Security Risk Analysis of Grid Edge Computing

Yixin Jiang*, Yunan Zhang, Aidong Xu, Xiaoyun Kuang, Jiaxiao Meng, Lin Chen and Boya Ma
Guangdong Provincial Key Laboratory of Power System Network Security, Electric Power Research Institute, CSG, Guangzhou, China.
Email: {jiangyx*, zhangyn2, xعاد, kuangxy, mengjx, chenlin1}@csg.cn, 1214788565@qq.com

Abstract. The emergence of edge computing technology brings new development direction to the construction of power grid industry. At present, for the edge computing technology of China is still in the exploratory stage, the combination of power grid and edge computing may face new security risks. This paper analysed the security risks that may occur in grid edge computing under the circumstances of identification system, communication technology, equipment protection and resource constraints, and put forward the relevant security risk analysis model and defense, aiming at solving the security problems of grid edge computing and promoting the better development of power grid.

1. Introduction
At present, the safety risk assessments of the power industry are fundamental and most of them are based on the existing assessment theories and models. Qian Shengjie et al. [1] built a risk assessment system based on fuzzy set theory and analytic hierarchy process in the study on security risk assessment of smart micro grid, which effectively improved the accuracy of security risk assessment of smart micro grid. Langer et al. [2] proposed a network security risk assessment method, which involves two interrelated analysis flows and can be used to determine the risks associated with the architectural concept of smart grid containing traditional systems and new ICT concepts. Zhan Xiong et al. [3] also proposed a security risk assessment method about state grid edge computing based on fuzzy analytic hierarchy process, and used a free threat modelling tool developed by Microsoft to build a relevant threat model for security threat analysis and security reinforcement.

More of the above research is in view of the power system risk assessment methods, the instances about combination of power grid and edge computing are rarely. However, we can carry out the risk analysis by referring to the security knowledge related to the Internet of Things and cloud computing, and combining with the practical application of edge computing in different fields.

Grid edge computing is a combination of power business and edge computing. The security risks it faces are not only related security risks at the grid level, but also security threats of edge computing technology. In literature [4], the security challenges of grid edge computing in communication network security, access control management, data and privacy protection and edge access are mentioned. This paper studied and analysed the information security risk of power grid edge computing, combined with the grid facilities, edge equipment, industrial IoT etc. We analysed the security risks of the grid edge computing from the four categories: the grid identification system security, communication technology security, equipment protection security and security on resource-constrained devices. Meanwhile, we gave some risk defence suggestions on the basis of risk analysis.
2. The Risks of Grid Identification System

2.1. The Risks of Domain Name Service

2.1.1. Distributed denial of service attacks
Distributed Denial of Service (DDoS) is a hard-prevented attack method that hackers often use. Domain name service (DNS) DDoS attack is mainly aimed at DNS system, which uses various network resources to send DNS service request and run out of DNS service resources, then makes DNS resolution service unable to handle DNS resolution request normally.

2.1.2. Cache poisoning attack
DNS cache poisoning attack means changing an item in the DNS server's DNS cache, causing the IP address associated with the host name in the cache to point elsewhere and no longer point to the correct location.

2.1.3. DNS redirection
Generally, users send DNS requests to the LOCAL DNS, LOCAL DNS will check whether there is a result in the cache. If there is no result, the LOCAL DNS initiates a recursive request to get the corresponding resolution result from the authorized DNS. In the interactive process of LOCAL DNS and authorization DNS, the attacker sends a fake response packet to the LOCAL DNS before the authorized DNS response, then the LOCAL DNS will cache the mistake result and sent it to the user, making the user access be guided to the attacker's web site.

2.1.4. DNS spoofing
DNS spoofing is a form of spoofing that an attacker imitates a domain name server. Its basic principle is an attacker can pretend to be the domain name server, and then set the queried IP address as the attacker's IP address, or construct a dummy DNS server response packet to match these parameters. In this case, users will not see the home page they want to access, but the home page of attacker.

2.2. The Risks of Object Name Service

Combined with the principle and process of object name service (ONS) analysis [5], it can be analysed that the security threats of ONS mainly exist in the following aspects:

2.2.1. The lack of authentication for the parsing server
The lack of authentication for the parsing server will bring two threats: (1) It is difficult to guarantee the authenticity of the returned results, and the resolution results may be linked to some illegal websites such as spam; (2) It is difficult to guarantee EPC privacy information. Once the ONS server discloses EPC codes, users' privacy information will be disclosed.

2.2.2. The lack of authentication for the client
ONS service records hold different application service resource entries and should return different results for users with different permissions. The DNS service itself does not authenticate the user, but returns all the information. Thus, the lack of user authentication can lead to a more common method of server attack -- Deny of Services (DOS), or even DDoS attack.

2.2.3. Plaintext transmission
ONS resolution process still relies on DNS methods, then the returned results are plaintext transmission, it brings two threats: (1) Malicious attackers can arbitrarily tamper with the content of the returned results and implement deception; (2) Plaintext transmission makes it easy for attackers to listen to users' access requests in real time, leading to the disclosure of users' privacy.
2.2.4. The lack of data integrity checks
ONS does not provide users with a method to verify the integrity of the returned result data. Attackers can tamper with the intercepted information and send it out, so as to provide users with the wrong application service resource entry and guide users to the fake resource service.

2.2.5. Security defects of DNS system
The design and architecture of ONS is based on DNS, so the system architecture of ONS also inherits the security defects of DNS system. The threats of DNS include distributed denial of service attacks [6-8], man-in-the-middle attacks, domain name spoofing, single point of failure, etc.

2.3. The Risks of Handle
The Handle identity resolution technology provides a complete security mechanism; however, the Handle system still has security risks in the following aspects.

- Privacy Protection. In general, most identification data stored in the Handle system is open, unless the there’s permission. Another weakness in Handle system is the Log files produced by the Handle server, which makes customers’ privacy vulnerable to be attacked.
- Caching and Proxy Servers. Proxy and caching servers, which could provide performance improvements and other value-added services, both position themselves as “man-in-the-middle” and are easy to get “man-in-the-middle” attacks.
- Mirror Image. The Handle system may have a delay in copying content between mirror sites. Therefore, when sending any time-sensitive data, sending the requests to primary service sites should be considered.
- DDoS Attack. The Handle system also will suffer the denial-of-service attacks, and there are no universal methods to prevent such attacks. Network situation awareness techniques can be used to perceive these attacks and to inform the administrators when an attack occurs.

3. Security Risks of Power Grid Communication Technology

3.1. Security Risks of Wire Communication Technology
Modern wire communication mainly refers to wire communication, that is, a series of tangible media such as metal wires and optical fibres are used for information transmission, in which words, images and sounds can be represented by electrical signals or optical signals [9].

Wire communication security threats include four aspects:

- Electromagnetic and equipment security. With the rapid development of computer processing power and interception technology, electromagnetic radiation will also bring many security risks. Facing the equipment with increasing capacity, technology is also increasingly complex, so it is easy to cause a series of security problems.
- Security of the signalling network. With the continuous emergence of soft exchange and other related technologies, the openness of the signalling network is also increasing, which brings a lot of security risks to a certain extent.
- Flow impact. When the communication network is impacted by a certain amount of traffic, it is likely to cause an avalanche effect, which will have a serious impact on the network performance and lead to the service suspension. Such impact is usually caused by a series of emergencies or malicious attacks [10].

3.2. Security Risks of Wireless Communication Technology
Wireless communication technology is a more convenient data transmission technology developed by wire communication technology. It can transmit data information by using electromagnetic wave propagates in the air as a carrier.

The security threat of wireless communication includes the following aspects:

- Spoofing and unauthorized accessing. Using computer or network resources without approval in advance will be regarded as unauthorized access. It primarily has the following several
forms: impersonation, identity attack, illegal user entering the network system to make illegal operation, the legal user operating in the unauthorized way and so on.

- Unauthorized information destroying and tampering. In the process of transmission, unauthorized third-party attackers tamper with the data and forge the data, which is unknown to both data transmission parties. This may cause the data receiver use the wrong data.
- Denial of service (DoS) attack. The purpose of DoS attack is to consume too many service resources continuously through reasonable service request, making legitimate users cannot get normal service response.
- Sybil attack. In this attack, a data acquisition node illegally occupies multiple identities and masquerades as multiple legitimate nodes. This has seriously affected the fault tolerance mechanism of the network, and has great harm to the routing protocol based on location.
- Wormhole attack. The idea of this attack is that the attacker transmits the information received in a certain area of the network through a high-speed tunnel, and then replay it in other areas, which disrupts the normal routing and attracts forwarding information [11].

4. Risks of Power Equipment Protection

4.1. Tampering Risk of Field Equipment
The equipment deployment of grid edge computing is not only deployed in places with security measures, such as central machine room, but also deployed in open field environment. There are few people in the field environment, and the corresponding supervision measures are not perfect, which may easily lead to some illegal users to intervene and tamper with the information and data in the equipment.

4.2. Attack Risk in Complex Urban Environment
The relevant facilities and equipment of grid edge computing may operate in some open and uncontrolled environment in the city, like public environment with dense population. With the in-depth development and extensive application of Internet of Things technology, the smart city is also under construction. Gateways, large and small, are all over the city. Coupled with the popularization of smart phones and wireless devices, a complex urban network environment has been formed, and corresponding security problems also follow. Edge equipment includes mobile terminals, iot devices or sensors etc. in all edge network. Sensor nodes at the edge computing terminal is easy to suffer attacks. If an iot terminal was invaded, controlled, an attacker can infection more Internet terminals by communication means, finally it will form a large-scale botnet, launch a large number of service requests to backbone network or service network, which may make the network paralysis [12].

5. Risks on Resource-constrained Devices

5.1. Risk of Low Computing Power
Low computing power may lead to data not being processed in real time, which will consume more time, and also lead to congestion of subsequent data transmission. In the process of data transmission, in order to ensure the security of data and prevent data leakage, the sender of data will encrypt the data and then send it out. Low computing power of the device will result in incomplete data encryption, and some encryption algorithms requiring high computational power cannot be used. As a result, data will be easily leaked in the process of transmission, which will be cracked by a third party and the information content will be obtained. At the same time, the data needs to be decrypted at the receiving end of the data. Due to the insufficient computing power of the device, more time will be spent on decrypting and the real-time transmission of data cannot be completed, which will cause delay.

5.2. Risk of Low Storage Capacity
The storage capacity of equipment is very important in grid edge computing. The data storage of edge computing is to store the data in the data collection point without transferring the collected data to the central server, which can guarantee the low delay and high reliability of data processing. However, if
the storage capacity of the device is low, it will bring the security risk of data storage. Under the condition of edge calculation, the amount of data will be very large. With large amount of data and low storage capacity, there will be no space for data isolation technology, which will lead to data storage chaos, data leakage and other phenomena. If the storage capacity of the device is low, when the data is transferred for storage, the data cannot be encrypted. Then the method of plaintext storage will be adopted, it is easy for external intruders to take advantage of this to steal data files. In addition, when the storage capacity of the device is low, there is no enough space for data caching.

6. Calculated Security Risk Analysis Model and Risk Defence for Power Grid Edge

6.1. Security Risk Analysis Model
The security risk analysis model of grid edge computing can be constructed from three aspects: risk analysis, risk management and risk measures.

- Risk analysis. Risk analysis is mainly conducted from six aspects of node security, network security, identity security, data security, application security and operation security.
- Risk management. Risk management mainly consists of four parts: establishing risk target, constructing index system, identifying risk and formulating risk strategy.
- Risk measures. Risk measures clear methodological guidelines, achieve closed-loop management and risk control from the perspective of the full life cycle. Risk measures mainly include industry supervision, safety monitoring, situation awareness, threat early warning and response and disposal the five links.

6.2. Risk Defense
The security defence system of grid edge computing should take corresponding protection measures form following six risk analysis objects.

6.2.1. Node security
Node security can provide basic ECN protection security, such as virus detection, vulnerability repair, host monitoring pre-audit and other functions [13]. Secure and reliable remote upgrade can complete the repair of vulnerabilities and patches in a timely manner, also can avoid the failure of the system after upgrade; lightweight trusted computing, which solves basic trust problems, can be applied in devices with limited computing power and storage capacity.

6.2.2. Network security
Network security can guarantee network security from inside to outside from network security protocol, network security isolation, network security monitoring, network protection. For the problem of security protocol, it can be encapsulated again by adding communication module or gateway outside the original protocol layer, transmit via VPN, SSL and other secure channels, or carry out covert communication or encrypted communication.

6.2.3. Identity security
The functions of identity authentication are all over the functional level of edge computing. Due to the access of massive devices at the edge of the network, the traditional centralized security authentication faces great performance pressure. Especially in the centralized and online equipment, the authentication system is often overwhelmed, which requires the implementation of decentralized and distributed authentication by adopting the minimum authorization model based on demand behaviour.

6.2.4. Data security
Data security includes data isolation and destruction, data encryption, data leakage prevention and data privacy protection, etc. The data leakage prevention of edge computing is different from the traditional data leakage prevention, the equipment of edge computing is usually distributed deployment, it needs to consider that the data obtained from these stolen devices will not reveal any information.
6.2.5. Application security
Application security mainly includes white list, malicious attack prevention, security detection and response, software reinforcement and patch, sandbox and access behaviour supervision, etc. Among them, white list is an important function of edge computing security architecture. Due to the massive heterogeneous access of terminals and the wide variety of services, the traditional IT security authorization model is no longer applicable. It is necessary to use the minimum authorization security model to manage applications and access rights.

6.2.6. Operation safety
Operation security is mainly a variety of management security. Physical environment management need to do different management for the open environment and relatively closed computer room environment; access control risks include physical access control risks and system access control risks. Implementing different security access control measures for different physical environments in different security areas can effectively avoid such risks. The setting of system access control policy should consider the principle of “minimum permission” and authentication requirements. In terms of personnel management, information security awareness of relevant personnel should be cultivated, and some technical personnel who understand information security management can be introduced.

7. Conclusion
Nowadays, edge computing technology has been increasingly applied in a wide range, which makes it possible for new technologies like artificial intelligence to be applied in a wider range, and also enables computing resources and computing power to obtain a wider range of services [14]. Smart power grid and ubiquitous power IOT are now the important application scenarios of edge computing. The application of edge computing technology in power grid will better promote the development of power grid. This paper mainly studied the possible security risks of power grid edge computing, constructed the security risk analysis model of power grid edge computing from three directions, and introduced the security risk defence of power grid edge computing. Edge computing is still in the exploratory stage, and its related security problems still need to be explored and solved. In the subsequent exploration, the security problems related to grid edge computing are bound to be solved.

8. References
[1] Qian S and Yang T 2020 Research on security risk assessment of smart microgrids based on fuzzy set theory J. Energy Conservation 39(02) 6-9.
[2] Langer L, Skopik F, Smith P, et al. 2016 From old to new: assessing cybersecurity risks for an evolving smart grid J. Computers & Security 62 165-176.
[3] Zhan X, Guo H, He X, Liu Z, Sun X and Chen H 2019 Research on security risk assessment method of state grid edge computing information system J. Computer Science 46(S11) 428-432.
[4] Li G, Wang Z, Zhang J and Yue R 2020 Computational security protection for power grid edge J. China Science and Technology Information 15 63-64.
[5] Wang H and Sun Z 2016 ONS security mechanism research J. Computer Science 43(1) 1-7.
[6] Claude F, Elias B-H and Mourad D 2014 Fingerprinting internet DNS amplification DDoS activities 2014 6th International Conf. on New Technologies Mobility and Security.
[7] Li W, Cao X, Liu F, et al. 2011 Improving DNS cache to alleviate the impact of DNS DDoS attack Journal of Networks 6(2) 279-286.
[8] Dhananjay P, Sherman A T, et al. 2013 Spread identity: A new dynamic address remapping mechanism for anonymity and DDoS defence Journal of Computer Security 21(2) 233-281.
[9] Lin X 2016 Research on the construction of public security wired communication network J. Science and Technology Innovation Herald 13(16) 80-81.
[10] Chang L 2017 Development and future prospect of wired communication network security J. Digital Communication World (04) 122+124.
[11] Wang X, Chen T, et al. 2013 Security analysis and research of power internet of things communication technology Chinese Society for Electrical Engineering.
[12] Liang Q 2020 Analysis of edge computing security threat status and protection technology *J. Network Security Technology & Application* (04) 9-10.

[13] Dai X, Liao F and Chen J 2020 Research on edge computing security protection system *J. Communications Technology* 53(01) 201-209.

[14] Lu G 2018 Research on enterprise security in the context of edge computing application *J. Cyberspace Security* 9 (10) 87-93.