2019 International Computer Science and Applications Conference (ICSAC 2019)

Security Architecture of Wireless Private Networks for Smart Grid

Bin Yang, Yue Hou, Yefeng Zhang
State Grid Corporation of China
Beijing, P.R.C
{yang-bin, houyue,
zhangyefeng}@sgcc.com.cn

Shiying Feng
Potevio Information Technology Co., Ltd.
Beijing, P.R.C
fengshiying@potevio.com

Yong Zhang
Beijing University of Posts and Telecommunications
Beijing, P.R.C
Yongzhang@bupt.edu.cn

***Abstract*—Due to the open nature of wireless networks, power wireless private networks (PWPNs), as the carrier of smart grid service, must provide highly reliable and secure communication capabilities. The security risks of terminals, wireless channels, base stations, core networks, host systems and data applications are analyzed. Aiming at the multi-service characteristics of smart grid, a security architecture based on service isolation is proposed in PWPNs. The architecture implements end-to-end service security isolation and can effectively combat different security threats from outside.**

***Keywords*—Wireless private networks, Grid communications, Network security**

I. Introduction

The terminal communication access network is an extension of the backbone communication network and an important component of the power communication network. As the scale of power service terminals grows rapidly and the types of service applications continue to increase, the existing communication methods gradually expose some problems. For example, due to the wide coverage of power service terminals and the high investment of optical fiber networks, it is difficult to construct and maintain the power communication network. A cable network based on optical fiber networks is hard to achieve comprehensive and rapid coverage. The wireless public network cannot provide enough security for smart grid. Therefore, it is imperative to build a power wireless private networks (PWPNs).

However, due to the real-time and security requirements of power services, PWPNs face many challenges [1]. At present, many scholars have carried out research on security issues in smart grids. Reference [1] analyzes the security requirements of smart grids, including high level security requirements, privacy, availability, and integrity, etc. Reference [2] presented an overview of the security and privacy issues of Internet of Things (IoT) including smart grid. Reference [3] and reference [4] developed the smart grid security testbed. Reference [5] presents a survey of recent security advances in smart grid, by a data driven approach. These studies focused more on the security issues of the smart grid itself, and less on the security of communication networks in smart grids.

Currently, the main standard for China's PWPNs is based on long term evolution (LTE) [6-9]. However, LTE networks are not absolutely secure and are still susceptible to a number of security threats. Raza, et al. uncovered the vulnerabilities in the current LTE security measures [10]. Danish, et al. presented an asset-focused threat model for small cell LTE networks [11]. Three major risks, the availability of the network resources, unauthorized access, end-user privacy and confidentiality, can affect the security of the LTE networks and their users [11]. Kazi J. et al. analyzed the security issues in LTE-based vehicle to everything (V2X) network and proposed a security architecture [12]. Caidan, et al. presented an overview of the machine-type communication (MTC) architecture and security threats, and solutions [13]. The authors proposed a cross-layer authentication solution based on MTC devices' hardware fingerprints toward an LTE heterogeneous network. To the best of our knowledge, there is no literatures that proposed the security architecture for PWPNs.

II. PWPNs Architecture and Security risk

A. PWPNs architecture

At present, the PWPNs based on TD-LTE technology have been developed in China, mainly to solve the problem of IoT service such as distribution automation, power consumption information collection, distributed power supply, etc. PWPN provides communication link between power service main station and service terminal (such as power distribution terminals, concentrators, data collectors, negative control terminals, etc.). Therefore, its information security protection is the primary problem to be solved.

The basic network elements of the PWPNs includes a wireless communication terminal, an evolved NodeB (eNB), an evolved packet core (EPC), etc. The transmission links includes the wireless channel between the wireless communication terminals and the base stations and the wired channels between the base station and the core network. All wireless communication terminals, base stations, core networks and other nodes are not connected to the public Internet. After the data comes out of the core network, it is connected to the production control area and the management information area through the security access area. The overall deployment architecture of the PWPNs is shown in Figure 1.

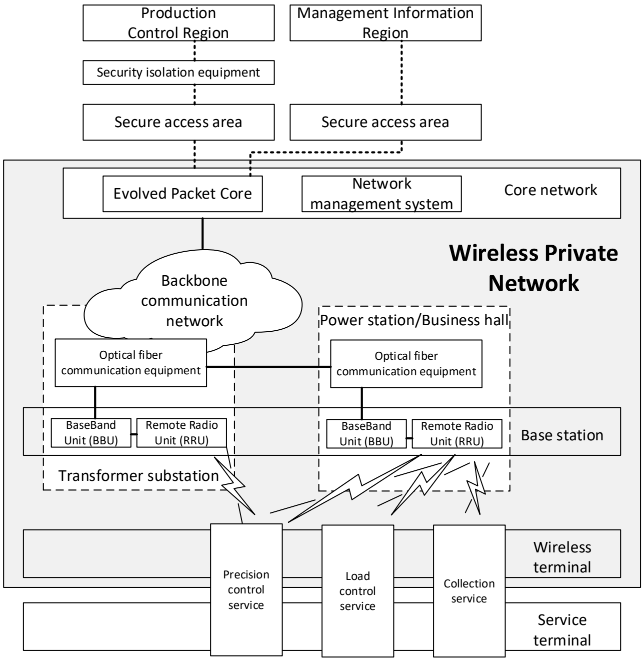


Fig. 1. System architecture

B. Risk analysis

The PWPNs mainly carry the services of power distribution, power consumption and management, and mainly faces various malicious attacks from wireless communication terminals, wireless channels, base stations, wired channels, core networks, application, host systems, and data. These risks are analyzed.

(1) Network level risk

a) Wireless communication terminal

By copying Internet protocol (IP) address, media access control (MAC) address, universal subscriber identity module (USIM) card and other ways, the attacker may implant malicious code, infiltrate the core network and sniff service data. In addition, there are further risks of access to the service system after the attacker establishes a connection with the core network through the wireless communication terminal. For example, the attacker could send fake data and sniff service data. Illegal access may lead to communication interruption, service terminals out of control, wrong instructions issued by service systems due to illegal data, sensitive service data leakage and other problems.

b) Wireless channel

The openness of the wireless channel makes it possible to be interfered by a wireless transmitter, resulting in communication interruption. Narrow-band interfering is relatively easy to be employed. Furthermore, it is possible to interfere the PWPNs through multiple narrow-band interferers at different frequencies. In addition, the use of wireless network sniffing technology to illegally intercept wireless signals may eavesdrop or tamper with wireless data transmission. However, the transmission information of the LTE-based power wireless private network has been encrypted, and it is difficult to crack and tamper.

c) Base station

By destroying physical protection devices or exploiting management vulnerability to illegally invade the base station can interrupt the communication. This kind of attack means can making the service terminal blind and out of control. However, the base station is generally in a controllable physical environment, and the physical security vulnerability of the base station needs to be exploited after the physical illegal access, which is difficult to implement.

Another attack method is the use of pseudo base station. When the terminal powers on to select networks or reselect, one base station will be selected according to the received signal strength of the terminals. When a pseudo base station occurs and the signal is strong, the terminal will select the pseudo base station, causing communication interruption. The same as the consequences of wireless interference, causing the service terminal out of control. The LTE system has taken certain security measures against attacks from pseudo base station, which can prevent such attack means.

d) The wired channel

Traditional cyber-attacks can be initiated over a wired network. Base stations, core network equipment and service terminals in the production control area face traditional network attacks such as denial of service attacks, IP address spoofing, and retransmission attacks, etc. This kind of attack is the traditional cyber security risk. Different from the public network, the attacked targets are in a controllable environment, so it is difficult to launch such attacks. It is also difficult to access production service through the intranet.

e) The core network

The possible methods include breaking physical protection devices or using management vulnerability to illegally access the core network, illegally controlling the base station to conduct network attacks to the core network, exploiting the core network vulnerability to obtain core network permissions to illegally obtain, forge, tamper with service data, or attack service terminals. Similarly, the core network is in a controllable physical environment and has protection functions such as security filtering, making it difficult to launch such attacks.

f) Internal network boundary

The internal network boundary might be breached so that the service main station is under attacks. Attacks can be initiated from the service terminal or the core network to attack the internal network of the company. The attacker can also break through the border of the internal network in the management information to attack the service terminal. However, the internal network boundary comprehensively utilizes hardware firewall, encryption and authentication devices, and horizontal one-way security isolation device. So this type of attack is difficult to carry out.

(2) Application level risk

By destroying physical protection devices or exploiting management vulnerabilities, and further utilizing software system bugs, weak passwords, and improper policy configuration, the permission of network management system could be illegally acquired, thereby causing risks such as leakage of sensitive information and tampering of configuration information.

(3) Host level risk

The hosts inside the PWPNs could be infected with a malicious code such as viruses and cannot work normally. An attacker can exploit the host system vulnerability, weak password, improper policy configuration, etc. to attack the network management system, causing the system to fail to operate normally and system data to leak. In the face of this type of attack, virtual private network technology is usually used to divide the security zone that can protect sensitive systems.

(4) Data level risk

The database in the core network is facing the risks such as SQL (Structured Query Language) injection, default account password, database platform vulnerability, abuse of legal authority, and illegal lifting of rights.

III. Security Architecture of PWPN

A. Protection Objectives of Power wireless private

Considering the risk which the PWPNs face, we can see that the PWPNs carries information transmission and the wireless terminal, base station and core network are invaded and the risk is small. Host and data-level security threats can be prevented by traditional security measures. The main risk of PWPNs is interference and intrusion of wireless channel, which affects base station and core network. Therefore, the main protection objectives of the PWPNs include:

(1) Ensure that the PWPNs are safe in itself, in order to prevent the PWPNs from affecting the security and stable operation of the service system due to the attack.

(2) Ensure the wireless transmission of power is safe, so that the service data carried by the PWPNs is illegally eavesdropped or tampered during transmission.

(3) Ensure the access of service terminals and the secure of network borders to prevent unauthorized access to the company's internal network or service system through the PWPNs.

B. Service-based PWPNs security architecture

The power communication network carries the power services, including precise load control, distribution automation, and information collection of power consumption. In order to ensure the safe, stable and reliable transmission of high-level services, we have designed a PWPNs security architecture based on service isolation. The design objective of the proposed architecture is to achieve horizontal isolation of production control area and management information area. Furthermore, the dedicated channel for precise load control services is provided to guarantee the delay and secure access requirements of the millisecond-level precise control service. The specific plan is listed.

(1) Air interface and base station side: The air interface uses independent time-frequency resources. The base station equipment uses independent baseband board/port and transmission board/port to process and transmit different services, and realizes the physical isolation of precision control service, other control service and management information.

(2) Transmission channel: Different services are transmitted through the independent Ethernet card/port of the SDH/MSTP device, and the physical isolation of the fine control service, other control services, and management information area services is realized in the transmission channel.

(3) Core network side: realize physical isolation between precision control service and other control services and management information through two sets of equipment.

The optimized architecture is shown in Figure 2. The physical isolation transmission channels are provided for different services to meet the security access requirements of various services.

(1) For the precision control service: Provide dedicated channels for precision control services through independent time-frequency resources, base station transmission boards/ports, SDH transmission channels, and core network equipment/ports.

(2) For the load control service: Provide physical isolation channel from the service of management information area through the independent time-frequency resources, base station transmission boards/ports, SDH transmission channels to remote measure/control/communication, the information collection and other control services. In addition, the control services are isolated by APN (Access Point Name) and VPN (Virtual Private Network), and resources are guaranteed by configuring QCI (QoS Class Identifier) priorities for different services

The precision control service and load control service are access the production control area, such as control room and transformer substation.

(3) Management information area service: Management information area services include fixed information acquisition terminals and mobile acquisition terminals. These services will transmitted to management information. The independent time-frequency resources, transmission board of base station, the SDH transmission channel, and the core network equipment provide a physical isolation channel between the service of management information area and the service of production control area. The services in the management information region are isolated through APN and VPN, and the resources are guaranteed for QCI priority by configuring QCI priority for different services.

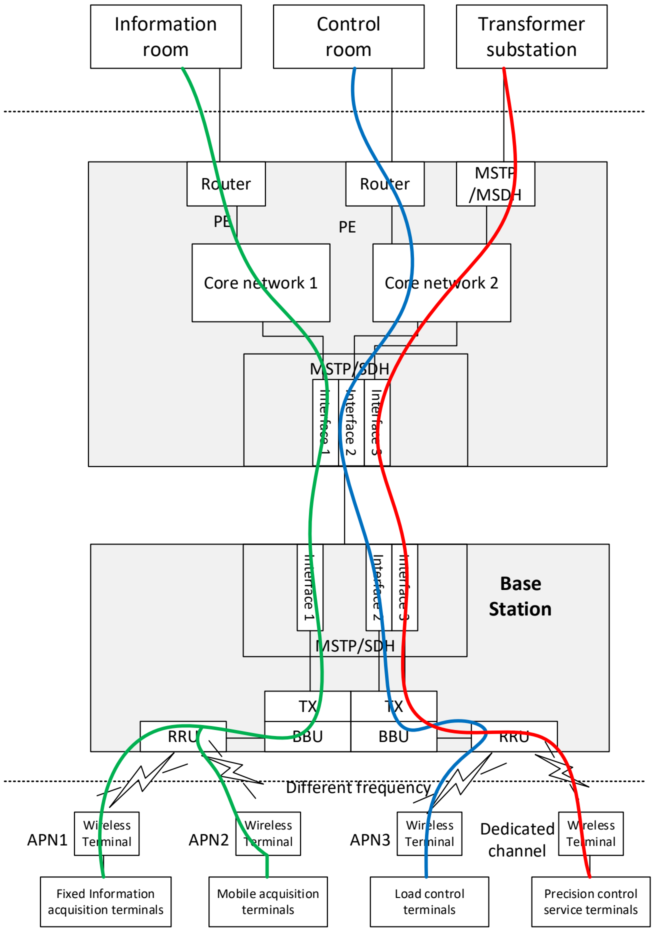
C. Experiments and Discussions

The proposed security architecture adopts different working frequencies, RRU (Radio Remote Unit) and BBU (Base band Unit) , as well as different core networks according to the different type of services, to realize the security protection of different service bursts and improve the reliability of the system.

The proposed security architecture is evaluated using a LTE-G230 system which is designed by Potevio Information

Technology Co., Ltd. For the interference effect of the wireless channel, the interference threshold can be tolerated by no more than -81dBm when the minimum reference signal receiving power (RSRP) of network coverage of the LTE-G230 system is not less than -90dBm. When the RSRP is no less than -110dbm, the interference threshold can be tolerated no more than -105dbm. It can be seen that the current device design can resist the interference of illegal signals to a certain extent.

In order to verify the service isolation, three different types of services are loaded from the terminals. When any two types of traffic are overloaded, the throughput and delay of the third type of traffic are not affected. The experimental results show a good service quality assurance effect for important service.



PE: Provider Edge
CE: Customer Edge
MSTP: Multi-Service Transfer Platform
SDH: Synchronous Digital Hierarchy

Fig. 2. Security network architecture for Smart Grid

IV. Conclusion

PWPNs face a lot of security threats. To improve the security, a service-based architecture is proposed in this paper. First, the security risks faced by the PWPNs are analyzed. The sources of security threats on the end-to-end communication link are present. The proposed architecture provides service isolation and security protection from terminals, wireless channels, base stations, core networks, and application systems. Practice has proved that the protection method has better service protection characteristics and can guarantee the performance of various services of the PWPNs.

References

[1] Yan, Ye, et al. "A survey on cyber security for smart grid communications." IEEE Communications Surveys and tutorials 14.4 (2012): 998-1010.

[2] Lin, Jie, et al. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE Internet of Things Journal 4.5 (2017): 1125-1142.

[3] Hahn, Adam, et al. "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid." IEEE Transactions on Smart Grid 4.2 (2013): 847-855.

[4] Metke, Anthony R., and Randy L. Ekl. "Security technology for smart grid networks." IEEE Transactions on Smart Grid 1.1 (2010): 99-107.

[5] Tan, Song, et al. "Survey of security advances in smart grid: A data driven approach." IEEE Communications Surveys & Tutorials 19.1 (2017): 397-422.

[6] Da Guo, Yong Zhang, Guangnian Xu, and Park Hyeongchun, spectrum aggregation scheme in wireless broadband data transceiver system, International Journal of Robotics and Automation, 2018, 33(5): 510-517

[7] Miao, Wei-Wei, et al. "Analysis on TD-LTE wireless private network capacity meeting the interaction demand of future smart grid." Journal of International Council on Electrical Engineering 8.1 (2018): 57-64.

[8] Gözde, Haluk, et al. "4G/LTE technology for smart grid communication infrastructure." Smart Grid Congress and Fair (ICSG), 2015 3rd International Istanbul. IEEE, 2015.

[9] Miao, Weiwei, et al. "Coverage Analysis in TD-LTE Wireless Private Networks for Power Systems: A 3D Ray-Tracing Approach." Big Data and Smart Computing (BigComp), 2018 IEEE International Conference on. IEEE, 2018.

[10] Raza, Muhammad Taqi, Fatima Muhammad Anwar, and Songwu Lu. "Exposing LTE Security Weaknesses at Protocol Inter-Layer, and Inter-Radio Interactions." International Conference on Security and Privacy in Communication Systems. Springer, Cham, 2017.

[11] Sattar, Danish, et al. "Threat Modeling in LTE Small Cell Networks." 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE). IEEE, 2018.

[12] Ahmed, Kazi J., and Myung J. Lee. "Secure, LTE-based V2X service." IEEE Internet of Things Journal (2017).

[13] Zhao, Caidan, et al. "Secure machine-type communications toward LTE heterogeneous networks." IEEE Wireless Communications 24.1 (2017): 82-87.