Computer Aided Research on the Physical Security of Ubiquitous Power Internet of Things Equipment

Long Tan and Chunming Wei, Kexin Zhang, Shiyu Chen
State Grid Heilongjiang Electric Power Research Institute, Harbin 150000, China

Abstract. Through the analysis of the microgrid architecture under the access of the ubiquitous power Internet of Things and the current construction of the peak shaving auxiliary service market, the feasibility, necessity and economy of the microgrid participating in the peak shaving auxiliary service market are demonstrated. The thesis makes full use of information technology such as Internet of Things technology, computers, big data analysis, distributed applications, and mobile technology. It focuses on the safety management and control of the work site of power grid enterprises, and uses intelligent monitoring terminal equipment to access, such as access control (barrier), Authorize locks, intelligent safety monitoring robots and electronic fences to supervise and control production sites and operating equipment, standardize operating procedures, and improve on-site safety management and control capabilities and terminal operating equipment real-time supervision capabilities.

Keywords: Ubiquitous Power Internet of Things, trusted and secure access, physical security, computer.

1. Introduction
With the orderly progress of the ubiquitous power Internet of Things construction process, the number of devices connected to the power distribution side will reach a massive level, and the access method will be more flexible. At the same time, many new services will be derived, such as low-voltage visualization and demand-side response. These new services are transmitted through the power distribution communication network, which puts forward higher requirements on the economy, reliability, and safety of the power distribution communication network. However, the current research on the intelligent distribution and utilization communication network for the ubiquitous power Internet of Things lacks scientific and effective guidance methods, and it is impossible to quantify the performance of the communication network. Therefore, it is necessary to study the intelligent distribution under the background of the ubiquitous power Internet of Things. Analysis method of telecommunications network.

With the continuous deepening of the construction of the ubiquitous power Internet of Things, there is a gap and incompatibility between the overall perception of the entire power grid equipment operation information and operation standardization process management and control, and the traditional safety production organization and the application of new technologies and equipment. For these problems and contradictions, we must basically start with the cultivation of advanced safety concepts and safety technology innovations, and work hard to improve the level of intrinsic safety. This article focuses on the application of new technologies and new equipment in the intelligent...
management and control of production operations from the perspective of the Industrial Internet of Things, and effectively improves the level of intrinsic safety [1].

2. Overall scheme design of safe access

The development of the full-service ubiquitous power Internet of Things and the changes in the security situation have put forward new requirements for network security, especially the security of the IoT terminal layer. In terms of the protection system, there is a problem of compatibility and adaptation between the interconnected and interactive IoT business requirements and the isolation and blocking security system. In terms of technical requirements, the current national information system level protection and related security protection requirements can be generally applied to the application, platform, and network layers, but the protection requirements at the terminal layer are still unclear. The main security requirement is reflected in the need to establish a security authentication mechanism adapted to the terminal layer of the Internet of Things.

The State Grid Corporation's management information system has established a relatively complete unified authority management system, and the user authentication method is mainly based on user names/passwords or PKI digital certificates. However, the existing identity authentication and authority management facilities cannot meet the security and practicability requirements of a large number of IoT terminal devices, which are mainly reflected in: 1) Unified authority management is only for "people" and does not cover "things"; 2) The existing security authentication mechanism based on PKI digital certificate is difficult to apply in massive heterogeneous, multi-level cascaded IoT devices on site, and the key distribution and management costs are high. Therefore, it is necessary to establish a security authentication mechanism suitable for full-service ubiquitous power Internet of Things terminal equipment to solve the "who am I" problem when a large number of Internet of Things terminals interact with upper-level IoT agents and IoT platforms, and prevent illegal terminal access. And related network security incidents can be traced.

This article mainly studies the access authentication technology of the full-service ubiquitous power Internet of Things terminal layer equipment. The research mainly includes the following three parts: 1) Device discovery and identification technology for heterogeneous terminals of the power Internet of Things; 2) Internet of Things platform, edge The security transmission mechanism of identity information between IoT agents and multi-layer cascaded terminals; 3) Access authentication and key management technology for full-service ubiquitous power IoT terminal layer equipment. Figure 1 shows the implementation route of the trusted and secure access scheme [2].
3. Abnormal analysis technology of terminal layer business traffic

Aiming at the abnormal analysis of the business flow at the terminal layer of the power Internet of Things, this article establishes the network flow order based on the basic attributes of the network flow, and fully describes the external characteristics of the network flow. Based on the network flow order, deep learning methods are used to realize the self-learning of anomaly detection features, and the detection of abnormal traffic is carried out with the help of methods such as single-class classification. Because the method proposed in this paper only relies on the external characteristics of the network flow without analysing the content of the message, it can be applied to the anomaly detection of encrypted traffic [3]. The specific technical route is shown in Figure 2.
3.1. Queuing theory model of information collection business

The business data of intelligent power distribution and consumption information collection oriented to the ubiquitous power Internet of Things is uploaded to the power distribution IoT platform through the edge IoT gateway, and the processing process is similar to the process of queuing theory. With reference to the traditional queuing theory model, using edge IoT gateways as the business section, a queuing theory model including information collection services such as low-voltage centralized reading, environmental monitoring, power distribution equipment operation status monitoring, distribution transformer monitoring, and video monitoring is established. As shown in Figure 3.

\[ \lambda \text{ and } \mu \text{ respectively represent the average arrival rate of smart power distribution information collection service data and the forwarding rate of edge IoT gateway communication nodes; } \lambda_e \text{ is the actual arrival rate of data considering the packet loss rate; } k \text{ is the maximum number of data packets buffered by the edge IoT gateway. The edge IoT gateway processes and forwards the information collection business data. The processing principle is that the data buffer is full and discarded. The forwarding principle is first-come, first-served, and the forwarding time obeys exponential distribution. Therefore, the intelligent power distribution information collection business conforms to M/M/1/ k queuing theory model [4]. According to related theories of queuing theory, in a balanced state, the forwarding rate of communication nodes and the data arrival rate should be equal, so the edge IoT gateway predicts that the communication bandwidth } B \text{ should not be less than the forwarding rate } \mu, \text{ that is, } B \geq \mu. \]

3.2. Calculation method of data arrival rate of information collection service

(1) The method of calculating the arrival rate of low-voltage collective reading data. The edge IoT gateway integrates the original concentrator function and directly accesses the user-side smart meter data. The data arrival rate \( \lambda_i \) (unit: bit/s) of low-voltage collective reading data can be expressed by equation (1).

\[ \lambda_i = B_i \times N_i \times F_i \]  

In the formula: \( B_i \) represents the data flow of the user meter, bit/s; \( N_i \) represents the number of user meters connected to a single power distribution room (station area); \( F_i \) represents the concurrency factor of the user meter data sent to the edge IoT gateway, taking 5%.
(2) The method of calculating the arrival rate of environmental monitoring data. Environmental monitoring data collection is mainly completed with the help of various smart sensors. According to the actual requirements of the environmental monitoring of the smart power distribution room (station area), the arrival rate $\lambda_2$ of the environmental monitoring collected data can be expressed by formula (2)

$$\lambda_2 = \sum_{i=1}^{N} B_i \times N_i \times F_i$$

Where: $B_i$ represents the data flow of the i-th environmental sensor, bit/s; $N_i$ represents the number of the i-th environmental sensor in the power distribution room; $F_i$ represents the concurrency factor of all environmental sensors in the power distribution room, consider The most extreme case, that is, all sensors upload data at the same time, so $F_i$ takes 100%.

(3) The method of calculating the arrival rate of monitoring data of equipment operating status. The equipment operating state monitoring data arrival rate $\lambda_3$ can be expressed by equation (3).

$$\lambda_3 = \lambda_1 + \lambda_2 + \lambda_4 + \lambda_5$$

4. Case analysis
The maximum number of data packets cached by the edge IoT gateway $k$ is rounded down to $\lambda C_p$, refer to the general IP data packet size, the average data packet size is 512Byte, according to the bandwidth calculation method proposed in this article, according to formulas (1)-(3) Obtain the relationship between different bandwidth configurations of type I-V power distribution rooms and QoS indicators and bandwidth utilization [5]. Among them, $C_T$ is 1s and $C_{loss}$ is 0.1%. The results are shown in Figure 4-Figure 5.

![Image of Figure 4](image-url)

**Figure 4.** The relationship between queuing delay and predicted bandwidth
Figure 5. The relationship curve between packet loss rate and predicted bandwidth

From Figures 4 and 5, the following conclusions can be drawn: (1) The packet loss rate index is the main factor that affects the bandwidth utilization of the information collection service of various types of intelligent power distribution rooms. When the packet loss rate is set to meet the maximum constraint value of the information collection service, that is, at 10^{-3}, the bandwidth utilization of each type of intelligent power distribution room is the largest, and the optimal predicted bandwidth value can be obtained. The optimal predicted bandwidth values of the I - V intelligent power distribution room are 8.658, 7.705, 4.281, 4.172, 3.831 Mbit/s, and the bandwidth utilization rates are 82.3%, 83.4%, 81.9%, 81.7%, and 82.7% respectively. The extensions are 0.037, 0.030, 0.022, 0.021, 0.020s, respectively.

(2) The service queuing delay and packet loss rate decrease rapidly as the bandwidth of the edge IoT gateway increases, and the packet loss rate decreases faster than the queuing delay. The service QoS indicators can be controlled by adjusting the bandwidth configuration of the edge IoT gateway, but the bandwidth utilization will decrease as the bandwidth of the edge IoT gateway increases, resulting in a waste of communication resources [6].

(3) The queuing delay and optimal predicted bandwidth of various types of intelligent power distribution room information collection services are related to the actual configuration of the power distribution room. The better the predicted bandwidth value is, the larger the packet loss rate and bandwidth utilization rate and the actual configuration of the intelligent power distribution room are not obvious [7].

(4) All types of smart power distribution rooms have critical bandwidths. When the bandwidth configuration is lower than the critical bandwidth value, the QoS indicators of the information collection services of smart power distribution rooms cannot be met.

5. Conclusion
For terminal service traffic monitoring, this paper selects effective basic network traffic attributes, and through Fourier transform, normalization and other processing on the basic attributes, forms a uniform length network flow order vector for different traffic, which is the subsequent abnormal network traffic Lay the foundation for testing. In order to obtain effective anomaly detection features, this paper further optimizes the network flow order vector to improve the detection effect. For the plaintext traffic generated by the terminal, the abnormal monitoring of the service agreement can be continued. At the protocol grammar level, aiming at network malformed messages, a parallel parsing method of messages is implemented to improve the speed of message parsing. At the level of protocol semantics, anomaly detection based on business protocol modelling is implemented, which can effectively detect abnormal protocol instructions. Finally, combining the results of business traffic anomaly analysis and business protocol analysis, comprehensively considering the abnormal characteristics of the physical
layer, network layer, and protocol layer of the terminal device, a portrait of the terminal device is established, and the network access status of the terminal device is described. Based on device portraits, combined with specific attack scenarios, counterfeit and malicious terminal devices can be accurately identified, and the goal of security monitoring for heterogeneous full-service ubiquitous power IoT terminals can be achieved.

Acknowledgments
This work was supported by Science and Technology Project of SGCC (Research on Low-temperature Resistance Characteristics and Evaluation Technology of New Sensors for Power Transmission and Transformation).

References
[1] Wang, W. C., Zhao, C., & Gupta, P. Assessing layout density benefits of vertical channel devices., 37 (12) (2018) 3211-3215.
[2] Zhou, J., Huang, J., Li, P., & Li, N. Hybrid modelling of microwave devices using multi-kernel support vector regression with prior knowledge. International Journal of RF and Microwave Computer-Aided Engineering, 25 (3) (2015) 219-228.
[3] Couceiro, M. S., Fernandes, A., Rocha, R. P., & Ferreira, N. M. F. Understanding the communication complexity of the robotic darwinian pso. Robotica, 33(1) (2015) 157-180.
[4] Choi, K., Lim, S. H., & Kim, J. H. Cost-effective monitoring algorithm for cyber-physical system platform using combined spatio-temporal model. Journal of Supercomputing, 74(8) (2018) 3537-3548.
[5] Zheng, B., Deng, P., Anguluri, R., Zhu, Q., & Pasqualetti, F. Cross-layer codesign for secure cyber-physical systems. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 35(5) (2016) 699-711.
[6] Ahmed El Shafie†, Ahmed Sultan*, & Naofal Al-Dhahir†. Physical-layer security of a buffer-aided full-duplex relaying system. IEEE Communications Letters, 20(9) (2016) 1856-1859.
[7] Oh, M. K., Lee, S., Kang, Y., & Choi, D. Wireless transceiver aided run-time secret key extraction for iot device security. IEEE Transactions on Consumer Electronics, 66(1) (2020) 11-21.