Mobile job security protection under the ubiquitous power Internet of Things

Chi Feng1*, Yuan Fang2, Liang Zhang2, Junhao Yu2, Jianqiao Sheng2, Lisha Wu1 and Shan Chen1

1 State Grid Anqing Power Supply Company, Anqing City, Anhui Province, 246000, China
2 State Grid Anhui Electric Power Co., Ltd. Hefei City, Anhui Province, 230000, China
*Corresponding author’s e-mail: fchi@163.com

Abstract. The rapid development of the new generation of information intelligence technology is closely related to people's life, work and other social activities. The ubiquitous power Internet of Things is a complex multi-network flow system, with the power system as the core, composed of communication network, cloud platform technology, intelligent terminal sensor and artificial intelligence; characteristics are open sharing, ubiquitous connection, holographic perception, fusion innovation. With the development of the energy Internet, the power system is required to fully perceive and widely interconnect massive data and propose the concept, which will become a new idea for the development of information sharing networks in the field of energy Internet power. New mode. Mobile intelligent terminals are important access devices for ubiquitous power Internet of Things and play an important role in mobile operations; mobile smart terminals face more security risks. In the context of ubiquitous power Internet of Things, it is of great significance to analyze the problems existing in the security protection of mobile intelligent terminals and explore the security protection technology of mobile intelligent terminals.

1. Introduction

With the development of production and the progress of society, the demand for electricity has been greatly increased, which has enabled the power industry to rapidly expand the scale of AC and DC transmission. Due to the rapid increase in the number of distributed power generation equipment and access types, the grid structure is more complicated, making the tradition the grid form facing severe challenges [1]. The maturity of 5G networks, the development of high-performance processors and smart sensors have made the application of artificial intelligence in various fields a reality [2]. At present, in the development planning of the State Grid, the construction of ubiquitous power Internet of Things is the most important task and the most urgent task. Some research and analysis results show that there are many similarities between ubiquitous power Internet of Things and integrated energy systems. Under the current circumstances, it is necessary to use data as the driving force for innovation of energy business model and explore effective strategies for realizing massive data interconnection and interconnection of power systems.

2. Ubiquitous power Internet of Things and basic architecture

2.1. Ubiquitous power internet
Ubiquitous IoT mainly refers to the interconnection of information without the influence of time, place, and characters. The ubiquitous power Internet of Things is the application of Internet of Things technology in power systems, mainly involving information interconnection between power generation enterprises, power supply enterprises, suppliers, and their respective power equipment.

2.2. The basic characteristics of ubiquitous power Internet of Things

Based on the existing power network system entities, combined with modern network communication technologies, the ubiquitous power Internet of Things combines different energy systems with physical interconnection, commerce, and spatio-temporal information interconnection, presenting open sharing, ubiquitous connectivity, holographic awareness, and fusion innovation. Open sharing is mainly reflected in data sharing, unified data platform, intelligent technology sharing and management of data, ensuring the continuity and real-time interaction of data information, so as to be able to mine effective information. A ubiquitous connection is a full-time connection that implements devices and information. A mobile network or a power private network is used as a connection medium to connect all power devices, user information, and data.

Terminal ubiquitous access. In the ubiquitous power Internet of Things, fully compatible sensing devices are deployed in all aspects of the power system, and various types of application terminal devices can be flexibly connected to the system, enabling real-time power production, transmission, and utilization of various types of data; The interaction requirements of various network resources can be satisfied through the ubiquitous communication network to achieve ubiquitous connectivity; the ubiquitous power communication network has multiple levels such as ground coverage, satellite and wireless.

2.3. The basic structure of the ubiquitous power Internet of Things

From the basic composition structure, the ubiquitous power Internet of Things can be divided into four levels, as shown in Figure 1.

![Fig. 1 Technical architecture of the UPIoT](image)

Fig. 1 Technical architecture of the UPIoT

The sensing layer is composed of a sensor and a terminal device. The sensor is a high-precision, micro-intelligent sensor that collects data of various links of power generation, transmission, power transformation, power distribution, and power consumption, and enhances intelligentization of each terminal through edge calculation. The main structure of the sensing layer is shown in Figure 2.

![Figure 2 The main components of the perception layer](image)
The platform layer utilizes the data center and the IoT management center to improve data processing and cloud collaboration capabilities. Mainly provide big data services, including business modeling, data storage and data publishing; Internet of Things services, including information model and device management; resource scheduling and operation; cloud intermediate services and application infrastructure services; full-service data centers. The infrastructure mainly includes a cloud computing resource pool, a cloud storage resource pool, and a network resource pool. The main structure of the platform layer is shown in Figure 3.

![Figure 3 The main components of the platform layer](image)

The main task of the application layer is to promote the safe and stable operation of the power grid and build a smart integrated energy Internet. The services provided mainly include status monitoring, operation and maintenance, fault repair, power trading, data mining and panoramic display. The application layer interacts with the intelligent resource integrated service platform. The service content and organization of the application layer are shown in Figure 4 below.

![Figure 4 Service structure of the application layer](image)

The application of ubiquitous power Internet of Things is divided into three parts, and the following three tasks are completed: ensuring the safe and economic operation of the power grid, building a smart energy integrated service platform, and opening up the power market and building an energy ecosystem. Data sharing is the basis of the ubiquitous power IoT architecture. The communication network runs through the entire ubiquitous power Internet of Things architecture. Intelligent defense and secure interactive IoT security technologies provide an important guarantee for the safe and stable operation of the entire system.

3. **Security Analysis of Ubiquitous Internet of Things Terminals**

At present, most on-site data acquisition devices are based on traditional industrial acquisition devices, and the collected data has low precision and poor reliability, resulting in a low degree of intelligence of the terminal devices. Most of the modern miniature intelligent terminal sensors are based on smart chip design and have the advantages of miniaturization, high precision and intelligent calculation, which can effectively solve the problems existing in traditional data acquisition devices; The
difference is that the intelligent terminal sensor can collect, extract and transmit device information. At the same time, through local edge calculation, the terminal is intelligent and achieves the effect of local self-control.

The ubiquitous power Internet of Things is a manifestation and special category of the Internet of Things. Its application scenarios are complex. Compared with traditional terminals, the smart terminal devices are diversified and there is a big difference between the two. In industrial production, there are many scenes that can be used in the ubiquitous power Internet of Things, and its operation and maintenance features are also obvious. The ubiquitous power IoT terminal security factor includes traditional IT security and operation and maintenance security; the ubiquitous power Internet of Things security protection also adheres to the basic principles of reliability, privacy and recoverability, and the security protection architecture has end-to-end And based on the "pre-event, after-the-fact, after-the-fact" model. In the Internet of Things, due to the lack of common communication protocols, the protocol itself also has security problems, making the security problem more difficult. From the perspective of the smart terminal device itself, these devices store the relatively private information of individuals and units. Private information is easily stolen if deployed outdoors. There are more factors in the security risks of ubiquitous intelligent Internet access types and numbers.

The application of massive data in the power system is the core of the ubiquitous power Internet of Things. Openness is the characteristics of the mobile intelligent terminal operating system platform, and there are contradictions with the requirements of security. Android, the mainstream operating system on the market, has a low development threshold and has many applications. The overall quality is low and the security issues are more prominent. Currently, Web technology standards are still evolving, and there are certain loopholes in security mechanisms. Taking HTML5 as an example, it tends to have user experience and functions, resulting in security vulnerabilities. Considering the cost of product development, there is a lack of sophisticated hardware encryption and authentication mechanisms for mobile terminal devices. Because the hardware encryption chip is used to encrypt all operating system files, the iPhone is more secure than the Android device, but the cost of the terminal device is relatively high.

The security risks of mobile intelligent terminals ubiquitous in the power Internet of Things, in addition to the terminal itself, when the mobile terminal performs network connection, the network link, and the access server manages the mobile terminal, there are various security risks. Mobile terminal devices have a greater security impact on the ubiquitous power Internet of Things. Viruses are transmitted through e-mail, and terminal devices are lost or stolen, which will bring greater security risks.

4. Network security protection technology under the Internet of Things

5G communication technology promotes the development of ubiquitous power Internet of Things. 5G performance enhancement technology can enable ubiquitous power Internet of Things to meet the needs of grid business. 5G softening and open technology can help manage ubiquitous power Internet of Things and make power grid Actively and freely control communications; 5G autonomous optimization technology enables ubiquitous power Internet of Things to target grid users and achieve new user-centric services. The ubiquitous power Internet of Things integrates power networks and communication networks to make scheduling management more convenient and faster.

4.1. 5G access network security technology

5G supports wireless and wired access networks, mainly based on wireless access networks. Due to the openness of the wireless environment, the security of the 5G access network has an impact on the entire mobile network. The 5G mobile network pays more attention to privacy protection, signaling security and user data security, and designs an enhanced security protection scheme.

In terms of privacy security, the user needs to pass the permanent user ID in plain text for the initial access. For this security problem, the 5G mobile network adopts asymmetric encryption technology to protect the permanent user identity. The operator, by presetting the relevant information such as the
home network public key, enables the user terminal to encrypt and protect the permanent user identity by using the home network public key. In the 5G communication protocol standard, it is clearly stated that in the registration and service initiation process, the 5G mobile network must refresh the temporary user identity.

In terms of signaling protection, the mobile network sends the initial signaling in plaintext when the terminal initiates a service from the idle state to the network. There are various types of security risks associated with information transmitted in an open wireless environment. In the 5G mobile network, the initial signaling mechanism of encrypted transmission is designed, and only the plaintext is allowed to transmit information related to establishing a secure connection. All other information is encrypted and transmitted, and the security key negotiated based on the current or previous security establishment process is utilized. In the ubiquitous power Internet of Things, there are many types of IoT terminals, and the number is huge. User data protection needs to be customized as needed. The 5G mobile network supports secure encryption on the user side as needed to ensure the security of the wireless network.

4.2. Mobile terminal intelligent protection measures

The application layer security protection of the ubiquitous power Internet of Things is mainly for user services and mobile applications, focusing on data security, intelligent defense and security linkage. The protection technology for intelligent terminals mainly involves the following aspects:

In terms of data security protection, the use of data classification authorization and anti-leakage technology is strengthened to strengthen the management of the data security life cycle.

In terms of safety linkage handling, the construction of emergency command and early warning capabilities will be strengthened, and the linkage capacity of safety equipment will be improved to ensure application safety.

In terms of intelligent defense, we will strengthen the research on large-scale verification technology for the security risks of the Internet of Things and improve the intelligence level of security defense.

4.3. Terminal identity authentication technology

In the ubiquitous power Internet of Things, each IoT terminal is assigned a unique identifier, and each terminal has its own certificate key. The identity authentication technology is for the mass IoT terminal identification and certificate binding and correspondence. At present, in most power grid enterprises, public key infrastructure (PKI) technology is used for identity authentication. However, PKI needs to run a certificate directory online, and it is impossible to generate a public key on a large scale, which makes it difficult to implement a large-scale application. Combined public key cryptography (CPK) is based on the authentication mechanism of the identity, based on the new key management algorithm and mapping technology, enabling scaled applications.

Due to the large scale of the ubiquitous power Internet of Things, identity authentication is greatly restricted, which has an impact on the efficiency of power grid operations. The combination-based public key cryptography is more suitable for mutual trust authentication in the ubiquitous power Internet of Things environment.

4.4. Terminal behavior analysis

The ubiquitous Internet of Things terminal equipment is widely distributed, large in number, and difficult to protect. There is a risk of leaking sensitive data of users, which has an impact on the normal production and operation of enterprises. Therefore, it is necessary to solve the ubiquitous IoT terminal security and access authentication. Security issues such as monitoring and analysis. At present, the company's secure access and unified rights management system is mainly for intelligent terminal access and human-machine authentication, and the object-material mutual trust problem of the Internet of Things cannot be completely covered.
The Internet of Things terminal behaviour analysis technology can discover all the devices in the Internet of Things, and implement secure access control and fault monitoring for the devices. On the basis of machine learning, behaviour analysis technology can automatically carry out learning analysis; based on behaviour analysis, using mathematical model to automatically establish a white list of network access relationships, to help users fully understand network behaviour and extract illegal behaviour; using behaviour analysis technology, the attack activity identifies and discovers hidden attackers; analysis network traffic and behaviours, automatically aggregates abstract massive network access relationships, and combines known device information to automatically determine the network behaviour of terminal devices to avoid violations and harmful behaviours.

5. Conclusion
The security protection of mobile operating terminals that are ubiquitous in the power Internet of Things is of great significance to the safe operation of power systems, and can improve the network security protection capabilities of power grid enterprises as a whole. For the security protection of intelligent operation terminals, through the security chip and key technical defense measures, the security management and control capabilities of the IOT terminal are improved, the unified identity security control of the IOT terminal is realized, and the identity security mark and verification problem are solved. Through the introduction of new technologies, the security of the power Internet of Things is improved, and comprehensive ubiquitous security measures are used to timely discover and quickly resolve ubiquitous power Internet of Things issues, effectively ensuring network security of power grid enterprises.

References
[1] Zhu Yongli, Shi Xin, Wang Liuwang. An introduction to the recent research hotspots of artificial intelligence in power systems[J]. Power Generation Technology, 2018, 39(3): 204-212.
[2] Rifkin J. The third industrial revolution: how lateral power is transforming energy, the economy, and the world[M]. New York: Palgrave Mac Millan, 2011.
[3] Hongbin S, Qinglai G, Boming Z, et al. Integrated energy management system: concept, design, and demonstration in China[J]. IEEE Electrification Magazine, 2018, 6(2): 42-50
[4] Wang D, Liu L, Jia H J, et al. Review of key problems related to integrated energy distribution systems [J]. CSEE Journal of Power and Energy Systems, 2018, 4(2): 130-145.
[5] Dai L, Gao X, Wang Z. Energy-efficient hybrid precoding based on successive interference cancelation for millimeter-wave massive MIMO systems[C]// 2015 IEEE Radio and Antenna Days of the Indian Ocean(RADIO). Mauritius: IEEE, 2015: 1-2.
[6] Liu Yunhao. Introduction to the Internet of Things [M]. Beijing: Science Press, 2013: 5.
[7] Kang Chongqing, Liu Jingkun, Zhang Ning. A new form of energy storagein future power system: cloud energy storage[J]. Automation of Electric Power Systems, 2017, 41(21): 2-8, 16(in Chinese).