Security Management Method of Power Communication Access Network Based on EPON Technology

Chengfei Qi[1(✉)], Chaoran Bi[1], Yan Liu[1], Tongjia Wei[1], Xiaobo Yang[1], and Licheng Sha[2]

[1] Metrology Center of State Grid Jibei Electric Power Co., Ltd., Beijing 100045, China
qichengfei48586@163.com

[2] State Grid Beijing Electric Power Company, Beijing 100031, China

Abstract. Generally, to ensure the security of the network is at the expense of network performance. In view of this problem, this paper attempts to apply EPON Technology to the security management of power communication access network. It is found that EPON Technology can provide a key with a length of 48 bits, with a total number of 248 keys, which is close to DES encryption in key length, which is more suitable for the service carrying requirements of power communication access network.

Keywords: EPON Technology · Power Communication · Safety Management

1 Introduction

EPON adopts point to multipoint structure and passive optical fiber transmission to provide a variety of services on Ethernet. EPON Technology is standardized by IEEE802.3 EFM working group. In June 2004, the IEEE802.3 EFM working group issued the EPON standard, ieee802.3ah (incorporated into the ieee802.3-2005 standard in 2005) [1]. In this standard, Ethernet and PON technology are combined, PON technology is adopted in the physical layer, Ethernet protocol is used in the data link layer, and Ethernet access is realized by using the topology of PON. Therefore, it combines the advantages of PON technology and Ethernet Technology: low cost, high bandwidth, strong scalability, compatibility with existing Ethernet, convenient management, etc. [2–4]. The concept of passive optical network has a long history. It has the characteristics of saving optical fiber resources and being transparent to network protocols. It plays a more and more important role in optical access network. At the same time, after 20 years of development, Ethernet technology has almost completely dominated the LAN with its characteristics of simplicity, practicality and low price. In fact, it has been proved to be the best carrier to carry IP packets. With the increasing proportion of IP services in Metro and trunk

B. Wang et al. (Eds.): ICMTEL 2023, LNICST 533, pp. 12–22, 2024.
https://doi.org/10.1007/978-3-031-50574-4_2

transmission, Ethernet is gradually infiltrating into access, Metro and even backbone networks through the improvement of transmission rate and manageability. The combination of Ethernet and PON produces Ethernet passive optical network [5, 6]. It has the advantages of both Ethernet and PON, and is becoming a hot technology in the field of optical access network. EPON is a new broadband access technology. It realizes the comprehensive service access of data, voice and video through a single optical fiber access system, and has good economy. Industry insiders generally believe that FTTH is the ultimate solution for broadband access, and EPON will also become a mainstream broadband access technology [7]. Due to the characteristics of EPON network structure, the special advantages of broadband access and the natural organic combination with computer network, experts all over the world agree that passive optical network is the best transmission medium to realize the "integration of three networks" and solve the "last kilometer" of information highway.

Access network is also called user access network. For a long time, the service of communication network is mainly voice service, and the traditional access method is to use twisted pair copper cable to connect the user terminal to the switch of the local exchange. With the continuous improvement of social informatization, the types of communication services also began to develop from a single voice service to data service, image service and comprehensive service. The traditional twisted pair access mode is difficult to adapt to this development trend. Countries are developing a variety of access methods. Combined with the overall development ideas, principles and strategies, this paper analyzes the current situation, existing problems, development objectives, networking technology selection, EPON introduction and evolution, as well as the principles, application scenarios and technical schemes of network planning, and designs the security management method of power communication access network based on EPON Technology as follows.

2 Design of Security Management Method of Power Communication Access Network Based on EPON Technology

2.1 Security Risk Analysis of Power Communication Network

Power communication network security is mainly composed of physical security and information security.

Physical Security Risks

Physical security mainly refers to line security, communication equipment security, communication network structure security and other aspects, mainly including transmission network, service network, access network and other aspects. Link line safety mainly refers to the safety of wired or wireless lines such as communication optical cable, microwave, wireless and power line carrier. The interference factors include lightning strike, external force damage, frequency interference, etc. Communication equipment security refers to the reliability of SDH, ont, microwave, carrier and other transmission

equipment in terms of communication equipment configuration, redundancy protection technology, performance index, aging degree, electromagnetic compatibility, etc. in terms of security structure, power enterprises are generally configured as server, switch, working host, dual route backup protection, dual power supply backup protection and dual board backup protection [8]. The physical security risks of general power enterprises include the security protection deployment of the machine room against natural disasters such as fire or earthquake, whether the network cables laid in the machine room have electromagnetic radiation shielding, equipment fire wire grounding and other measures, dual UPS power supply configuration, preventive measures to prevent man-made damage to power communication equipment, and disaster recovery and backup of important data information.

Information Security Risks

Information security mainly refers to data transmission channel, Internet boundary protection, host equipment and terminal port security, data information security, etc. mainly at the network and business level based on IP protocol such as data network, there are risks such as malicious code propagation, Internet boundary penetration, illegal control of information network equipment, data source camouflage, transmission message tampering, transmission message eavesdropping, etc. [9, 10]. The security risks of IMS and other new technologies and business networks include insufficient protection level of core equipment, unclear application, no security protection, illegal outreach, untimely software version update, unclear security positioning, insufficient protection awareness, etc. The security risks supporting the network include host equipment security, Internet border security, data security and so on. The security risks of access network include illegal authentication, too complex networking, illegal access, too much information, malicious attack, eavesdropping information, intercepting information and monitoring information.

2.2 Zoning and Hierarchical Management Mode

According to the above analysis results, the information security defense mode of power communication access network is designed. According to the implementation standards of power grid operation and management and different application directions and use requirements of various professional networks, the defense mode of power communication access network is built into “three layers and four areas”, and the carrying business is divided intothree layers of automation, production management and information management according to the vertical level, It is divided into four areas: real-time control, non controlled production, production management andmanagement information, which correspond to the structure ofpowercommunication access network. See the following Fig. 1:

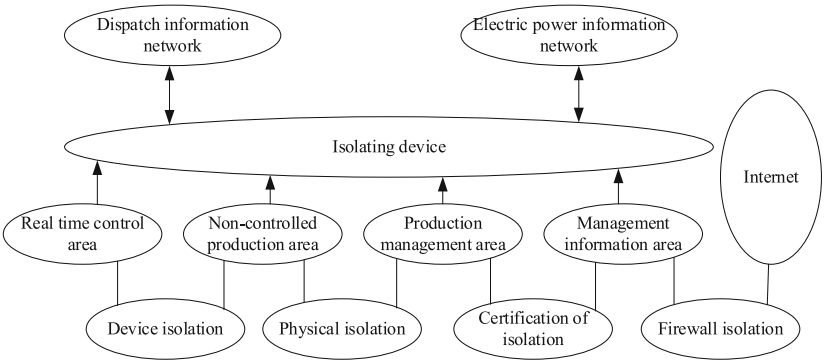

Fig. 1. Information protection layer of power communication access network

Hierarchical management: technical means to manage equipment, system and network separately at the three levels of automation, production management and information management. So that the three levels can operate independently without affecting each other. At the same time, network connection is adopted, and isolation devices with different means are adopted between zones. They can be accessed and read by using information technology means, but can not be modified and written.

Partition management: network physical equipment, such as authentication system, identity recognition [11] and firewall, are used to isolate each area, focus on the protection of key business nodes such as real-time control area, and adopt security isolation devices with different permissions and different functional strength according to the importance of each area, so as to cover the information security protection of the covered businesses.

Among the four regions. The real-time control area includes a sensing and receiving device, which can display the electric quantity value and marketing data index in real time. Non controlled production areas include businesses that can provide data services but do not have control functions in production and marketing, such as simulation, work ticket generation, etc. The production management area needs to realize the coordination and cooperation between disciplines and departments. The management information area needs to realize collaborative office and external contact. Therefore, the area should have the function of logging in to the Internet on the basis of ensuring no disclosure.

Different areas are distinguished by physical isolation. For example, the identity verification system, access control, keys, etc. are divided into different office areas, so that the personnel in different areas cannot reach other areas without identity authorization. So as to ensure the isolation of personnel in the geographical environment. Between different levels, we grant different levels of access rights to different users in the management operating system. Access to other professional controlled information systems needs to be confirmed through the firewall and data interface, and the information stored under each user name is subject to technical encryption and certificate authentication, Users without corresponding qualifications cannot access the information possessed by other users [12]. In this way, low-level users will not be able to obtain the data held by high-level users. On the contrary, high-level users can control and manage the

identity permissions of low-level users. So as to achieve the ultimate goal of zoning and hierarchical management.

2.3 Physical Security Management Based on EPON Technology

According to the requirements of relevant technical standards and specifications of power communication access network equipment, as well as the safety risk, reliability risk, electrical and electromagnetic compatibility safety risk of EPON equipment technical indicators, the following safety protection points are put forward:

(1) According to the security risk factors of technical indicators of access network equipment, it is required that the OLT MAC function and performance of EPON equipment, the MAC performance of ONU, uplink bandwidth allocation function, ONU loopback operation, Ethernet performance, QoS function [13, 14], multicast function and performance, service interface function and performance, and optical interface characteristics meet the requirements of relevant standards and specifications for network access detection, Select equipment manufacturers with high reputation.
(2) In view of the safety risk factors of electromagnetic compatibility, the electromagnetic compatibility radiation and immunity of access network equipment are required to meet the requirements of standards and specifications for network access detection, including port withstand voltage detection, impulse voltage detection, immunity detection, etc.
(3) According to the reliability requirements and safety risk factors, the topology of EPON networking optical cable shall be designed according to the power grid structure, the importance of carrying business and the construction of optical cable, and support three switching modes: trunk optical fiber protection, full protection and hand-in-hand. 10 kV communication access network should adopt ring, tree or star topology, and 0.4 kV communication access network should adopt bus, tree or star topology. For EPON network [15, 16], the networking structure carrying important services of distribution network (such as distribution automation) shall adopt double star backbone ring, double chain backbone ring or hand-in-hand networking mode. Important board redundancy of EPON equipment, such as OLT main control board and power board redundancy protection.
(4) Safety management: carry out safety management on environment, assets and network, carry out safety management on network operation and maintenance, and formulate safety incident disposal plan and emergency plan.
(5) Personnel safety management: formulate communication personnel management system, including personnel departure, assessment, safety training, etc.

2.4 Information Security Management Based on EPON Technology

The EPON network of power communication network carries the data transmission of remote protection service and the transmission of power information collection service, which requires high confidentiality and controllability of information. At the same time, the load-bearing service of power communication EPON network is sensitive to time delay. Therefore, the technical means of encryption authentication, service isolation,

message filtering, access control and security management are adopted in EPON networking to ensure the integrity, confidentiality, availability and controllability of the transmitted data in the network.

(1) Encryption authentication
EPON downlink data is subject to triple agitation and de agitation processing to isolate information among users. The uplink MAC (media access control) frame and OAM (operation management and maintenance) frame are processed by triple stirring encryption algorithm to prevent malicious users from forging MAC frame or OAM frame in the data channel to change the original configuration of the system or destroy the system.
(2) Service isolation
EPON shall support the implementation of VPN based on VLAN technology according to user services [17], and shall support VLAN based on port or MAC address. The number of MAC addresses received by the user port shall be limited, or the user's MAC address shall be bound with the specified port. At the same time, the Mac and IP addresses of users shall be bound.
(3) Message filtering
In EPON system, ACL stream filtering mechanism is adopted to enable the system to support the source and destination MAC address frame filtering of ports, and also realize the packet filtering of upper layer protocol types, such as source, destination IP address, vlanid and TCP port number.
(4) Access control
Access control for servers, equipment terminals, etc. shall be realized in EPON networking, and network access control means such as 802.1× shall be used for authentication before access to the network.
(5) Safety management
For EPON networking, safe remote management mode and safe network management system shall be adopted for monitoring and management.

3 Experimental Analysis

Build a distribution network integrated service communication access test platform, and verify the application effect of EPON Technology in power communication access network security management through the analysis of test data.

3.1 Experimental Platform

The integrated service communication access test platform of distribution network is used to simulate the integrated access of real-time and non real-time services such as distribution automation, power consumption information acquisition and video monitoring in distribution network, and to realize the comprehensive monitoring and management of various communication equipment in distribution communication network. The test platform consists of hardware platform and software platform. The hardware platform includes EPON system, distribution automation system, such as data transmission unit, feeder terminal, contactor, power consumption information acquisition system (concentrator, collector), three-layer Industrial Ethernet switch, server, front-end computer,

workstation, camera terminal, communication power supply, etc. The software platform includes three parts: distribution network communication network management system, distribution automation system and remote meter reading system. The test platform is composed of master station layer, convergence layer and access layer. The master station layer includes integrated network management system, distribution automation master station system, power consumption information acquisition master station system and integrated access hardware platform; The convergence layer is a ring network composed of three three-layer Industrial Ethernet; The access layer is EPON system. The test platform can realize the remote control, remote signaling and telemetry functions of distribution automation and the remote meter reading function of power consumption information acquisition. At the same time, on the test platform, all communication equipment of the platform can be centrally monitored and managed through the distribution network communication network management, realizing the comprehensive access of a variety of communication technologies, as well as the access of distribution automation and power consumption information acquisition services, and isolating the power consumption information acquisition and distribution automation services through different PON ports.

3.2 Experimental Setup

Establish a test platform, log in to the test platform network management, ensure the normal monitoring and control of all equipment on the network, and ensure the normal data transmission of the network. The MAC address of each ONU is bound with the OLT. In the process of data transmission, the data is further processed by using the above design method, the key update cycle is set to 10 s, and the peak bandwidth and minimum guaranteed bandwidth of each ONU are allocated according to the service requirements. Observe the data transmission and record the changes of system throughput and forwarding delay.

Secondly, in order to ensure the reliability of power communication EPON networking service, trunk optical fiber redundancy protection or full protection is usually adopted. Therefore, in the test platform, the above two protection measures are adopted for EPON networking carrying distribution automation service and power consumption acquisition service respectively to simulate link or equipment failure, switch transmission service and record protection switching time. First, create backbone optical fiber protection or full protection on EPON equipment, and bind any two PON ports in PON service board on OLT to make the two PON ports have the same configuration. Secondly, the bandwidth of each ONU is allocated according to the bandwidth requirements of the bearer service.

3.3 Analysis of Experimental Results

Throughput Test

In the power communication access network, the services with packet length of 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes, 1280 bytes and 1518 bytes are transmitted respectively. The uplink and downlink throughput of the network are tested when EPON technical safety protection measures are adopted. The recorded results are as Table 1:

Table 1. Throughput

Byte	Tradition (down)	After EPON technology processing(down)	Tradition (up)	After EPON technology processing(up)
64	978.4	978.4	989.4	989.4
128	981.8	981.8	974.3	974.3
256	993.5	993.5	988.4	988.4
512	995.2	995.2	986.2	986.2
1024	994.7	994.7	982.4	979.7
1280	995.4	995.4	977.1	978.5
1518	998.3	998.3	977.0	978.4

It can be seen from Table 1 that when EPON Technology is used to process downlink data (including data frame and control frame) and EPON Technology is used to process uplink MAC frame and OAM frame in networking, it has no impact on system throughput.

Forwarding Delay Test

When EPON Technology is adopted, 90% of the throughput services are forwarded in the network, that is, seven services with different packet lengths of 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes, 1280 bytes and 1518 bytes are forwarded respectively. Test whether the forwarding delay is affected by security measures, and record the average forwarding delay results of multiple groups for comparison.

It can be seen from Table 2 that in networking, EPON Technology has little impact on data forwarding delay after processing downlink data, including data frame and control frame, that is:

$$\Delta T_{avg(down)} \approx 0.25(\mu s) \tag{1}$$

Table 3 shows that EPON Technology has little impact on data transmission delay when processing uplink MAC frames and OAM frames, that is:

$$\Delta T_{avg(up)} \approx 0.05(ms) \tag{2}$$

Table 2. Downlink forwarding delay (μs)

Byte	Tradition			After EPON technology processing		
64	17.564	17.621	17.623	17.845	17.816	17.884
128	20.465	20.549	20.654	20.847	20.647	20.716
256	25.504	25.648	25.624	25.843	25.741	25.769
512	36.142	36.249	36.654	36.491	36.287	36.347
1024	57.814	57.864	57.889	57.984	57.915	57.934
1280	68.945	68.951	68.934	69.087	69.051	69.054
1518	79.148	79.201	79.219	79.413	79.148	79.201

Table 3. Uplink forwarding delay (μs)

Byte	Tradition			After EPON technology processing		
64	1.287	1.301	1.301	1.342	1.331	1.323
128	1.306	1.304	1.306	1.387	1.337	1.314
256	1.325	1.324	1.304	1.399	1.357	1.387
512	1.354	1.351	1.327	1.471	1.367	1.397
1024	1.465	1.475	1.413	1.487	1.447	1.448
1280	1.423	1.416	1.447	1.489	1.466	1.487
1518	1.489	1.476	1.487	1.497	1.504	1.516

Class B Protection Test

The tester sends uplink and downlink data through ONU/OLT, the frame length is 1230 bytes, the rate is 100 Mbps, and the data service is normal; Simulate the disconnection or abnormality of the working optical fiber, check whether the service can be automatically switched to the standby optical fiber, check the packet loss, record the uplink and downlink packet loss, and convert it into the service switching time according to the rate:

$$T_a = \frac{f_m - f_x}{v} \tag{3}$$

where T_a refers to the service switching time, and the unit is s; f_m represents the total number of bytes sent, in MB; f_x represents the total number of bytes received, in MB; v represents the transmission rate, in Mbps.

It can be seen from Table 4 that in order to ensure the safety of EPON networking services, when class B protection (backbone optical fiber protection) is adopted for important lines, if the optical fiber is damaged or abnormal conditions occur, the transmission services will be switched to the standby link, the data will be lost during the switching process, and the packet loss rate will not increase with the increase of traffic.

Table 4. Average switching time of backbone optical fiber protection (MS)

The number of ONU	down	up
1	2	6
2	1.5	5.25
3	2	6.25
4	2	6.2

Class C Protection Test

Class C protection is full protection, and standby protection is used for trunk optical fiber and branch optical fiber. The tester sends uplink and downlink data through ONU/OLT, the frame length is 1230, the rate is 100 Mbps, and the data service is normal; Simulate the disconnection or abnormality of the working optical fiber, check whether the service can be automatically switched to the standby optical fiber, check the packet loss, record the uplink and downlink packet loss, and convert it into the service switching time according to the rate.

It can be seen from Table 5 that in order to ensure the security of EPON networking services, full protection is adopted for important lines. Because EPON adopts broadcast mode in downlink and time division multiplexing technology in uplink, if the optical fiber is damaged or abnormal, the uplink switching time is significantly greater than the downlink switching time in the switching process. The switching time will not increase with the increase of business volume, and the switching time is less than 50 ms.

Table 5. Average switching time of full protection (MS)

The number of ONU	down	up
1	3.80	24.50
2	3.70	30.10
3	5.80	31.00
4	4.10	30.23

4 Conclusion

With the development and application of national, local and large-scale enterprises and institutions' communication networks, all kinds of communication networks are required to not only provide safe information transmission channels, but also the nodes necessary for transmitting information, because the security equipment providing security protection function is usually located at network nodes such as terminals, routers, gateways and front-end computers, It is a problem that must be considered in the future development of power communication network. I hope the above contents can provide effective reference for relevant research.

References

1. Jiang, Y., Zou, X., Yan, X., et al.: Point-to-multipoint phase-stabilized microwave signal transmission in optical fiber links using passive phase compensation. Acta Optica Sinica **39**(09), 86–92 (2019)
2. Yan, X., Yu, P., Nan, Y., et al.: Experimental analysis of four-wave mixing effect on next generation Ethernet passive optical network. Opt. Eng. **59**(7), 1–14 (2020)
3. Li, Y., Zhang, Z.: Network security risk loss assessment method based on queuing model. Comput. Simulat. **38**(04), 258–262 (2021)
4. Zhang, R., Li, Y., Tian, G., Li, T.: Research on the management methods of network security risk in Colleges and Universities. J. Changsha Telecommun. Technol. Vocat. College **20**(02), 29–31+56 (2021)
5. Wang, Z., Zhou, J.: Cyber security risk assessment and construction scheme design of community hospital. Inf. Secur. Technol. **12**(Z2), 50–56 (2021)
6. Li, X., Guo, T., Xiang, Y., Ning, H.J., et al.: Application of blockchain technology in industrial internet and analysis on its network security risks. Indust. Technol. Innov. **08**(02), 37–42 (2021)
7. Jiang, R.: Design of network security risk detection system based on N-gram algorithm. Mod. Electron. Techniq. **44**(01), 25–28 (2021)
8. Cui, W., Duan, P., Zhu, H. et al.: Security risk assessment on of attack graph and HMM industrial control network. Comput. Moderniz. **2020**(07):32–37+49 (2020)
9. Zhou, S.: Design of novel optical fiber communication electronic system and big data prediction method of its loss. J. Nanoelectron. Optoelectron. **16**(8), 1308–1316 (2021)
10. Jin, H.S.: Analysis of network security risk detection based on immunity. Comput. Eng. Softw. **41**(10), 201–203 (2020)
11. Tang, F., Luo, Y., Cai, Y., et al.: Arc length identification based on arc acoustic signals in GTA-WAAM process. Int. J. Adv. Manuf. Technol. **118**(5/6), 1553–1563 (2022)
12. Huang, M., Qi, H., Jiang, C.: Coupled collaborative filtering model based on attention mechanism. J. South China Univ. Technol. (Nat. Sci. Edn.), **49**(07), 59–65 (2021)
13. Kalibatiene, D., Miliauskaite, J.: A dynamic fuzzification approach for interval type-2 membership function development: case study for QoS planning. Soft Comput. **25**(16), 11269–11287 (2021)
14. Laki, S., Nadas, S., Gombos, G., et al.: Core-stateless forwarding with QoS revisited: decoupling delay and bandwidth requirements. IEEE/ACM Trans. Netw. **29**(2), 503–516 (2021)
15. Roy, D., Dutta, S., Datta, A., et al.: A cost effective architecture and throughput efficient dynamic bandwidth allocation protocol for fog computing over EPON. **4**(4), 998–1009 (2020)
16. Thangappan, T., Therese, B., Suvarnamma, A., et al.: Review on dynamic bandwidth allocation of GPON and EPON. J. Electron. Sci. Technol. **18**(4), 297–307 (2020)
17. Rayapati, B.R., Rangaswamy, N.: Bridging electrical power and entropy of ONU in EPON. Optoelectron. Lett. **17**(2), 102–106 (2021)