Research on Security Control Scheme of Power Distribution Internet of Things

Ranxin Gao, Yue Sun*, Min Li
State Grid Jibei Electric Power Co. Ltd. Research Institute, North China Electric Power Research Institute Co. Ltd., Beijing, China
*Corresponding author: Yue Sun e-mail: sun.yue.d@jibei.sgcc.com.cn

Abstract. With the rapid development of the Internet, the process of Power Distribution Internet of Things has been pushed continuously. At present, the number of IoT terminals has increased sharply, and the types are also diverse. Meanwhile, the requirements for the communication timeliness and transmission safety between distribution networks are increasing. The current traditional distribution network structure is unable to properly manage the new terminals. As an emerging technology for information security protection, trusted computing can guarantee a safe and reliable operating environment and management mechanism in the power distribution IoT. Through the optimization of the hierarchical structure of the distribution network and the use of binary trusted security control model, we can build the hierarchical control structure model of the power distribution IoT. It makes the security level of the system has been greatly improved.

1. INTRODUCTION
At present, intelligent distribution system has ushered in great development opportunities. Especially with the diversification of user-side caused by the rapid development of Internet, the value of distribution network refinement and automation development becomes more prominent. It also promotes the further development of IoT technology, artificial intelligence technology and big data storage technology[1]. The current situation of distribution network in China has basically met the conditions of building power distribution IoT. As an important part of power grid, distribution network directly faces power users. It is closely related to production and life. It is also an important infrastructure to ensure and improve people's livelihood. Power distribution network can be perceived intuitively by users. However, in the current system, there is a wide range of points and wide business differences. Large business differences also exist in the current system. The requirements of communication timeliness and transmission security are constantly improving [2]. Therefore, if the distribution automation terminal can not control the lower layer equipment, it may lead to many problems in the power distribution IoT system, such as low control efficiency and poor security.

2. AN OVERVIEW OF RELATED TECHNOLOGIES

2.1 Power Distribution IoT
Power Distribution network has the task of monitoring, operation and control. It is a very important part of the power system, and also an important link in the development of energy transformation. At present, the power distribution network has become a node of energy production and consumption, which undertakes both energy production and energy consumption, carrying the two-way flow of...
energy. Based on the current situation of China's distribution network and the needs of energy transformation, it is an urgent and essential requirement to build a reliable power distribution Internet system. Power Distribution IoT is a new network form, which is deeply integrated by traditional industrial technology and Internet of things technology. The new system includes a large number of nodes with the functions of perception, calculation and control. Through the power distribution IoT, the interconnection and intelligent deployment of terminal equipment can be met, and the comprehensive perception, data-driven and business connection of the power distribution network can be realized. There are three major propositions of the new system: The first is the edge intelligence with distribution transformer terminal as the core; the second is multi-source data fusion supports the power grid state visibility (including data perception, data edge calculation, data efficient transmission, data fusion and data application); The third is the rapid launch of business supported by the Internet of things platform [3-4]. The new system integrates the IoT technology with the power industry technology, which can achieve the purpose of all-round interconnection of the internal equipment of the distribution network, so as to realize the comprehensive perception of the power grid, data fusion and intelligent application. In this way, the comprehensive perception, data fusion and intelligent application of power grid are realized.

2.2. Trusted computing

Trusted computing is a technology to ensure the predictability of information system, which makes the whole process of computing measurable and controllable. Different from the traditional protection methods, trusted computing firstly collects the system and application information, determines the trusted characteristics of the system and establishes the trusted policy base. According to the user's trust requirements, we determine the trusted characteristics of the system and establish the trusted policy base, and then determine the known characteristics. The behavior of non-compliance policy is marked as unknown, and the known is protected, destroyed and rejected by trusted control. Trusted computing builds a logical independent trusted computing subsystem outside the traditional system as a trusted node, and connects the trusted nodes through trusted connections to monitor the system and provide trusted support. A trusted computing system consists of trusted root, trusted hardware platform, trusted operating system and trusted application. From the root of each trust chain, each level is layer by layer authentication and trust the next level, thus building a secure and reliable computing environment. Its goal is to improve the security of the computing platform.

In this paper, faced with multiple security issues, this study combine the current structure of power distribution IoT and its development prospect. The paper studies how to improve the security of the system by strengthening the security management. Combined with trusted computing technology, the security management of power distribution IoT is realized through binary trusted network, which makes it possible to realize efficient and intelligent security management.

3. RESEARCH OBJECTIVE

With the digital transformation of power industry, the concept of IoT has been infiltrated into all aspects of power system. The addition can improve the information perception and sensitivity of all aspects of smart grid, and provide data support for intelligent power system. The new technology helps improve productivity and profitability by unleashing the data potential of distribution systems. However, with the interconnection of equipment and the integration of information technology and operation technology, network security risk also increases. Energy security is not only the sufficient energy supply in the traditional concept, but also the network security problems caused by digital transformation [5-6].

For the distribution terminal side, with the increasing demand of user, various terminal devices have more functions. The new device needs to have in-depth interaction with the power system. In the face of higher functional requirements, the information security of distribution terminal and distribution load has become very important. If the load on the power side is occupied by illegal users, it will lead to serious consequences. The separation of traditional information security to the network
environment is not conducive to the wide interconnection. The existing vertical authentication method of distribution network is mainly applied to the master-station and sub-station mode, but there is no unified management scheme for the secure access of the IoT terminal [7]. There are still many security problems in the terminal access.

4. OUR SCHEME
At present, with the rapid development of power distribution IoT, the demand of terminal access is increasing rapidly. However, there is no unified management for the terminal access process. The process of terminal access faces many security problems. The traditional hierarchical structure of distribution network is mainly the three-layer wired transmission structure and the two-layer wireless transmission structure. In order to achieve the security management of terminals, the traditional hierarchical structure of distribution network is optimized, and the hierarchical structure is redefined. The hierarchical management structure adds the first layer of the cluster in the traditional structure, and uses the self-organization characteristics to cluster management, forming a new four layer structure [8]. The four layer structure includes master station, automation terminal, IoT cluster head and IoT sensing node. Through cluster head layer, the terminals connected to the next layer terminals safely. The hierarchical structure of power distribution IoT is shown in Figure. 1.

![Hierarchical structure of power distribution IoT](image)

4.1. Trusted authentication process
In the four layer structure, there is a binary trusted security management between two layers, which forming a three-level binary trusted security management mode. The binary trusted security management uses trusted computing technology to realize the state security of each layer nodes and the trusted access of the whole network. The technology improves the security of the distribution IoT, which also meets the safe requirements with high efficiency. The four layer structure includes three levels of binary trusted process. The trusted authentication process is shown in Figure. 2:
The first level trusted process is completed by the main station layer and the automation terminal layer. On the premise that the master station is trusted in the hierarchical structure of the power distribution network of things, the trusted authentication between the master station and the distribution network automation terminal layer is carried out under the leadership of the master station, so as to ensure the safety and credibility of the distribution network automation terminal, and establish the trusted connection between the distribution network automation main control layer and the distribution network automation terminal layer.

The first level of trusted process is completed by the main station layer and the automation terminal layer. On the premise that the master station is trusted in the structure, the trusted authentication between the master station and the automation terminal layer is carried out. This process can ensure the security and credibility of the automation terminal, and establish the trusted connection between the main control layer and the automation terminal layer.

The second level of trusted process is established on the premise of the first level. The automation terminal takes over the leading function of the master station to authenticate the lower level. In this trusted process, the IoT cluster head layer is the requester, and the distribution network automation terminal is the responder. These two parties constitute the trusted authentication between the distribution network automation terminal and the cluster head. This process realizes the security of the cluster head, and establishes the second level trusted connection.

Similarly, the third level of trusted process is established on the premise of the upper level. The cluster head takes over the role of responder. The responder authenticates the underlying structure to achieve the trusted connection between the IoT cluster head and the IoT sensing node, so as to realize the trusted security management of the IoT sensing nodes.

In the four level of trusted process, the trusted authentication process is pushed forward layer by layer. The trusted connections are established level by level. The trusted connections at all levels transmit level by level, and make a trust chain.

In the process of establishing the trusted connection, each level of connection is established by two layers in the structure. These two layers are the requester and responder in binary trust.

4.2. Interaction Process
The requester of trusted network connection is the lower level unit, and the responder is the upper level equipment. The responder controls the lower layer access equipment through the trusted network. Taking four level of trusted process as an example, The sensing node layer is the connection requester, and the cluster head of the distribution IoT is the connection responder. At the same time, both the requester and the responder have the function of integrity measurement and trusted connection.
The trust building process between the requester and responder is shown in Figure. 3. Before the requester and the responder establish the network connection, they need to measure their own trusted state. The integrity module uses the hash algorithm SM3 to realize the integrity measurement and generate the trusted report. The hash algorithm SM3 is a process of filling and iteratively compressing the message \( m \) with the length of \( L \) (\( L < 264 \)) bits to generate the hash value. The output length of the hash value is 256 bits. The integrity is determined by judging the output of the hash value.

In order to achieve binary trusted management, it is necessary to establish a communication channel between the requester and the responder. Through the session key, we can ensure the confidentiality of channel data. Before the completion of binary trusted access, the communication channel should be in a limited state. It only supports the interaction of related information of the trusted connection. At this time, the requester initiates an access request to the responder. After receiving the request, the two parties conduct two-way identity authentication to verify the validity of their identity keys. The two parties can control the local port according to the result of user identification. After the two parties receive the information of successful user authentication, they start to conduct two-way trusted authentication. After the authentication is successful, the interactive integrity module generates the integrity report and implements the trusted evaluation protocol. At this time, the responder verifies the integrity report of the requester, and finally generates the trusted verification results of the two parties. Both parties will get the complete authentication and integrity verification results.

After the trust verification evaluation of both parties is completed, the responder will make decisions based on the evaluation results of the trusted platform, and determine the decision type as allow / prohibit / isolate according to the evaluation results. After the decision result is obtained, the responder sends the decision result to the requester. If the decision result is allowed, the requester completes the trusted network connection according to the received decision.

5. CONCLUSION

Our country clearly proposes to promote the transformation of traditional energy system to low-carbon, clean and efficient. From the technical characteristics, the function of power grid is to create a new generation of power system, and from the functional form, it is the transformation of traditional power grid into energy Internet. Distribution network is a very important link in the development of energy transformation. It directly faces customers and has a great impact on customer experience. The essence of the distribution IoT is the deep integration of informatization and industrialization. The productivity of the original distribution network can be further released through the power of informatization, so as to achieve a qualitative leap. The rapid development of distribution IoT also brings a series of security problems. This paper studies the hierarchical security management method of distribution IoT on binary trust, and proposes a four layer hierarchical management structure. By adding the cluster head layer, three-level binary trusted security management is carried out, which provides reliable support for the security of distribution IoT.
ACKNOWLEDGMENT

This project is supported by the Science and Technology Project of State Grid Jibei Electric Power Co. Ltd. (52018K190024).

REFERENCE

[1] Yue Sun, Jiaxuan Yang, Wei Chen, et al. Research on Typical Architecture and Application of Distribution Internet of Things Based on Blockchain. 2020, 1621(1):012095-.

[2] Siyang Shao, Xiang Ma and Wei Yuan. Research on Construction and Application of Power Distribution Internet of Things. 2020, 1634(1):012038-.

[3] Jun L, Wanxing S, Riliang L, et al. Design and Application of Power Distribution Internet of Things[J]. High Voltage Engineering, 2019.

[4] Sharma D D . The Challenges in Development of Internet of Things Based Smart Power Distribution System[C]/ IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering. 0.

[5] Yunshuo L , Jian D , Jun L , et al. Research on distribution power quality monitoring based on distribution internet of things[C]/ 2019 14th IEEE International Conference on Electronic Measurement & Instruments (ICEMI). IEEE, 2019.

[6] Jianming L , Ziyan Z , Xiang J I . Research and application of Internet of things in power transmission and distribution system[J]. Chinese Journal on Internet of Things, 2018.

[7] Lee Y S . Authentication Method for Safe Internet of Things Environments[J]. Journal of Korea Institute of Information Electronics & Communication Technology, 2015, 8(1):51-58.

[8] Sun B , Yan J , Yang Y , et al. Research on Load Distribution Planning of Power Grid Based on IoT[C]/ 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA). IEEE, 2019.