Security control of unstructured data in the power IoT for isolation network between internal and external

Ruxia Yang¹, Di Wang² and Fei Liang¹

¹State Grid Key Laboratory of Information & Network Security, Global Energy, Interconnection Research Institute Co., Ltd. Nanjing, China
²Big Data Center, State Grid of China, Beijing China

Abstract. As a key national infrastructure, the safety of the power grid is an overall and strategic issue that affects the development of the national economy and society. With the popularization and development of the Internet of Things in the power industry, power Internet of Things terminal equipment has become a key target of network attacks. Using network attacks to damage power Internet of Things equipment has a strong detrimental power. As the main data storage method of the power Internet of Things, the security management and control of unstructured data has become the focus of the power Internet of Things security. This paper proposes a reformulation of access control policies based on the different attribute states and trust levels of power Internet of Things terminal equipment to reduce its access control authority, and on this basis, proposes a dynamic access control based on the isolation of internal and external networks. The detailed function design of each core security protection component is given, and the component module is explained.

1. Introduction

As a national critical infrastructure, the security of the power grid is a global and strategic issue that affects the national economic and social development[1]. Incidents such as the Iranian earthquake network virus[2-3] and the Ukrainian power grid being attacked by a network leading to a major blackout have shown that information network attacks against the power system will seriously threaten the safe and stable operation of the grid and can lead to major security incidents such as a major blackout in serious cases[5].

Power IoT as a national critical information infrastructure, facing increasingly severe network security situation, once suffered from network security attacks will likely lead to large-scale power outages, a serious threat to enterprise and national security[6]. 2015 a country during the Christmas blackout, followed by a series of network attacks on the local energy companies, most of the region is in a power outage state[7]. Therefore, the establishment of a power IoT full-scene situational awareness system to achieve all-round, all-weather network security situational awareness of the company's various power monitoring systems and timely discovery of various network security risks as well as illegal access events has become a top priority for the security of the power system.

The application area of power IoT security covers all aspects of power production "generation, transmission, transformation, distribution, use and regulation"[8]. The network security system of power IoT adopts the form of independent networking for network deployment and is divided into three categories: encryption device, isolation device and platform operation device. Although the
existing power IOT security protection system has played some role in a certain development period, but in the current real situation, it still faces many risks such as illegal access to power IOT terminals, legitimate terminals being used to attack and unauthorized access to terminals, etc. The hazards are: malicious access and attack on the power information intranet; illegal detection and attack on the power marketing master station system; malicious load control and stop and resume power control attacks on users; false reporting of collection information resulting in power theft, etc.

2. Related work
Unstructured data is data that has an irregular or incomplete data structure, does not have a predefined data model and cannot be easily represented by a two-dimensional logical table in a database. This includes all formats of office documents, text, images, XML, HTML, reports of all kinds, images and audio/video information, etc[13][14].

Power IOT is the application of Internet of Things in smart grid, which is the result of the development of information and communication technology to a certain stage. It will effectively integrate communication infrastructure resources and power system infrastructure resources, improve the level of informationization of power system, improve the utilization efficiency of existing infrastructure of power system, and provide important technical support for power grid generation, transmission, transformation, distribution and use of electricity. Song et al.proposed a IoT device fingerprinting for relieving pressure in the access control[4]. In 2019, Zhang et al. proposed a security level evaluation system for wireless local area network access devices [9].Song et al proposed delegation authorization mechanism with controllable permissions propagation for IoT devices sharing[18]. In 2020, Deng et al.proposed a abnormal traffic detection of IoT terminals based on Bloom filter[10].Song et al.proposed a smart collaborative tracking for ubiquitous power IoT in edge-cloud interplay domain[11].Choi et al.proposed a ontology-based security context reasoning for power IoT-cloud security service[12].Song et al proposed Two-stage multi-classification algorithm for Internet of Things equipment identification. In 2021,Chen et al proposed an automated authentication of large-Scale IoT devices with hybrid feature selection[16].

Network isolation technology refers to the exchange of information and sharing of resources between two or more computers or networks on a disconnected basis, meaning that network isolation technology enables two networks to be physically separated while allowing data to be exchanged in a secure network environment[15]. The main objective of network isolation technology is to isolate harmful network security threats in order to guarantee the safe interaction of data and information within a trusted network.

3. Dynamic access control of terminals

3.1. Dynamic access control based on physical isolation
According to the "Security Protection Regulations for Electricity Secondary Systems" issued by the National Electricity Regulatory Commission (NERC) and the "Security Partitioning, Network Dedication, Horizontal Isolation, Vertical Authentication" security defense policy for electric power systems, as well as the "Security Protection Program for Electricity Monitoring Systems" issued by the National Development and Reform Commission, the intranet access to electric power information needs to be protected by high-intensity network isolation measures. Therefore, the design of this paper adopts the technical architecture of physical isolation, which is based on one-way isolation and traffic message ferrying for dynamic access control of power marketing terminals. Fig.1 illustrates the implementation principle of physical isolation.

A dynamic access control enforcement architecture based on physical isolation, with the master side connected to the power marketing master system and the terminal side connected to the power marketing terminals. Under normal circumstances, the master side and the terminal side are completely disconnected physically.
3.2. Physically isolated data transmission
When the power master system needs to have data transmission to the power terminal, the power marketing master system initiates the data transmission connection to the dynamic access control component. The dynamic access control component strips all transport layer protocols and filters the original application layer data according to the dynamic access control policy, and writes the application layer data that meets the access control policy requirements to the high-speed data transmission channel, at which time the terminal cannot interact with the data through the isolation island.

4. Dynamic access control component functionality
According to the type of response received the sender could detect the condition of receiver. There are many ways to perform port scanning, either by manual scanning or by port scanning software. The commonly used port scanning methods are divided into TCP connection scanning, TCP (SYN) scanning and ICMP scanning.

The dynamic access control component of the power IoT terminal uses a physically isolated hardware architecture to perform access control actions, so the component is divided into access control front-end, access control back-end and physical isolation card parts from the hardware architecture. From the software function, it is mainly divided into eight parts, such as access control decision module, security risk assessment module, internal and external network connection management module, upstream and downstream message processing module, upstream and downstream message forwarding module, isolation card interface module, configuration management module and unified monitoring module, as shown in Figure 2.

(1) Access control decision module
The module uses both least-privilege division of access control policy formulation and dynamic adjustment of access control policy based on risk assessment. In the case of successful terminal authentication and no abnormal trust assessment, a full hierarchy of attribute least privilege access control policies for terminal-permission, application-permission and user-permission are determined to avoid coarse-grained access control authorisation. As the trust level of the terminal is continuously evaluated and dynamically changed, this module provides dynamic access control policy decision and update management functions based on the trust level, dynamically adjusting the access rights of the access subject according to its trust level, and generating blocking policies to be sent to the isolated card to block access behaviour and adjust or revoke access rights if the access conditions are not met.

(2) Security risk assessment module
The module receives the user trust assessment results from the continuous trust assessment component on a regular basis, extracts the authentication information and business behaviour sequence information of the terminal based on the assessment results, uses a small habitat genetic algorithm to perform risk assessment on the relevant information, and sends a policy update request to the security policy decision module when the risk exceeds the limit, thus realizing dynamic permission shrinkage and abnormal access defence disposal. This function avoids the drawbacks of the traditional "once authenticated, always authorised" authentication and authorisation implementation model, which requires online authorisation determination for any business access, and realises on-demand authorisation for business access. Considering the delay in online authorization determination in the actual implementation process, the access control point can set up a cache of determination results for the set of access subject, object and operation, and block or release them directly according to the cache of determination results if the cache conditions are met. The module inherits the traditional role-based authorisation model and can be implemented without much modification to existing permission management technology solutions.

(3) Internal and external network connection management module

The module network connection uses Reactor event listening mode, listening for network connections and data messages separately, and provides a connection pool and a worker thread pool, as shown in Figure.3.

Connection listener: receives new network connections and takes a return connection from the connection pool and forwards the established connection to the event listener.

Event listening: maintains the connection state and listens for network messages and triggers an event action on the received network messages. Depending on the type of message, the corresponding message parsing and processing function is used and a thread is called to work on it.

![Figure 3. Network event monitoring mode.](image)

(4) Uplink and Downlink Message Processing Module

This module parses, filters and classifies continuous data stream messages and processes responses to link management messages.

Parsing messages extracts those messages in the network stream that meet the private protocol format; filtering messages analyse whether each field meets the expected size on top of meeting the private protocol format; message classification extracts each message type and will be cast to a designated processing thread. Messages of the negotiation type will be passed to the negotiation processing thread, the data of the service messages will be passed to the encryption and decryption thread, and the link management processing messages, which are processed directly by themselves, will be passed to the forwarding thread.

(5) Uplink and Downlink Message Forwarding Module

This module accurately forwards the packets received by the network according to the forwarding address, as shown in Figure.4.

- 1) Extract the destination address of the message from the private format;
- 2) Use the destination address to match the network descriptor in the connection pool;
- 3) If the match is successful, it will be forwarded through the data in the network descriptor and end;
4) If the match is unsuccessful, extract the terminal descriptor in the message;
5) Calculate the hash value of the descriptor, use the hash value described by the terminal to modulate the length of the connection pool, connect the network descriptor corresponding to the remainder, forward the data, and end.

Figure 4 Message forwarding process

(6) Isolation card interface module
The module uses a hardware security isolation card to provide an external read and write interface between the internal and external networks, and internally uses high-speed file exchange for data exchange processing, and supports concurrent writes, as shown in Figure 5. The read isolation card is similar to the event listening mechanism of the framework, when new data arrives.

Figure 5. Isolation card data exchange process

(7) Configuration management module
This module provides online configuration and management of components, allowing only intranet side login, login management, user management, log management and rule management.

(8) Unified monitoring module
The module monitors the operation status of the device on a regular basis and alerts on abnormal conditions, and submits the relevant information to the integrated information and communication scheduling and operation support platform and the network and information security risk warning and analysis platform.

5. Conclusion
This paper proposes a reformulation of access control policies based on the different attribute states and trust levels of power Internet of Things terminal equipment to reduce its access control authority, and on this basis, proposes a dynamic access control based on the isolation of internal and external networks. The detailed function design of each core security protection component is given, and the component module is explained.
Acknowledgments
This paper is supported by the science and technology project of State Grid Corporation of China: "Research and Application of Scenario-Driven Data Dynamic Authorization and Compliance Control Key Technology" (Grand No. 5700-202058481A-0-0-00).

References
[1] AITZHAN N Z, SVETINOVIC D. (2018) Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. IEEE Transactions on Dependable and Secure Computing, 15(5): 840–852.
[2] KERMAN A, BORCHERT O, ROSE S, et al. (2020) Implementing a Zero Trust Architecture. National Institute of Standards and Technology, 2020: 17–17.
[3] TIAN J, TAN R, GUAN X, et al. (2020) Moving Target Defense Approach to Detecting Stuxnet-Like Attacks. IEEE Transactions on Smart Grid, 2020, 11(1): 291–300.
[4] Y. Song, Q. Huang, J. Yang, M. Fan, A. Hu and Y. Jiang. (2019) IoT device fingerprinting for relieving pressure in the access control, ACM TURC ’19, pp. 8.
[5] ZENG H, SUN F, LI T, et al. (2017) Analysis of “9·28” Blackout in South Australia and Its Enlightenment to China. Dianli Xitong Zidonghua/Automation of Electric Power Systems, 41: 1–6.
[6] GARBIS J, CHAPMAN J W. (2021) Zero Trust Security: An Enterprise Guide. Berkeley, CA: Apress
[7] Zhang C, Song D, Chen Y, et al. (2019) A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data//Proceedings of the AAAI Conference on Artificial Intelligence. 33: 1409-1416.
[8] G. Abirami and R. Venkataraman. (2019) Performance Analysis of ABAC and ABAC with Trust (ABAC-T) in Fine Grained Access Control Model. 11th International Conference on Advanced Computing (ICoAC), Chennai, India.
[9] ZHANG Mingyuan, WU Wei, SONG Yubo, et al. (2020) Security level evaluation system for wireless local area network access devices. Journal of Tsinghua University(Science and Technology), 60(5): 371-379.
[10] Fengjie Deng, Yubo Song, Aiqun Hu, Min Fan, and Yu Jiang. (2019) Abnormal traffic detection of IoT terminals based on Bloom filter. In Proceedings of the ACM Turing Celebration Conference - China (ACM TURC '19). Association for Computing Machinery, New York, NY, USA, Article 126, 1--7.
[11] F. Song, M. Zhu, Y. Zhou, I. You and H. Zhang. (2020) Smart Collaborative Tracking for Ubiquitous Power IoT in Edge-Cloud Interplay Domain. IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6046-6055.
[12] C. Choi and J. Choi. (2019) Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service. IEEE Access, vol. 7, pp. 110510-110517.
[13] Anthes G. (2010) Topic models vs. unstructured data. Commun ACM 53:16–18
[14] Azad, P., Navimipour, N.J., Rahmani, A.M. et al. (2020) The role of structured and unstructured data managing mechanisms in the Internet of things. Cluster Comput 23, 1185–1198.
[15] ZHANG Kui, YANG Li. (2019) Application of Access Control List in Internal and External Network Isolation. Experiment Science and Technology, 17(5): 13-16
[16] Chen Q., Song Y., Hu A., Wang J. (2021) Automated Authentication of Large-Scale IoT Devices with Hybrid Feature Selection. In: Sun X., Zhang X., Xia Z., Bertino E. (eds) Advances in Artificial Intelligence and Security. ICAIS 2021. Communications in Computer and Information Science, vol 1424.
[17] SONG Yubo, QI Xinyu, HUANG Qiang, et al. (2020) Two-stage multi-classification algorithm for Internet of Things equipment identification. Journal of Tsinghua University(Science and Technology), 60(5): 365-370.
[18] Yubo SONG, Shanshan QI, Aiqun HU. (2019) Delegation authorization mechanism with controllable permissions propagation for IoT devices sharing. Chinese Journal of Network and Information Security, 5(2): 40-49.