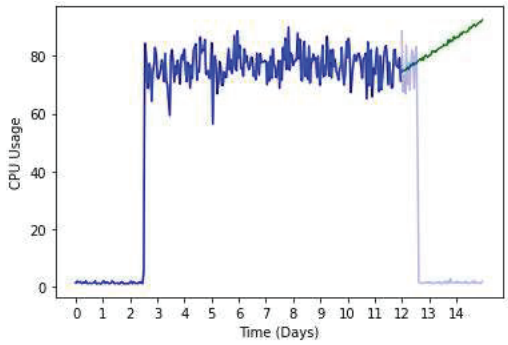

Figure 3 Regression analysis results of CPU utilization.

Table 2 Comparison of local linear fitting effects (threshold value is 0.6)

	Actual attack	A1	A2	A3	A4
Improve	A1	0.889686	0.328561	0.187562	0.005982
program	A2	0.068317	0.763295	0.397341	0.187429
trust	A3	0.004592	0.534278	0.668423	0.532916
	A4	0.196832	0.578391	0.000404	0.815329
	Discrimination result of the improvement plan	A1	A2	A3	A4
Trust in	A1	0.000397	0.203981	0.005978	0.373102
traditional	A2	0.100328	0.743985	0.665328	0.443536
solutions	A3	0.419726	0.013975	0.398561	0.510018
	A4	0.504295	0.287139	0.476482	0.855421
Discrimination result of the traditional scheme			A2	A2	A4

weighting algorithm is used to weight the fitting. The regression fitting effect is closer to the security event attribute value and has a better fitting effect. The specific data is shown in Table 2.

It can be seen from Table 2 that compared with the traditional D-S evidence theory. We proposed the improved D-S evidence theory based on deviation calculation and local linear weighting. This method has higher recognition accuracy for a single attack source, and we can obtain a sufficiently high trust value for the corresponding network attack source.

According to the experimental statistics of multiple single attack source attack results, the detection and identification of a single attack source found

that the recognition accuracy of our proposed improved scheme is 97.83%, which is much higher than the 74.92% of the traditional D-S evidence theory. This shows that the linear weighted improvement scheme based on the deviation value has a better probability function of critical safety events. This method can give a high degree of trust to the actual key network attack types.

4.2 Multiple Attack Sources Attack the Power Monitoring Network at the Same Time

Suppose multiple types of attack sources attack the power monitoring network at the same time. In that case, it is necessary to introduce clustering discrimination based on evidence classification based on the calculation of deviation degree and the improvement of local linear weighted combinations. In this way, the conflict of evidence generated by multiple types of attacks can be overcome.

Combine the four attack types $A_1 \sim A_4$ in Table 1 to form a multi-type network attack active detection for the power monitoring network. To reflect the advantages and disadvantages of the proposed improvement scheme, we choose the traditional rule-based multi-type attack protection strategy for comparison. At the same time, we choose the false positive rate (P_{wrong}), the false-negative rate (P_{miss}), and the correct rate (P_{acc}) as the evaluation indicators of the two schemes.

The experimental results show that when the types of attacks increase if the power monitoring network is attacked simultaneously, the proposed scheme's false alarm rate and the traditional rule-based scheme will increase. The reason is that the more types, the more diverse the attack methods, and the lower the accuracy of the discrimination results. In comparison, the correct rate of the proposed scheme is higher than that of the traditional rule-based scheme, and the rate of false positives and false negatives is lower than that of the traditional rule-based scheme. This shows that the proposed scheme can effectively screen multiple types of network attacks.

5 Concluding Remarks

The experimental results show that the improved network attack detection and protection scheme based on D-S evidence theory can obtain a more reasonable degree of trust. It can accurately identify a single attack source and has a high recognition accuracy rate for multiple types of attack sources.

References

[1] Nasir, V., Cool, J., & Sassani, F. Acoustic emission monitoring of sawing process: artificial intelligence approach for optimal sensory feature selection. The International Journal of Advanced Manufacturing Technology. **102(9)**, pp. 4179–4197, 2019.

[2] Liu, S., You, S., Yin, H., Lin, Z., Liu, Y., Yao, W., & Sundaresh, L. Model-free data authentication for cyber security in power systems. IEEE Transactions on Smart Grid. **11(5)**, pp. 4565–4568, 2020.

[3] Ghadimi, N., Akbarimajd, A., Shayeghi, H., & Abedinia, O. Application of a new hybrid forecast engine with feature selection algorithm in a power system. International Journal of Ambient Energy. **40(5)**, pp. 494–503, 2019.

[4] Michau, G., Hu, Y., Palmé, T., & Fink, O. Feature learning for fault detection in high-dimensional condition monitoring signals. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. **234(1)**, pp. 104–115, 2020.

[5] Guo, W., Li, B., & Zhou, Q. An intelligent monitoring system of grinding wheel wear based on two-stage feature selection and Long Short-Term Memory network. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture. **233(13)**, pp. 2436–2446, 2019.

[6] Lai, C. F., Chien, W. C., Yang, L. T., & Qiang, W. LSTM and edge computing for big data feature recognition of industrial electrical equipment. IEEE Transactions on Industrial Informatics. **15(4)**, pp. 2469–2477, 2019.

[7] Akrivopoulos, O., Amaxilatis, D., Mavrommati, I., & Chatzigiannakis, I. Utilising fog computing for developing a person-centric heart monitoring system. Journal of Ambient Intelligence and Smart Environments. **11(3)**, pp. 237–259, 2019.

[8] Sassi, P., Tripicchio, P., & Avizzano, C. A. A smart monitoring system for automatic welding defect detection. IEEE Transactions on Industrial Electronics. **66(12)**, pp. 9641–9650, 2019.

[9] Kumar, P., & Hati, A. S. Review on machine learning algorithm based fault detection in induction motors. Archives of Computational Methods in Engineering. **28(3)**, pp. 1929–1940, 2021.

[10] Selvarajan, S., Shaik, M., Ameerjohn, S., & Kannan, S. Mining of intrusion attack in SCADA network using clustering and genetically

seeded flora-based optimal classification algorithm. IET Information Security. **14(1)**, pp. 1–11, 2020.

[11] Mohanraj, T., Shankar, S., Rajasekar, R., Deivasigamani, R., & Arunkumar, P. M. Tool condition monitoring in the milling process with vegetable based cutting fluids using vibration signatures. Materials Testing. **61(3)**, pp. 282–288, 2019.

[12] Wu, X., Han, X., & Liang, K. X. Event-based non-intrusive load identification algorithm for residential loads combined with underdetermined decomposition and characteristic filtering. IET Generation, Transmission & Distribution. **13(1)**, pp. 99–107, 2019.

Biographies

Che Xiangbei, male, born in August 1984 in Baoji, Shaanxi Province, is a postgraduate and senior engineer. His research direction is network security of power monitoring system.

Ouyang Yuhong, male, born in February 1993, from Zhangzhou, Fujian Province, bachelor degree, engineer, research direction: network security of power monitoring system.

Kang Wenqian, female, born in April 1988 in Xuzhou, Jiangsu Province, is a graduate student and engineer. Her research direction is network security of power monitoring system.

Su Jing male, born in March 1990 in Chaozhou, Guangdong Province, master degree, engineer, research direction: power monitoring system network security.